170x240titel.fm Seite 1 Freitag, 18. Oktober 2002 3:50 15

Firewall-Systeme

170x240titel.fm Seite 2 Freitag, 18. Oktober 2002 3:50 15

170x240titel.fm Seite 3 Freitag, 18. Oktober 2002 3:50 15

Norbert Pohlmann

Firewall-Systeme

5., aktualisierte Auflage

170x240titel.fm Seite 4 Freitag, 18. Oktober 2002 3:50 15

Die Deutsche Bibliothek –
CIP-Einheitsaufnahme

Ein Titeldatensatz für diese Publikation ist bei
Der Deutschen Bibliothek erhältlich.

ISBN 3-8266-0988-3
5., aktualisierte Auflage 2003

Alle Rechte, auch die der Übersetzung, vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (Druck, Fotokopie, Mikrofilm oder einem anderen Verfahren) ohne schriftliche Genehmigung des Verlages reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden. Der Verlag übernimmt keine Gewähr für die Funktion einzelner Programme oder von Teilen derselben. Insbesondere übernimmt er keinerlei Haftung für eventuelle, aus dem Gebrauch resultierende Folgeschäden.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Printed in Germany
© Copyright 2003 by mitp-Verlag/Bonn,
ein Geschäftsbereich der verlag moderne industrie Buch AG & CO. KG/Landsberg

Lektor: Norbert Schwob, Aachen
Satz: reemers publishing services gmbh, Krefeld
Druck: Media-Print, Paderborn

fw5IVZ.fm Seite 5 Samstag, 19. Oktober 2002 11:37 11

Inhaltsverzeichnis

Über den Autor 17

Vorwort 19

Übersicht 21

1 **Einführung: Gesellschaftlicher Wandel und IT-Sicherheit** 25
1.1 Entwicklung von IT-Technologie und IT-Sicherheit 25
1.2 Siegeszug des Internet 26
1.3 Gefahren aus dem Internet 30
1.4 Notwendigkeit von IT-Sicherheit 32
1.5 IT-Sicherheit als Wirkungs- und Handlungszusammenhang 35
1.6 Chancen und Risiken – zwei Extreme der Ungewissheit 36
1.7 Der Firewall-Markt 38
1.8 Fazit 40

2 **Ziele von Firewall-Systemen** 43
2.1 Analogien zu Firewall-Systemen 43
2.2 Zielsetzung eines Firewall-Systems 46

3 **TCP/IP-Technologie für Internet und Intranet** 51
3.1 Von den Anfängen bis heute 51
3.2 Vorteile der TCP/IP-Technologie 53
3.3 Das OSI-Referenzmodell 54
3.4 TCP/IP-Protokollarchitektur 56
3.5 Internet-Adressen 58
3.6 Die Kommunikationsprotokolle 61
3.6.1 IP-Protokoll 61
3.6.2 Routing Protokolle 63
3.6.3 ICMP 64
3.6.4 Portnummern 67
3.6.5 UDP 69
3.6.6 TCP 70

fw5IVZ.fm Seite 6 Samstag, 19. Oktober 2002 11:37 11

3.6.7	DNS	72
3.6.8	Telnet	72
3.6.9	FTP	73
3.6.10	SMTP	74
3.6.11	HTTP	75
3.6.12	NNTP	79
4	**Bedrohungen im Netz**	81
4.1	Angriffsmöglichkeiten in Kommunikationssystemen	81
4.1.1	Passive Angriffe	82
4.1.2	Aktive Angriffe	85
4.1.3	Zufällige Verfälschungsmöglichkeiten	88
4.2	Weitere Aspekte potenzieller Bedrohungen bei der Kommunikation über das Internet	90
4.2.1	Angriffstools aus dem Internet	92
4.2.2	Implementierungsfehler in Anwendungen und fehlerhafte Konfigurationen	92
4.3	Wie hoch ist das Risiko?	92
4.4	Schadenskategorien und Folgen	93
4.4.1	Verstoß gegen Gesetze/Vorschriften/Verträge	93
4.4.2	Beeinträchtigung der persönlichen Unversehrtheit	94
4.4.3	Beeinträchtigung der Aufgabenerfüllung	94
4.4.4	Negative Außenwirkung	95
4.4.5	Finanzielle Auswirkungen	95
4.5	Angriffsmethoden und prinzipielle Gegenmaßnahmen auf der Grundlage der TCP/IP-Protokolle	96
4.5.1	Idee eines Angriffs	96
4.5.2	Analyse des Netzes mithilfe von Scannerprogrammen	97
4.5.3	Password-Snooping und IP-Maskerade	99
4.5.4	Nutzung einer falschen Konfiguration	103
4.5.5	Hopping (Telnet)	105
4.5.6	Nutzung von Implementierungsfehlern in Anwendungen wie z. B. sendmail	106
4.5.7	IP-Adressen-Spoofing	108
4.5.8	ICMP-Angriffe	109
4.5.9	Internet-Routing-Angriffe	112
4.6	Ergebnisse der KES/Utimaco-Studien	112
4.7	Zusammenfassung	112

fw5IVZ.fm Seite 7 Samstag, 19. Oktober 2002 11:37 11

5	**Elemente eines Firewall-Systems**	115
5.1	Aktive Firewall-Elemente	116
5.1.1	Architektur von aktiven Firewall-Elementen	116
5.1.2	Designkonzept aktiver Firewall-Elemente	118
5.2	Packet Filter	120
5.2.1	Allgemeine Arbeitsweise von Packet Filtern	121
5.2.2	Überprüfungen auf der Netzzugangsebene	122
5.2.3	Überprüfungen auf der Netzwerkebene	124
5.2.4	Überprüfungen auf der Transportebene	125
5.2.5	Strategien für den Aufbau und die Bewertung der Filterregeln	130
5.2.6	Beispiel für den Einsatz eines Packet Filters	130
5.2.7	Dynamischer Packet Filter	133
5.2.8	Benutzerorientierter Packet Filter	134
5.2.9	Sicherheitsrelevante Informationen in einem Packet Filter	138
5.2.10	Realisierungsformen für Packet Filter	139
5.2.11	Anwendungsgebiete von Packet Filtern	141
5.3	Zustandsorientierte Packet Filter (stateful inspection)	142
5.4	Application Gateway/Proxy-Technik	144
5.4.1	Allgemeine Arbeitsweise des Application Gateway	145
5.4.2	Die Proxies	147
5.4.2.1	Application Level Proxies	147
5.4.2.2	SMTP Proxy	148
5.4.2.3	Benutzerorientierte Application Level Proxies	150
5.4.2.4	Telnet Proxy	152
5.4.2.5	FTP Proxy	157
5.4.2.6	HTTP Proxy	159
5.4.2.7	Java Proxy	161
5.4.2.8	E-Commerce Proxy	162
5.4.2.9	Authentication Proxy (Global Authentication)	165
5.4.2.10	Transparent Proxy	166
5.4.2.11	Spezielle Proxies	166
5.4.2.12	Circuit Level Proxies	166
5.4.2.13	SOCKS	172
5.4.2.14	Anwendungsbeispiel für den SOCKS v5 Server	177
5.4.3	Anwendungsgebiete von Application Gateways	178
5.5	Adaptive Proxy	179
5.6	Firewall-Elemente und das Verhältnis von Geschwindigkeit zu Sicherheit	180

fw5IVZ.fm Seite 8 Samstag, 19. Oktober 2002 11:37 11

5.7 Security Management für aktive Firewall-Elemente 181

6 Konzepte für Firewall-Systeme 185
6.1 Ausschließlicher Einsatz eines Packet Filters 185
6.2 Ausschließlicher Einsatz eines Application Gateway 187
6.3 Kombination von Firewall-Elementen 189
6.3.1 Packet Filter und single-homed Application Gateway 190
6.3.2 Packet Filter und dual-homed Application Gateway 193
6.3.3 Zwei Packet Filter als Screened Subnet und ein single-homed Application Gateway 196
6.3.4 Zwei Packet Filter als Screened Subnet und ein dual-homed Application Gateway (High-level-Security-Firewall-System) 197
6.4 Möglichkeiten eines High-level-Security-Firewall-Systems 200
6.4.1 Internet Server 200
6.4.2 Intranet Server 203
6.4.3 Mehrere Application Gateways parallel 204
6.5 Das richtige Firewall-Konzept für jeden Einsatzfall 206
6.6 Mail-Konzept 209
6.7 DNS-Konzepte 211

7 Firewall-Systeme und Verschlüsselung 213
7.1 Sicherheitsmechanismen für Verschlüsselung und Digitale Signatur 214
7.1.1 Private-Key-Verfahren 214
7.1.2 Public-Key-Verfahren 215
7.1.3 One-Way-Hashfunktion 217
7.1.4 Hybride Verschlüsselungstechnik 217
7.1.5 Ein Wettlauf um die Sicherheit 218
7.1.6 Zertifikations-Systeme 218
7.1.7 Chipkarte (SmartCard) 226
7.2 E-Mail Security 229
7.2.1 »Briefumschlag« und »Unterschrift« für die elektronische Post 230
7.2.2 Sicherheitsdienste des E-Mail-Sicherheitssystems 235
7.2.3 E-Mail Security aus Sicht des Benutzers 235
7.2.4 Objektverschlüsselung und Firewall-Systeme 235
7.2.5 Der elektronische Vertrag: Die Rechtsform der Zukunft? 236
7.2.6 Unterschiedliche Konzepte für objektorientierte Sicherheit (S/MIME, PGP) 237

fw5IVZ.fm Seite 9 Samstag, 19. Oktober 2002 11:37 11

7.2.7 Der Markt bestimmt den Erfolg 242
7.2.8 TeleTrusT – ein interdisziplinärer Verein zur Förderung der Vertrauenswürdigkeit in der Informations- und Kommunikationstechnologie 243
7.2.9 MailTrusT – interoperable Sicherheitslösung 244
7.2.10 ISIS-MTT-Spezifikation für Interoperabilität und Testsysteme 249
7.2.11 Bridge-CA 250
7.3 Virtual Private Networks (VPN) 256
7.3.1 Grundlagen 256
7.3.2 Anwendungsformen von VPNs 259
7.4 Secure Socket Layer (SSL) 262
7.5 Virtual Private Networks, Secure Socket Layer und Firewall-Systeme. 265
7.6 Vergleich zweier Konzepte: E-Mail Security versus VPN/SSL-Sicherheit 267
7.7 Firewall-Systeme versus VPN/SSL-Systeme 268

8 Authentikationsverfahren 271
8.1 Identifikation und Authentikation 271
8.2 Generelle Authentikationsverfahren 273
8.2.1 Passwort-Verfahren 273
8.2.2 Einmal-Passwort 274
8.2.3 Challenge-Response-Verfahren 274
8.3 Authentikationsverfahren für Firewall-Systeme 275
8.3.1 S/Key (MD5) 275
8.3.2 Authentikationsverfahren mit Security Token 278
8.3.3 Signaturkarte (Chipkarte) 280
8.3.4 SSL Client Authentication 282
8.3.5 Authentikationsverfahren mittels Mobiltelefon 284

9 Verschiedene Firewall-Lösungen und ihre Bewertung 287
9.1 Public Domain Software oder ein Firewall-Produkt? 287
9.1.1 Public Domain Software für die Firewall-Application 287
9.1.2 Firewall-Produkte 288
9.1.3 Linux als sicheres Betriebssystem für Firewall-Lösungen 289
9.1.4 Anforderungen an ein Firewall-Betriebssystem 289
9.2 Software-Lösung oder Turn-Key-Lösung? 291
9.2.1 Was bietet eine Software-Lösung? 291
9.2.2 Was ist eine Turn-Key Lösung? 293

fw5IVZ.fm Seite 10 Samstag, 19. Oktober 2002 11:37 11

9.3 Kriterien für die Beurteilung der tatsächlichen Sicherheitsleistung eines Firewall-Produktes 294
9.3.1 Offene und transparente Sicherheit 294
9.3.2 Geprüfte, nachweisbare Sicherheit 295
9.3.3 Sicherheit ohne staatliche Restriktionen 295

10 Praktischer Einsatz von Firewall-Systemen 297
10.1 Sichere Kopplung des eigenen Intranet an das Internet 299
10.2 Internet Server 301
10.3 Intranet Security (VPN) 303
10.3.1 Höhere End-to-End-Sicherheit 304
10.3.2 Abschottung von Organisationseinheiten untereinander 306
10.3.3 Skalierbare Sicherheit 307
10.4 Remote Access (Tele-Arbeit, Mobil-Arbeitsplätze) 307
10.5 Ankopplung besonderer Organisationseinheiten 309
10.6 Externe Modem-Anschlüsse 311
10.7 Modem-Verbindungen aus dem unsicheren Netz in das zu schützende Netz 312
10.8 Virengefahr 313
10.8.1 Integration von Viren-Scannern am Common Point of Trust 314
10.8.2 Weitere technische, personelle und organisatorische Maßnahmen . . 319
10.9 Intrusion-Detection-Systeme 320
10.10 Personal Firewall 322
10.11 Security Gateway 323
10.11.1 Das Authentication Gateway 324
10.11.2 Secure E-Mail Gateway 331
10.11.3 Signature Server 334
10.11.4 Zusammenfassung 337

11 Ein Firewall-System ist mehr als ein Produkt 339
11.1 Firewall-Sicherheitspolitik 339
11.1.1 Sicherheitsziele 340
11.1.2 Darstellung der zu schützenden Ressourcen 341
11.1.3 Festlegung von Kommunikationsanforderungen 341
11.1.4 Festlegung von Diensten und Anwendungen 342
11.2 Zusätzliche Sicherheitsmaßnahmen 344
11.2.1 Infrastruktur 345
11.2.2 Organisation 346

fw5IVZ.fm Seite 11 Samstag, 19. Oktober 2002 11:37 11

11.2.3 Personal 351
11.2.4 Notfall 354
11.3 Konzeptionelle Grenzen eines zentralen Firewall-Systems 354
11.3.1 Hintertüren 354
11.3.2 Interne Angriffe 355
11.3.3 Angriffe auf Datenebene 355
11.3.4 Trittbrettfahrer 355
11.3.5 Richtige Sicherheitspolitik und richtige Umsetzung der Sicherheitpolitik 355
11.3.6 Wissen und Hypothese 356
11.3.7 Security versus Connectivity – Risiko versus Chance 356
11.3.8 Vertrauenswürdigkeit des Kommunikationspartners und der empfangenen Daten 357
11.3.9 Zusammenfassung 357
11.4 Praktische Sicherheit 358

12 Besondere Aufgabenstellungen bei Firewall-Systemen 361
12.1 Network Address Translation 361
12.1.1 Firewall-System und Network Address Translation 362
12.1.2 Probleme für Netze, die mit illegalen IP-Adressen arbeiten 363
12.2 Domänen-Namen (Domain-Namen) 364
12.3 Verwaltung mehrerer Firewall-Systeme mithilfe eines Security Managements 364
12.4 Geschachtelte Firewall-Konstellationen 365
12.5 Verfügbarkeit 366

13 Weiterführende Aufgabenstellungen bei Firewall-Systemen 369
13.1 Logbuch – Belastung oder Nutzen? 369
13.1.1 Ziele der Protokollierung 369
13.1.2 Protokollierung von Ereignissen 370
13.1.3 Alarmierung 371
13.1.4 Beweissicherung 372
13.1.5 Schutz der Protokolldaten 373
13.1.6 Reaktionen auf eine Sicherheitsverletzung 373
13.1.7 Datenschutzaspekte 375
13.2 Aktive WWW-Inhalte – Java und seine Verwandten 376
13.2.1 Java 380
13.2.2 JavaScript 384

fw5IVZ.fm Seite 12 Samstag, 19. Oktober 2002 11:37 11

13.2.3 ActiveX 385
13.3 Firewall-Systeme zur Risikominimierung 386
13.3.1 Total Cost of Ownership 387
13.3.2 Beschaffungsphase eines Firewall-Systems 387
13.3.3 Aufrechterhaltung des Betriebs eines Firewall-Systems 389
13.3.4 Zusammenfassung der Kosten im Sinne der Total Cost of Ownership 392
13.3.5 Kosten-Nutzen-Betrachtung im Hinblick auf die Sicherheit 393
13.3.6 Kosten-Nutzen-Betrachtung im Hinblick auf die Nicht-Realisierung von Kommunikation 395
13.3.7 Gesamtwirtschaftliche Betrachtung von Firewall-Systemen 395
13.4 Evaluierung und Zertifizierung von Firewall-Systemen 396
13.4.1 ITSEC-Zertifizierung 398
13.4.1.1 Wirksamkeit der Firewall-Sicherheitsmechanismen 404
13.4.1.2 Mechanismenstärke und Evaluationsstufen 407
13.4.1.3 Korrektheit der Firewall-Sicherheitsmechanismen 410
13.4.2 ICSA-Zertifizierung 411
13.5 Weiterentwicklung von umfassenden Firewall-Systemen 414
13.6 Überprüfung von Firewall-Systemen im Betrieb (Security Audit) . . . 416
13.6.1 Einleitung 416
13.6.2 Definition von Security Audit 417
13.6.3 Komponenten eines Security Audit 421
13.6.4 Werkzeuge zur technischen Datensammlung 423
13.6.5 Zusätzliche Informationsquellen 428
13.6.6 Allgemeine Mailinglisten 429
13.7 Intrusion-Detection/Response-Systeme 430
13.7.1 Einleitung 430
13.7.2 Unterscheidung zwischen Detection und Response 431
13.7.3 Einbindung in Firewall-Systeme 432
13.7.4 Hauptaufgaben des IDS 432
13.7.5 Aufbau und Funktionsweise von IDS 433
13.7.6 Auswertekonzepte 436
13.7.7 Grenzen von IDS 440
13.8 DDoS-Angriffe – Beschreibung und Bewertung 441
13.8.1 Allgemeine Funktionsweise der DDoS-Angriffe 441
13.8.2 Weitere Entwicklung der DDoS-Tools 444
13.8.3 Zusammenfassende Bewertung 444
13.8.4 Bisher unbekannte Aspekte 444

fw5IVZ.fm Seite 13 Samstag, 19. Oktober 2002 11:37 11

13.9 Personal Firewall 445
13.9.1 Risiken bei der Internet-Anbindung 445
13.9.2 Zentrales Firewall-System 447
13.9.3 Virenscanner 448
13.9.4 Ziel einer Personal Firewall 448
13.9.5 Komponenten 449
13.9.6 Sicherheitskomponenten einer Personal Firewall 450
13.9.7 Beispiel: Schutz vor dem »I love You«-Virus 451
13.9.8 Sichere Umgebung für digitale Signaturen 452
13.9.9 Darstellung, Protokollierung und Statistik sicherheitsrelevanter Ereignisse 453
13.9.10 Fazit 453

14 Theoretische Grundlagen von Firewall-Systemen 455
14.1 Definition eines Kommunikationsmodells 455
14.1.1 Definition der Transmitter 458
14.1.2 Definition der Receiver 458
14.1.3 Definition der Protokollelemente 458
14.1.4 Definition der Aktionen 460
14.1.5 Kommunikationsabläufe 461
14.1.6 Angriffe aus dem Netz 462
14.1.6.1 Angriffe durch Dritte 463
14.1.6.2 Angriffe durch den Kommunikationspartner 465
14.2 Definition eines Firewall-Elements 468
14.3 Definition des Kommunikationsmodells mit integriertem Firewall-System 471
14.4 Angriffe auf das Firewall-System 473
14.5 Grundsätzliche Einflussfaktoren auf die Auswahl und Durchführung der Aktion auf der Empfängerseite 474
14.5.1 Fehlerquellen durch Angriffe aus dem Netz 474
14.5.2 Fehlerquellen der Kommunikationslösung beim Receiver 475
14.5.3 Fehlerquellen des Firewall-Systems 475
14.5.4 Sicherheitsdienste eines Firewall-Systems 476
14.5.5 Sicherheitsziele bei der Umsetzung eines Firewall-Systems 479
14.5.6 Einflussfaktoren auf die Sicherheit und Vertrauenswürdigkeit von Firewall-Systemen 480
14.5.7 Die Wirkung der Sicherheitsdienste 481
14.5.7.1 Zugangskontrolle auf der Netzwerkebene 482

fw5IVZ.fm Seite 14 Samstag, 19. Oktober 2002 11:37 11

14.5.7.2 Zugangskontrolle auf Benutzerebene 483
14.5.7.3 Zugangskontrolle auf Datenebene 483
14.5.7.4 Rechteverwaltung 483
14.5.7.5 Kontrolle auf der Anwendungsebene 484
14.5.7.6 Entkopplung von Diensten 484
14.5.7.7 Beweissicherung und Protokollauswertung 484
14.5.7.8 Alarmierung 485
14.5.7.9 Verbergen der internen Netzstruktur 485
14.5.7.10 Grundlegende Aspekte für die Erbringung der Sicherheitsdienste . 485
14.5.8 Die Wirkung der Einsatzumgebung 488
14.5.8.1 Vertrauenswürdigkeit des Netzes 489
14.5.8.2 Vertrauenswürdigkeit des Kommunikationspartners 489
14.5.8.3 Sicheres Security Management 490
14.5.8.4 Sicheres Betriebssystem 490
14.5.8.5 Firewall-Schutzmechanismen 491
14.5.9 Die Wirkung einer vertrauenswürdigen Realisierung eines Firewall-Systems 492
14.5.10 Die Wirkung der Einflussfaktoren der eigenen Organisation 493
14.5.10.1 Bewertung der Einfussfaktoren der eigenen Organisation 493
14.5.10.2 **Infrastruktur** **494**
14.5.10.3 **Organisation** **494**
14.5.10.4 **Personal** **495**
14.5.10.5 **Notfall** **495**
14.5.10.6 Sicherheitspolitik 495
14.5.10.7 Sicherer Betrieb von aktiven Firewall-Elementen 496
14.5.11 Die Wirkung der unterschiedlichen Firewall-Konzepte 498
14.5.12 Die Wirkung weiterer Sicherheitsmechanismen 500
14.5.13 Zusammenfassung der Wirkung eines umfassenden Firewall-Systems 501
14.6 Sicherheitsmechanismen und deren Wirkung 501
14.7 Angriffe und die Wirkung von unterschiedlichen Sicherheitsmechanismen 507
14.8 Zusammenfassung 512

15 Recht im Internet 513
15.1 Aktuelle Formen des Delikts »Computerkriminalität« 513
15.1.1 Persönlichkeitsrechtsverletzungen 514
15.1.2 Wirtschaftsdelikte 514

fw5IVZ.fm Seite 15 Samstag, 19. Oktober 2002 11:37 11

15.1.3 Sonstige Delikte 516
15.2 Rechtsfragen 517
15.3 Paradigmenwechsel und Perspektiven 517
15.4 Zusammenfassung 519

16 Computerkriminalität – Fakten und Zahlen 521
16.1 Kriminalitätsstatistik des BKA 521
16.2 Schätzungen der Schadenshöhe 524
16.3 Fallbeispiele 524

A Sicherheitsstandards 529
A.1 S-HTTP 530
A.2 SSL/TLS 533
A.3 SKIP 536
A.4 IPv6 538
A.5 IPSec 539
A.5.1 IPSec – Internet Protocol Security Architecture 539
A.5.2 Der Authentication Header (AH) 540
A.5.3 Encapsulated Security Payload (ESP) 542
A.5.4 Security Association 545
A.5.5 IPSec-Datenbanken 545
A.5.6 Schlüsselverwaltung unter IPSec 545

B Wichtige Adressen 547
CERT in Deutschland 548

C Legende 549

D Firewall-Produkte 551

E Literaturverzeichnis 553

F Sicherheitsanforderungen an Internet-Firewalls (BSI) 559
F.1 Einleitung 559
F.2 Gefährdungen bei der Benutzung des Internet 559
F.2.1 Vielfalt der Netzdienste 560
F.2.2 Verlust der Vertraulichkeit und Integrität 560
F.2.3 Konzeptionsfehler 561

fw5IVZ.fm Seite 16 Samstag, 19. Oktober 2002 11:37 11

F.2.4 Missbrauch von frei verfügbaren Informationen 562
F.3 Schutzmöglichkeiten 562
F.4 Forderungen an Firewalls 565
F.4.1 Forderungen zur Abwehr von Angriffen auf die Firewall-Anordnung 565
F.4.2 Forderungen zur Abwehr von Angriffen aus dem Internet auf das zu sichernde Netz 567
F.4.3 Organisatorische Maßnahmen 572
F.5 Adressen zu Anhang F 573
F.6 Literatur zu Anhang F 574

G Glossar, Abkürzungen 575

H Stichwortverzeichnis 599

neuKap00_Autor.fm Seite 17 Freitag, 18. Oktober 2002 3:50 15

Über den Autor

Norbert Pohlmann studierte Elektrotechnik mit dem Schwerpunkt Informatik. Von 1997 bis 2001 arbeitete er an seiner Dissertation zum Thema »Möglichkeiten und Grenzen von Firewall-Systemen«. Er war von 1985 bis 1988 Forschungsingenieur und später Leiter des Labors für Telematik an der Fachhochschule Aachen, in dem viele Forschungs- und Entwicklungsprojekte durchgeführt wurden, die sich mit der Einbindung von Sicherheitsmechanismen in IT-Systeme beschäftigten.

1988 gründete Norbert Pohlmann zusammen mit Professor Dr. Christoph Ruland das Unternehmen KryptoKom, Gesellschaft für kryptographische Informationssicherheit und Kommunikationstechnologie mbH, in Aachen. Das international tätige Systemhaus (Hardware, Software, Dienstleistungen, Consulting) expandierte rasch, wurde in vielen Bereichen der IT-Sicherheit Marktführer im deutschsprachigen Raum und beschäftigte 1998 mehr als hundert Mitarbeiter. Am 1. Juli 1999 fusionierte die KryptoKom GmbH mit der Utimaco Safeware AG in Oberursel; Norbert Pohlmann ist seit dem 1. Oktober 1999 Vorstandsmitglied der Utimaco Safeware AG.

Als Experte für Sicherheit in der IT-Sicherheit befasst sich Norbert Pohlmann bereits seit 1985 aktiv mit Kryptographie und ihren Anwendungsgebieten. Als Gründungsmitglied, seit 1994 Vorstandsmitglied und seit April 1998 Vorstandsvorsitzender von TeleTrusT e.V., hat er sich die Etablierung von vertrauenswürdigen IT-Systemen zur Aufgabe gemacht.

Mehrere Bücher und zahlreiche Fachartikel, Vorträge und Seminare zu Themen der Informationssicherheit dokumentieren seine Fachkompetenz und sein Engagement auf diesem Gebiet. Neben seinem nun in der fünften Auflage erschienenen Fachbuch »Firewall-Systeme – Sicherheit für Internet und Intranet« ist der Titel »Virtual Private Networks« von Markus a Campo und Norbert Pohlmann im MITP-Verlag verfügbar.

Norbert Pohlmann ist Träger des Preises der Stadt Aachen für Innovation und Technologie 1997 und wurde 1999 von der Zeitschrift ›IT.Services‹ als »Vordenker der deutschen Computerindustrie« ausgezeichnet.

neuKap00_Autor.fm Seite 18 Freitag, 18. Oktober 2002 3:50 15

Norbert Pohlmann ist Mitinitiator und Vorsitzender des Programmkomitees der »Information Security Solutions Europe«-Konferenzen (ISSE). Die erste Konferenz fand im Oktober 1999 statt. Die zweite ISSE wurde im September 2000 in Barcelona und die dritte im September 2001 in London erfolgreich durchgeführt. Die ISSE 2002 findet im Oktober in Paris statt.

Dr. Norbert Pohlmann
Utimaco Safeware AG

norbert.pohlmann@utimaco.de www.utimaco.de

neuKap00_Vorwort.fm Seite 19 Freitag, 18. Oktober 2002 3:50 15

Vorwort

Gegenwärtig erleben wir den Wandel zur Informations- und Wissensgesellschaft. Das Internet, das »Netz der Netze«, ist in den letzten Jahren rasant gewachsen und hatte Ende 2001 schätzungsweise 500 Millionen Nutzer.

Im Wirtschaftsleben ist zu beobachten, dass immer mehr Geschäftsprozesse mithilfe von IT-Systemen über das Internet abgewickelt werden. Damit nimmt auch die Notwendigkeit zu, angemessene IT-Sicherheitsmaßnahmen zu verwenden, damit in der »elektronischen Welt« eine Basis der Vertrauenswürdigkeit bestehen kann. Die herkömmlichen Geschäftsprozesse in der »realen Welt« wurden und werden durch Sicherheitsmechanismen wie Pförtner, Sicherheitstransporter, Safes usw. geschützt. Diese können zwar keine hundertprozentige Sicherheit gewährleisten, aber mit ihrer Hilfe kann man Risiken wirksam begrenzen. Solche – oder äquivalente – Sicherheitsmechanismen benötigen wir auch in der elektronischen Welt.

Das gilt um so mehr, wenn wir den immer weiter steigenden Wert elektronischer Informationen in Betracht ziehen. Immer öfter stellen Daten, die auf Rechnersystemen gespeichert oder durch Netze übertragen werden, erhebliche finanzielle Werte dar. Dazu zählen Entwicklungsunterlagen, Kundendaten, Logistikinformationen oder auch Strategiekonzepte, die z. B. Börsenwerte beeinflussen können. Diese Bits und Bytes können leicht mehrere Millionen Euro wert sein.

Dieser Entwicklung steht das häufig mangelnde Unrechtsbewusstsein in der elektronischen Welt gegenüber: Wer in der realen Welt Unternehmenswerte entwenden will, der muss über Zäune klettern, Türen und Fenster aufbrechen, vielleicht sogar Tresore sprengen. Jedem, der so etwas tut, ist bewusst, dass er eine Straftat begeht! In der elektronischen Welt können Hacker und Cracker mit Kaffee und Keksen vor dem Bildschirm sitzen und das Gleiche tun, aber sie haben dabei häufig nicht das Gefühl, etwas Unrechtes zu tun. Die Hemmschwelle ist niedriger, dadurch steigt die Wahrscheinlichkeit von Angriffen auf die elektronischen Werte.

In diesem Zusammenhang kommt ein wesentlicher Unterschied zwischen der elektronischen und der realen Geschäftswelt zum Tragen: In der elektronischen Welt müssen Unternehmen und Organisationen sich selbst gegen Gefahren schützen. Das Internet ist international, Gesetze sind gegenwärtig in ihrer Wirkung national begrenzt. Das heißt, der Staat kann zurzeit keinen angemessenen Schutz bieten. Bis internationale Gesetze – z. B. im Rahmen der G8-Bemühungen – diese

neuKap00_Vorwort.fm Seite 20 Freitag, 18. Oktober 2002 3:50 15

Lücke schließen, wird es sicherlich noch zehn Jahre dauern. Bis dahin müssen geeignete IT-Sicherheitsmaßnahmen die Lücken schließen.

Ähnlich wie in der traditionellen Geschäftswelt müssen wir auch in der elektronischen Geschäftswelt die Risiken begrenzen, um die Vorteile, die sich uns darin bieten, ausschöpfen zu können. Das heißt, wir müssen geeignete Sicherheitslösungen einsetzen und dafür sorgen, dass ihre Entwicklung mit der Entwicklung ihres Umfelds Schritt hält.

Die in der »realen Welt« bekannten und bewährten Sicherheitsmechanismen – Pförtner, Sicherheitstransporter, Safes usw. – stehen analog auch in der elektronischen Welt zur Verfügung.

So kontrolliert ein Firewall-System – entsprechend dem Pförtner am Eingang zu einem Firmengelände –, wer von außen auf die internen IT-Einrichtungen einer Organisation zugreifen will, und verhindert, dass durch unbefugte Zugriffe Schäden entstehen oder vertrauliche Informationen ausgespäht werden.

Dieses Buch verfolgt das Anliegen, dem Leser eine fundierte Einführung in das komplexe Themenfeld der Internet- und Intranet-Sicherheit zu geben. Es beschreibt die unterschiedlichen Ansätze von Firewall-Systemen und ihre theoretischen Grundlagen und zeigt ihre unterschiedlichen Einsatzmöglichkeiten. Damit gibt es dem Leser eine Hilfestellung für das Verständnis von Firewall-Systemen und für ihren praktischen Einsatz in Unternehmen und Organisationen.

In der jetzt vorliegenden 5. Auflage wurde das Buch erneut durchgesehen und aktualisiert. Das Kapitel 7 *Firewall-Systeme und Verschlüsselung* wurde um die SSL-Verschlüsselung ergänzt und der Abschnitt über Virtual Private Networks (VPN) wurde im Sinne einer Einführung in dieses weiterführende Thema umgestaltet. In Kapitel 10 *Praktischer Einsatz von Firewall-Systemen* wurde ein Abschnitt über das »Security Gateway«-Konzept hinzugefügt. Die Beschreibung des Security Audit wurde um einige praxisrelevante Aspekte erweitert und das Kapitel 14 *Theoretische Grundlagen von Firewall-Systemen* wurde weiter ausgearbeitet.

Mein Dank gilt den Firewall-Spezialisten der Utimaco Safeware AG und meinen Lesern, die mir auch weiterhin gerne Fragen stellen und Anregungen geben können. Sie erreichen mich dazu per E-Mail unter:

norbert.pohlmann@utimaco.de

neuKap00.fm Seite 21 Freitag, 18. Oktober 2002 3:50 15

Übersicht

Einleitung: Gesellschaftlicher Wandel und IT-Sicherheit

Die Einleitung zeigt mit »Meilensteinen« die Entwicklungssprünge der Informationstechnologie bis hin zu den Vorteilen der Internet- und Intranet-Technologie und den daraus folgenden gesellschaftlichen Veränderungen. Steigende Informationswerte führen zum Wandel von IT-Konzepten, mit der Notwendigkeit, sich mit dem Thema IT-Sicherheit auseinander zu setzen.

Ziele von Firewall-Systemen

Analogien verdeutlichen, dass die Sicherheitsmechanismen zur Absicherung von Geschäftsprozessen, die durch Technologieentwicklung über andere Medien als bisher abgewickelt werden, den neuen Bedingungen angepasst werden müssen. Die Sicherheitsziele, die mit einem Firewall-System realisierbar sind, werden dargestellt.

TCP/IP-Technologie für Internet und Intranet

Dieses Kapitel erläutert auf einfache Art und Weise die TCP/IP-Technologie mit ihren Nutzungsmöglichkeiten für Internet und Intranet, aber auch mit ihren Schwächen. Wer damit bereits vertraut ist, kann das Kapitel überspringen.

Bedrohungen aus dem Netz

Zuerst werden die potenziellen Angriffe auf Kommunikationssysteme beschrieben und eine Abschätzung über Eintrittswahrscheinlichkeit und mögliche Schäden vorgenommen. Dann werden Angriffe auf TCP/IP-Basis dargestellt und dazu die prinzipiellen Abwehrmöglichkeiten mit Firewall-Systemen aufgezeigt.

Elemente eines Firewall-Systems

Die grundsätzlichen Firewall-Elemente werden beschrieben: Wie können damit technische Sicherheitsmechanismen realisiert werden, welche konkreten Möglichkeiten bestehen, Sicherheit zu gewährleisten, wie ist die Architektur von Firewall-Systemen, wie wirken sie und wo liegen ihre Grenzen?

neuKap00.fm Seite 22 Freitag, 18. Oktober 2002 3:50 15

Konzepte für Firewall-Systeme

Die unterschiedlichen Konzepte über den Aufbau eines Firewall-Systems werden vorgestellt und diskutiert. Hier werden Hilfestellungen gegeben, welches Firewall-Konzept für welchen Einsatzfall verwendet werden kann.

Firewall-Systeme und Verschlüsselung

Mithilfe von Verschlüsselung kann in Verbindung mit Firewall-Systemen zusätzliche Sicherheit erreicht werden. Dadurch wird nicht nur eine kontrollierte, sondern auch eine vertrauliche Kommunikation erreicht. Die Konzepte für E-Mail-Sicherheit, SSL-Verschlüsselung und Virtual Private Networks werden dargestellt und verglichen.

Authentikationsverfahren

Das Kapitel beschreibt verschiedene Verfahren zur Authentikation von Benutzern, die über ein Firewall-System eine Kommunikation aufbauen wollen.

Verschiedene Firewall-Lösungen und ihre Bewertung

Die prinzipiellen Möglichkeiten zur Realisierung von Firewall-Lösungen werden vorgestellt. Insbesondere geht es in diesem Kapitel um die Gegenüberstellung von Public-Domain-Software-Lösungen, Software-Lösungen auf Standard-Betriebssystemen und Turn-Key-Lösungen. Weiterhin wird die Frage diskutiert, welche Randbedingungen erfüllt sein müssen, damit eine Firewall-Lösung wirklich sicher und vertrauenswürdig ist.

Praktischer Einsatz von Firewall-Systemen

Anhand von Beispielen wird gezeigt, wie mit verschiedenen Sicherheitskomponenten eine sichere und beherrschbare Ankopplung des eigenen zu schützenden Netzes an das Internet verwirklicht werden kann. Neben verschiedenen Anwendungsszenarien wird auch die Integration weiterer Sicherheitsmechanismen wie zentraler Virenscanner, Intrusion Detection System, Personal Firewalls und Security Gateway beschrieben.

Ein Firewall-System ist mehr als ein Produkt

In diesem Kapitel wird erläutert, welche Themen bei der Erarbeitung einer Firewall-Sicherheitspolitik berücksichtigt werden müssen und welche infrastrukturellen, organisatorischen und personellen Sicherheitsmaßnahmen das Firewall-System ergänzen müssen, damit ein hohes Maß an Gesamtsicherheit erreicht werden kann. Die Grenzen von Firewall-Systemen und zusätzliche Sicherheitsmaßnahmen werden aufgezeigt.

neuKap00.fm Seite 23 Freitag, 18. Oktober 2002 3:50 15

Besondere Aufgabenstellungen bei Firewall-Systemen

Die Network Address Translation stellt eine besondere Aufgabe der Firewall-Systeme dar. Die Verwaltung mehrerer Firewall-Systeme mithilfe eines Security Managements, geschachtelte Firewall-Konstellationen und die Ausfallsicherheit eines Firewall-Systems sind weitere Themen.

Weiterführende Aufgabenstellungen bei Firewall-Systemen

Mit dem Betrieb von Firewall-Systemen sind weiterführende Aufgabenstellungen verbunden: die Protokollierung der sicherheitsrelevanten Daten in Logbüchern, die Frage der Sicherheit von Java und ActiveX, die notwendigen Aufwendungen (Zeit und Kosten) für Beschaffung, Personal und Betrieb eines Firewall-Systems, die Evaluierung und Zertifizierung von Firewall-Lösungen, die Weiterentwicklung von Firewall-Systemen, Überprüfung von Firewall-Systemen im laufenden Betrieb (Security Audit), Intrusion-Detection/Response-Systeme, DDoS-Angriffe sowie Personal Firewall.

Theoretische Grundlagen von Firewall-Systemen

Das theoretische Modell der Kommunikation mit integriertem Firewall-System zeigt die Einflussfaktoren für die Wirkung von Sicherheit und Vertrauenswürdigkeit von Firewall-Systemen. Tabellen veranschaulichen die strukturellen Zusammenhänge über Angriffe und die Wirkung der verschiedensten Sicherheitsdienste/mechanismen/funktionen. Mit diesem Wissen können sichere Netzübergänge zu unsicheren Netzen vertrauenswürdig gestaltet werden: für IT- Sicherheit auf höchstem Niveau.

Recht im Internet

Die Rechtslage der Kommunikation im Internet und daraus resultierende Konsequenzen für die Benutzer werden erläutert.

Computerkriminalität – Fakten und Zahlen

Die Kriminalitätsstatistik des BKA, Schadensschätzungen und Fallbeispiele sollen zeigen, dass IT-Kriminalität eine reale Bedrohung ist.

Anhang

- Sicherheitsstandards zur TCP/IP-Technologie
- die BSI-Sicherheitsanforderungen an Internet-Firewalls
- eine Tabelle der auf dem deutschen Markt erhältlichen Firewall-Produkte
- wichtige Adressen
- ein Literaturverzeichnis
- die Legende für die Symbole, die im Buch verwendet werden
- ein Glossar mit Abkürzungen und
- das Stichwortverzeichnis

neuKap00.fm Seite 24 Freitag, 18. Oktober 2002 3:50 15

neuKap01.fm Seite 25 Freitag, 18. Oktober 2002 3:50 15

Kapitel 1

Einführung: Gesellschaftlicher Wandel und IT-Sicherheit

Dieses Buch beschäftigt sich mit Sicherheitslösungen, die vor Bedrohungen aus unsicheren Netzen, wie dem Internet, schützen. IT-Sicherheit ist dabei nicht allein eine technisch-organisatorische Aufgabe, sondern steht im gesellschaftspolitischen Zusammenhang. Deshalb beginnt dieses Kapitel mit einem kurzen historischen Rückblick.

1.1 Entwicklung von IT-Technologie und IT-Sicherheit

Schon immer hatte der technologische Fortschritt Einfluss auf alle Bereiche der Gesellschaft. Wasserleitungen machten einerseits Wasserträger brotlos, aber ermöglichten anderseits erst die Siedlungsform Großstadt. Der Traktor verdrängte das Pferd, die elektrische Schreibmaschine die mechanische und so fort. Die Agrargesellschaft wurde in Europa durch die Industriegesellschaft abgelöst, Triebfedern waren Kohle und Stahl, Dampfkraft und später Elektrizität.

Mit Energie, Maschinen, menschlicher Arbeitskraft und Intelligenz wurde immer mehr Materie formbar. Mit hoher Eigendynamik bildeten sich neue Lebensumgebungen; Mobilität für Güter und Menschen beschleunigte die Entwicklung, Handwerk und Wissenschaften organisierten sich.

Durch den Buchdruck wurde Wissen verteilbar, durch die Nachrichtentechnik körperlos übermittelbar und schließlich – nun »Information« genannt – durch die Informationstechnik prozessierbar.

Gegenwärtig erleben wir den *Wandel zur Informations- und Kommunikationsgesellschaft*. Die dazugehörenden Technologien sind die Schlüsseltechnologien für unsere Arbeits- und Lebenswelt von heute und morgen.

Meilensteine der Informationstechnik seit 1940:

- Im Zweiten Weltkrieg wurden die ersten Digital-Rechner entwickelt. Die Briten konnten mit einem Röhren-Rechner die als bis dato sicher geltende Verschlüsselung mechanischer Enigma-Apparate aus Deutschland brechen.
- Nach 1950 begann der Siegeszug des Transistors, er löste die langsame, anfällige, voluminöse und energiefressende Röhrentechnik ab. »Silicon, the new steel« lautete schließlich das Credo, als lochkartengespeiste Großrechneranla-

neuKap01.fm Seite 26 Freitag, 18. Oktober 2002 3:50 15

gen seinerzeit unglaubliche Datenmengen verarbeiteten. Als sich damals die Frage der Sicherheit stellte, wurde sie räumlich (Zugangsregelungen zum Rechenzentrum) und administrativ (Aufgabenteilung: Systemadministrator, Anwender, Daten-Eingabekraft) geregelt.

- In der zweiten Hälfte der 70er wurden an Großrechner Terminals angeschlossen, und der Siegeszug der Vernetzung begann. Bald gab es dezentrale Netze, wie SNA und Decnet nach dem ISO-Referenzmodell mit Ethernet-Topologie. Die IT-Sicherheit hatte endgültig ihre räumliche Abgeschlossenheit verloren.
- Der nächste Technologiesprung aus dem Silicon Valley brachte den (Home-)PC, mit eigenem Betriebssystem und schnellem Prozessorboard mit immer größeren Festplatten, Floppy-Disk- und später CD- und ZIP-Laufwerken zum Datenaustausch. Die Datenträger waren mobil, durch Miniaturisierung dann auch die Laptops und Palmtops.
  Die Frage der Sicherheit wurde zunächst viel zu einseitig auf den Bereich »Computerviren« ausgerichtet. Dabei gedieh im Verborgenen längst der Datenmissbrauch. In Deutschland wird seit 1987 der Bereich Computerkriminalität von der Polizei eigenständig erfasst.
- Immer preiswertere und leistungsfähigere PCs ermöglichten die Integration von Audio und Video. Inzwischen besitzt in den Industrienationen ein erheblicher Teil der Bevölkerung einen eigenen Multimedia-PC, oft mit zahlreichen Peripheriegeräten (Scanner, Drucker etc.).
- Firmen wie Privatleute rüsteten ihre PCs mit Modems aus, für den Zugang zu Mailboxen und später zu Online-Diensten über das Telefonnetz.
- Seit den 60er-Jahren wurden, ausgehend von den USA, militärische Netze und Firmennetze errichtet, z. B. das globale IBM-Netz. Die TCP/IP-Technologie wurde entwickelt, 1973 entstand das Internet, 1991 wurde es öffentlich und mit dem World Wide Web (WWW) startete das Online-Zeitalter.
- Heute sind Kommunikations- und Informationstechnik zusammengewachsen. Die kabelgebundenen Netze werden einerseits in ihrer Bandbreite erweitert, andererseits werden drahtlose Funkanbindungen mit hoher Bandbreite geschaffen. Bald ist die stationäre und mobile Netzanbindung von jedem Punkt der Erde aus möglich.

1.2 Siegeszug des Internet

In den letzten Jahren hat sich das Internet zum universalen, bidirektionalen und globalen Kommunikationsmedium etabliert. Das »Netz der Netze« ist unabhängig von den räumlichen und zeitlichen Begrenzungen, die den Informationsfluss über die klassischen Print- und Rundfunkmedien einengen.

neuKap01.fm Seite 27 Freitag, 18. Oktober 2002 3:50 15

Merkmale des Internets als das globale Datennetz:

- Einfacher und kostengünstiger Zugang
  Vom Notebook über PCs und Workstations bis zum Großrechner kann jeder Computer angeschlossen werden und zwar einfach und kostengünstig.

- Einheitlicher Standard
  Es gibt keine länderspezifischen Besonderheiten wie bei X.25-Netzen oder ISDN, denn die TCP/IP-Technologie ist netzunabhängig und für alle Betriebssysteme verfügbar.

- Weltweites Netz, shared infrastructure
  Hunderttausende Netzwerke verbinden über 100 Millionen angeschlossene Rechnersysteme in mehr als 240 Ländern. In praktisch allen Ländern der Welt kann man über das Telefonnetz Zugangsrechner von Onlinediensten wie AOL, CompuServe oder T-Online anwählen oder sich über Internet-Provider wie EUnet, MAZ, DFN direkt an das Internet anschließen.

- Steigende Akzeptanz
  Ende 2001 nutzten schätzungsweise 500 Millionen Menschen weltweit das Internet. Die Zuwachsrate ist weiterhin hoch, denn selbst in den Vereinigten Staaten haben lediglich knapp über 50 % der Haushalte einen Internet-Anschluss, in Deutschland sogar erst knapp über 25 %. Daraus kann man jedoch nicht ohne weiteres auf die Anzahl der Internetnutzer schließen, da eine erhebliche Zahl von Personen einen Internetzugang am Arbeits- oder Ausbildungsplatz hat und ferner die Nutzung eines Internet-Anschlusses durch mehrere Personen nur schwer abzuschätzen ist.

  Es ist zu erwarten, dass die Internetnutzung in diesem Jahrzehnt genauso alltäglich wird wie die Nutzung des Telefons und neuerdings des Mobiltelefons. Das Karlsruher Fraunhofer Institut für Systemtechnik und Innovationsforschung (ISI) berichtete im August 1998, dass nur 7 % der Internetnutzer in Deutschland aus der Arbeiterschicht kommen, was zeigt, dass starke gesellschaftliche Ungleichgewichte bestehen. Andererseits zeigt dies auch, dass das Potenzial hoch ist, denn in den nächsten Jahren werden sich die Unterschiede weiter angleichen. So berichtet die Gesellschaft für Konsumforschung (GfK) in Nürnberg, dass zwischen Ende 1997 und März 2001 der Anteil von Frauen unter den deutschen Internetnutzern von 29 % auf 42 % gestiegen ist.

- Extranet, Intranet
  Unternehmensweite *Intranets* können über das Internet zu einem *Extranet* verbunden werden. Das Extranet ist damit Teil des globalen Kommunikationssystems.

neuKap01.fm Seite 28 Freitag, 18. Oktober 2002 3:50 15

- Günstig für internationale Geschäftsbeziehungen
  Mitarbeiter eines Unternehmens, z. B. im Vertrieb, greifen von allen Ländern der Welt über das Internet auf die Rechnersysteme der Zentrale zu. Die Vorteile liegen auf der Hand: Preise, Lieferzeiten, neue Informationen können schnell abgerufen und Bestellungen sofort eingegeben und verarbeitet werden. Es gibt keinen Medienbruch, die Informationen müssen nur einmal eingegeben werden. Dies ermöglicht die effiziente Verarbeitung und rationelle Abwicklung immer komplexer werdender Aufgaben.

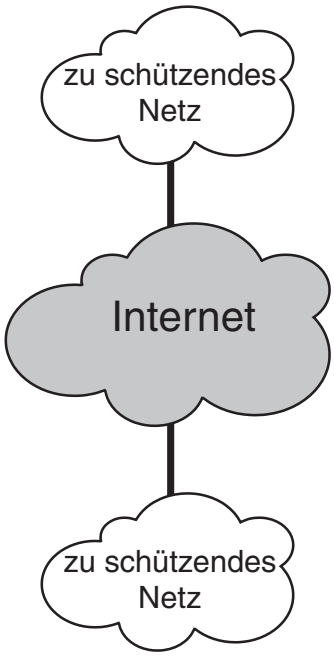


Abb. 1.1: Kommunikation über das Internet

Die elektronischen Dienste

Das Internet bietet eine Vielzahl von elektronischen Diensten, die im täglichen Umgang mit Rechnersystemen unverzichtbar werden:

Elektronische Post (E-Mail)

- Die Möglichkeiten sind gleichsam fabelhaft: Vom PC aus kann man allen Internet-Teilnehmern auf der ganzen Welt auf ganz einfache Weise elektronische Post senden. Der Empfänger hat die Mail in kürzester Zeit (ohne Postlaufzeiten) auf seinem Rechnersystem und kann sie weiterverarbeiten, ohne jeden Medienbruch. Die Textnachricht eines »elektronischen Briefs« kann um Anlagen (Dateien) mit beliebigem Dateiformat ergänzt werden.

neuKap01.fm Seite 29 Freitag, 18. Oktober 2002 3:50 15

- E-Mail ist die am häufigsten genutzte Anwendung im Internet und noch beliebter als das Surfen im multimedialen World Wide Web. Ende 2000 wurden weltweit über 10 Milliarden E-Mails pro Tag versendet.

Multimedia (World Wide Web)

- Die Möglichkeiten der kommerziellen Nutzung sind fast unbegrenzt.
- Die graphische Oberfläche ermöglicht eine hohe Benutzerfreundlichkeit.
- Das WWW bietet Firmen ein kostengünstiges Schaufenster für ihre Produkte und Dienstleistungen. Dabei können Kunden ihre Wünsche ganz einfach hinterlegen.
- Für Behörden gibt es keine einfachere, günstigere und umfassendere Möglichkeit, ihrer Informationspflicht nachzukommen.

Dateien-Transfer (FTP)

- Informationen jeder Art können einfach auf das eigene Rechnersystem kopiert werden. Hier können sie dann (ohne Medienbruch) weiterverarbeitet werden.
- Software-Häuser können schnell und unkompliziert neue Releases ihrer Produkte zur Verfügung stellen. Dies bedeutet eine hohe Kostenersparnis.

Weltweite Foren (News, Chat)

- Es gibt offline-Foren zu allen erdenklichen Themen, insgesamt zu mehreren zehntausend Fachgebieten. Ein solches Fachgebiet ist z. B. das Forum, in dem Entwickler von Software, die mit speziellen Werkzeugen arbeiten, Erfahrungen austauschen und Hilfestellung zu Problemen geben. In online-Foren (chatrooms) finden sich Gleichgesinnte zum »Schwätzchen« (chat).

Online-Ankopplung an Rechnersysteme (Telnet/Remote Login)

- Jeder kann von jedem Rechnersystem aus auf jedes andere Rechnersystem in der Welt zugreifen, als ob es das eigene wäre. Dadurch kann z. B. eine einfache Wartungsarbeit von Software-Häusern »remote« durchgeführt oder ein Hochleistungsrechner an einem ganz anderen Ort benutzt werden.

Internet als weltweite Informationsquelle

Wir leben in einer Informationsgesellschaft, in der die richtigen Informationen zum richtigen Zeitpunkt eine wichtige Rolle spielen, in vielen Bereichen sogar die Hauptrolle. Beispiele gibt es viele:

- *Organisationen* brauchen schnelle Informationen über Produkte und Dienstleistungen, damit sie ihre Aufgaben fristgerecht erfüllen können.
- *Banken* müssen Börsenbewegungen schnell erkennen und deuten, um entsprechend handeln zu können.
- *Pressemitarbeiter* benötigen oft hochaktuelle Hintergrundinformationen über Ereignisse des Tagesgeschehens.

neuKap01.fm Seite 30 Freitag, 18. Oktober 2002 3:50 15

- *Entwickler* brauchen konkrete Informationen von Software-Häusern, um ihre Entwicklung schneller fortführen zu können, z. B. Updates von fehlerhafter Software.
- *Kunden* können durch Online-Dienste nahezu vollständige Informationen über Angebot, Nachfrage und Preise erhalten, das bedeutet eine weltweite Marktübersicht über alle Produkte.

1.3 Gefahren aus dem Internet

Die Kommunikation über das Internet bietet Vorteile, auf die keine Organisation verzichten kann, die in der heutigen Zeit mithalten und zukünftige Entwicklungen nicht verpassen möchte.

Die unbestreitbaren Vorteile des Internets, die mit der Internet-Technologie auch Einzug ins Intranet gehalten haben, müssen aber häufig teuer bezahlt werden. Denn der Anschluss an ein öffentliches Netz ist keine Einbahnstraße, sondern öffnet eine Schleuse für potenzielle Eindringlinge.

Abbildung 1.2 zeigt einen direkten Anschluss an ein unsicheres Netz wie das Internet. Von jedem Rechnersystem des zu schützenden Netzes kann auf jedes Rechnersystem des unsicheren Netzes zugegriffen werden.

Umgekehrt gilt: Die Rechnersysteme des zu schützenden Netzes können von jedem Rechnersystem aus dem Internet angegriffen werden. In den Standardanwendungen des Internets sind keinerlei Sicherheitsmechanismen integriert, weshalb z. B. die Übermittlung sensitiver Daten via E-Mail äußerst problematisch ist.

Jedes einzelne Rechnersystem im Netz muss vor Angriffen aus dem Internet geschützt werden. In kleinen Organisationen sind vielleicht zehn, in großen Organisationen können über 10 000 Rechnersysteme von dieser Gefahr betroffen sein.

Wie sehen die Gefahren im Einzelnen aus, die den angeschlossenen oder miteinander vernetzten Rechnersystemen aus dem Internet drohen?

- High-Tech-Spione stehlen fremdes Know-how oder Strategiepläne und verkaufen sie lukrativ an die Konkurrenz.
- Hacker/Cracker brechen in das lokale Netz von Firmen und Behörden ein und fälschen Daten oder schleusen falsche Informationen ein.
- Cracker können die Rechnersysteme einer Organisation lahmlegen und so wirtschaftliche Schäden in Millionenhöhe verursachen.

Das Risiko eines Angriffs ist im Internet sehr hoch, denn das Internet kennt keine Hierarchie und keine Internet-Polizei. Jeder kann sich auf der so genannten Datenautobahn tummeln und nach Herzenslust »Datensurfing« betreiben.

neuKap01.fm Seite 31 Freitag, 18. Oktober 2002 3:50 15

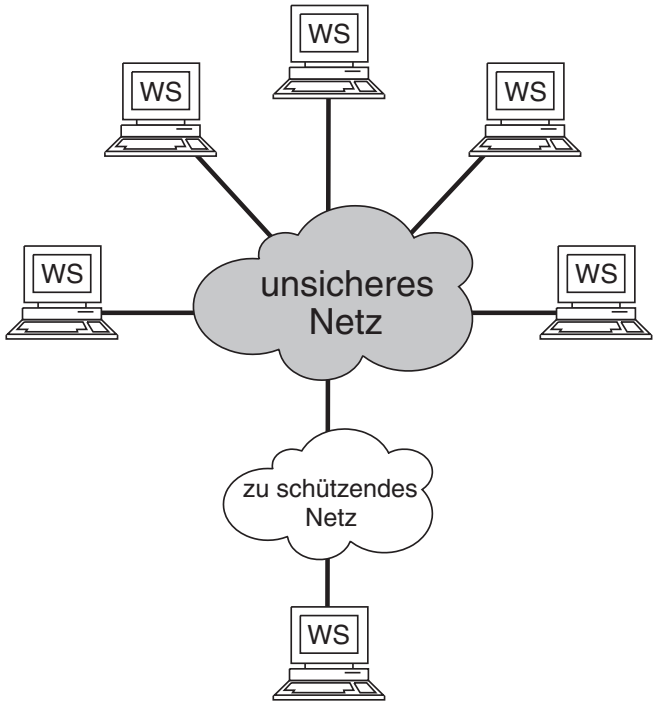


Abb. 1.2: Ein öffentliches Netz ist keine Einbahnstraße

Zurzeit fehlt den meisten Benutzern der Internet-Dienste das notwendige Sicherheitsbewusstsein. Wenn diese Dienste professionell eingesetzt werden sollen, dann müssen sie sicher und beherrschbar gemacht werden, damit ihr Nutzen berechenbar wird.

Allgemeine Bedrohungen aus dem Internet

In den letzten Jahren hat sich die Moral der Hacker gewandelt: Früher waren Hacker Tüftler, die aus Spaß an der Sache oder um ihr Können unter Beweis zu stellen in fremde Datenbanken einbrachen und sich einen Jux erlaubten, der dem Betroffenen allenfalls einen Schreck einjagte oder ihn ärgerlicherweise teure Arbeitszeit kostete.

Heute agieren Hacker professionell und organisiert als Cracker – was nicht weiter verwunderlich ist, wenn man bedenkt, wie viel Gewinn sich mit Daten und Informationen machen lässt, die in Netzen kursieren. Dabei haben die meisten Cracker kein Unrechtsbewusstsein und keine Moralvorstellung.

Obwohl viele Fälle von Computerkriminalität und Spionage bekannt geworden sind und die Schäden, die durch elektronische Einbrüche entstehen, in Milliardenbeträgen gerechnet werden – siehe dazu Kapitel 16 –, wurde das Thema Sicherheit

neuKap01.fm Seite 32 Freitag, 18. Oktober 2002 3:50 15

lange unterschätzt und sorglos übergangen. Die Schnelligkeit und die Informationsvorteile der Kommunikationsnetze werden genutzt, ohne dass man sich – bildlich gesprochen – um Sicherheitsgurt, Knautschzone und Airbag kümmert.

Der Missbrauch von Kommunikationsnetzen ist bereits heute ein großes Problem. Hinter mancher Hackergeschichte in der Presse verbirgt sich vielleicht eine Legende – das darf aber nicht darüber hinwegtäuschen, dass die Frage der Sicherheit vermutlich noch brisanter ist, als die bisher bekannt gewordenen Fälle von Einbrüchen und Missbrauch nahe legen.

Hacker und ihre Methoden werden immer erfindungsreicher, zumal die Beute, um die es geht, immer lohnender wird. Anders als bei einem Bankraub in der realen Welt ist das Risiko für Cracker nicht allzu groß, denn Cracker sind nur schwer zu verfolgen. Und sind die Diebe erst einmal im System, ist es fast unmöglich, sich an ihre Fersen zu heften.

1.4 Notwendigkeit von IT-Sicherheit

Wozu brauchen wir Sicherheit in der Informationstechnik?

Ein moderner Arbeitsplatzrechner hat heute die gleiche Leistungsfähigkeit wie ein klassisches Rechenzentrum vor einigen Jahren. Bei diesen Rechenzentren genügten noch Sicherheitsmaßnahmen, die mithilfe von organisatorischen und personellen Regelungen durchgeführt wurden. Dazu gehörten unter anderem

- Zugangskontrolle zu den Gebäuden und Räumen der Rechenzentren
- kontrollierte und definierte Arbeitsabläufe und entsprechende Auftragsabwicklung
- Trennung zwischen Personal der Fachabteilung (Anwendern) und DV-Mitarbeitern (Programmierern, Operateuren usw.)

Die EDV stand abgeschottet in einem Gebäude, wodurch die externen Bedrohungen überschaubar waren, und das Betriebssystem des Hostes war für den Schutz der Ressourcen vor unerlaubtem Zugriff zuständig.

Durch moderne informationstechnische Konzepte wie Client Server, Down-Sizing, Out-Sourcing, Internet, Intranet usw., in denen Informationen über ein angreifbares Netz ausgetauscht werden, sind besonders die Hard- und Software dieser Netze bedroht.

Außerdem sind die informationstechnischen Sicherungen von Arbeitsplatzrechnern, insbesondere von PCs, wesentlich schwächer als die klassischer Großrechner. Der Benutzer eines Arbeitsplatzrechners kann heute gleichzeitig Anwender, Operator oder Programmierer sein, was neue Probleme mit sich bringt.

neuKap01.fm Seite 33 Freitag, 18. Oktober 2002 3:50 15

Die heutigen verteilten Rechnersysteme lassen sich nicht mehr allein durch organisatorische Maßnahmen schützen. Es müssen zusätzliche *technische Sicherheitsmechanismen* bereitgestellt werden, die eine sichere und beherrschbare Informationsverarbeitung ermöglichen. Dazu sind strategische Sicherheitskonzepte notwendig, die *Vertraulichkeit, Integrität* und *Verfügbarkeit* von Rechnersystemen, Daten, Programmen und Personen als wesentliche Bestandteile von Organisationen aufbauen und erhalten. Außerdem müssen Verbindlichkeit und Zurechenbarkeit der Vorgänge und Veranlassungen – wo immer notwendig – garantiert werden.

Welche Rolle spielt IT-Sicherheit in der Informationsgesellschaft?

In den letzten Jahren hat sich der Wert der Informationen und damit der Schutzbedarf beträchtlich vergrößert.

Der steigende Wert von Informationen auf Rechnersystemen ist ein wichtiger, wenn nicht der wichtigste Wirtschaftsfaktor geworden. Beispiele sind:

- Vollständige Entwicklungs- und Fertigungsunterlagen: Manche Organisationen besitzen Hardware im Wert von 5 000 EUR, auf der Informationen im Millionenwert gespeichert sind.
- Geschäfts- und Betriebsergebnisse, Strategiepläne: Wenn solche Ergebnisse oder Pläne in der Öffentlichkeit bekannt werden, können damit z. B. Börsen-Aktivitäten in Bewegung gebracht werden, die wiederum einen hohen Schaden verursachen können.
- Logistikinformationen: Falls Rechnersysteme oder Daten nicht mehr verfügbar sein sollten, weiß kein Mitarbeiter mehr, wie groß das Lager ist, was produziert werden soll, welche Kunden was bestellt haben und wann an wen geliefert werden soll.
- Kundendaten stellen einen erheblichen Wert dar, den es zu schützen gilt.

Moderne Rechnersysteme ermöglichen eine effiziente Verarbeitung und rationelle Abwicklung von Aufgaben, die in vielen Bereichen anders kaum noch zu erfüllen sind. Wir sind in solchem Ausmaß von Rechnersystemen abhängig, dass unsere wirtschaftliche Leistungsfähigkeit gefährdet ist, wenn die Funktionsfähigkeit der Rechnersysteme nicht in angemessener Weise gewährleistet werden kann.

Globale Ausdehnung und Veränderung der Geschäftsprozesse

Die meisten Geschäftsprozesse wurden in der Vergangenheit auf dem Papier (z. B. Angebotserstellung, Auftragsannahme, Bestellungen, Liefereingang) oder persönlich (z. B. bei Kundenbesuchen) abgewickelt. Diese Abläufe können weitaus rationeller gestaltet werden, indem der personelle und materielle Aufwand durch elektronische Verfahren ersetzt wird. Alle oben aufgezählten Geschäftsprozesse können per Rechnersystem erstellt und elektronisch übertragen werden, sodass kein Medienbruch mehr auftritt.

neuKap01.fm Seite 34 Freitag, 18. Oktober 2002 3:50 15

Unsere Rechnersysteme, und insbesondere der Zugriff von außen auf unsere Rechnersysteme, werden für potenzielle Angreifer dadurch immer attraktiver. Gleichzeitig kommt keine Behörde, keine Bank und auch keine Firma heute mehr ohne die Verlagerung von Geschäftsprozessen und die Vernetzung von Rechnersystemen aus.

Einerseits möchte man eine leicht handhabbare und immer verfügbare Verbindung nach außen haben. Andererseits müssen geschäftsinterne Daten und Beziehungen zu Geschäftspartnern vor Diebstahl und mutwilliger Zerstörung geschützt werden.

In Kaufhäusern sind Wachpersonal und Detektive, Videoüberwachung und stählerne Rolläden selbstverständlich. Aber erst in jüngster Zeit machen sich Organisationen Gedanken darüber, dass auch Daten vor unbefugtem Zugriff geschützt werden sollten – weil sie einen erheblichen Wert darstellen, oft sogar den Hauptanteil des Vermögens einer Organisation.

Die Informationstechnologie hat Möglichkeiten geschaffen, Wirtschaftsspionage bequem mit Rechnersystemen zu betreiben. Für diese neue Form der Spionage, bei der keine Wände eingerissen oder Tresore geknackt werden müssen, fehlt häufig jegliches Unrechtsbewusstsein der Täter, die ihre Arbeit vom Wohnzimmer aus erledigen. Die Tools für solche Aktivitäten sind auf dem Software-Markt bzw. im Internet frei erhältlich, zu den Tricks gibt es ausführliche Informationen in der Literatur und im Web.

Experten schätzen die wirtschaftlichen Schäden, die durch Computerkriminalität entstehen, bereits heute auf Milliardenbeträge – mit steigender Tendenz.

Staatliche Industrie- und Wirtschaftsspionage

IT-Kriminalität wächst mit dem Kommunikationsmöglichkeiten: Wirtschaftsspionage ist ein Hauptproblem im heutigen Business und hat seit Beendigung des Kalten Kriegs die militärische Spionage abgelöst. Dabei werden die wesentlichen Gefahren nicht mehr geographisch-politisch geortet (west-östliche Länder), sondern nach der Konkurrenzfähigkeit der Länder eingeschätzt.

US-Präsident Bill Clinton erklärte »ökonomische Aufklärung« zum Staatsziel und stattete den »Supergeheimdienst« National Security Agency (NSA) mit entsprechenden Mitteln aus.

Die USA unterhalten mit einigen befreundeten Staaten das globale Echelon-System, um Kommunikation (Telefon, Fax, DFÜ, Internet, ...) abzuhören und automatisiert auszuwerten. Bürgerrechtler verfolgen dies mit Sorge, ein Zitat von `www.echelonwatch.org`:

neuKap01.fm Seite 35 Freitag, 18. Oktober 2002 3:50 15

»Echelon is perhaps the most powerful intelligence gathering organization in the world. Reports suggest that this network is being used to spy on private citizens everywhere, including on the Internet.«

Aufschlussreich ist auch der STOA-Report des Europäischen Parlaments »An Appraisal of the Technologies to Political Control«, Download und aktuelle Ergänzungen unter: `www.europarl.eu.int/dg4/stoa/en` oder `http://cryptome.org/stoa-atpc.htm`

Schließlich meldete die Berliner-TAZ am 10. Januar 2000 unter der Schlagzeile:

»Präsident Clinton legt Zwei-Milliarden-Dollar-Programm auf: Gegen Internet-Terroristen und für die Ausbildung des Spionage-Nachwuchses«

in dem Drei-Jahres-Plan seien – so die TAZ – allein 150 Millionen Dollar »Stipendien« enthalten, um Wissenschaftler und Studenten in IT-Sicherheitsfragen auszubilden.

1.5 IT-Sicherheit als Wirkungs- und Handlungszusammenhang

IT-Sicherheit beschäftigt sich mit dem Schutz von Werten gegen Angriffe, wobei Angreifer das Ziel haben, die Werte für eigene Zwecke zu nutzen oder den Eigentümer zu schädigen /Comm98/:

Die Sicherung der Werte (assets) liegt in der Verantwortung des Eigentümers (Owner) der Werte. Die Angreifer (Threat agents) wollen mit einem Angriff (threats) auf die Werte auch deren Vorteile ausnutzen und handeln somit gegen den Eigentümer der Werte. Der Eigentümer nimmt den Angriff als Reduzierung seiner Werte wahr – sofern er ihn bemerkt.

Spezielle Angreifer (z.B. Geheimdienste) sind in der Lage, die Hersteller von Gegenmaßnahmen zu beeinflussen, damit diese Möglichkeiten einbauen, die es diesem Angreifer erlauben, trotz der Gegenmaßnahmen auf die Werte zuzugreifen. Für den Eigentümer bedeutet dies wiederum eine Reduzierung seiner Werte und ist als »trügerische Sicherheit« in Wirklichkeit eine Scheinreduzierung seines Risikos.

Die Angriffe auf IT-Werte beziehen sich in der Regel – aber nicht ausschließlich – auf:

- **Verlust der Vertraulichkeit:**
  Angreifer kommen unberechtigt in den Besitz der Werte (Informationen).
- **Verlust der Integrität:**
  Angreifer sind in der Lage, unautorisiert Werte (Informationen) zu manipulieren.

neuKap01.fm Seite 36 Freitag, 18. Oktober 2002 3:50 15

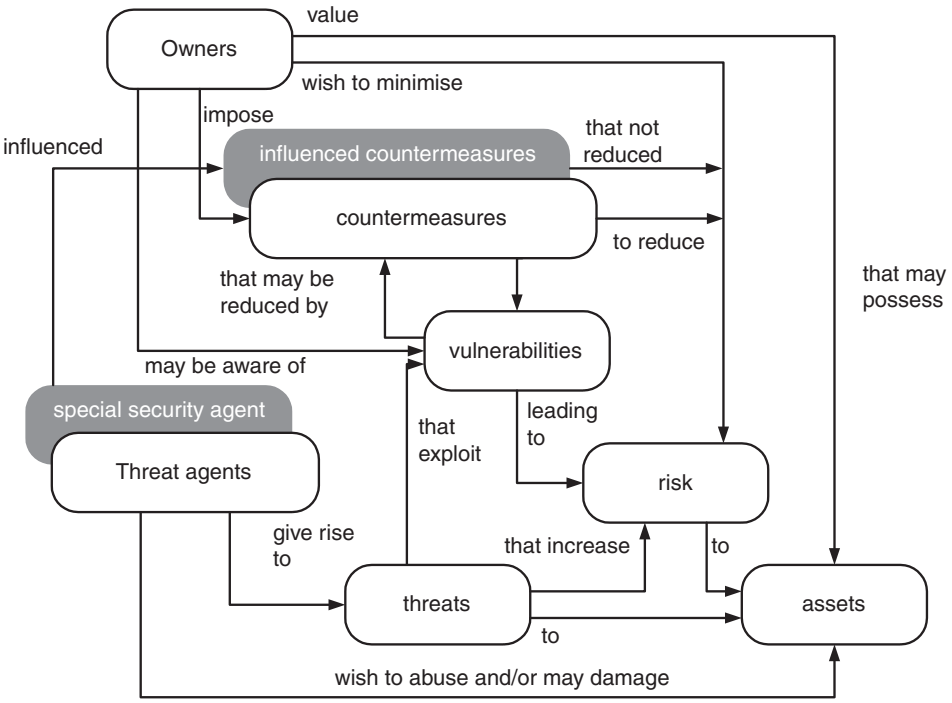


Abb. 1.3: IT-Sicherheit als Wirkungs- und Handlungszusammenhang

- **Verlust der Verfügbarkeit:**
  Angreifer enthalten dem Eigentümer den berechtigten Zugriff auf Werte (Informationen, Betriebsmittel) vor.
- **Verlust der Verbindlichkeit:**
  Die Verbindlichkeit der Transaktion ist nicht gewährleistet. Das Senden und Empfangen von Werten/Information kann geleugnet werden.
- **Verlust der Authentizität:**
  Die Echtheit des Kommunikationspartners wird gefälscht, der Ursprung der Information (Daten) ist nicht gesichert.

1.6 Chancen und Risiken – zwei Extreme der Ungewissheit

Ein Ereignis ist dann ungewiss, wenn es weder völlig ausgeschlossen werden kann, noch sein Eintreten völlig sicher ist. Die Wahrscheinlichkeit eines solchen Ereignisses ist größer 0 und kleiner 1.

Risiko ist dadurch charakterisiert, dass ein Ereignis auch einen negativen Ausgang haben kann. Die Möglichkeit eines erwünschten bzw. erhofften Ausgangs eines bevorstehenden Ereignisses dagegen ist die Chance (Profit/Marktanteile).

neuKap01.fm Seite 37 Freitag, 18. Oktober 2002 3:50 15

Der Eigentümer der Werte muss eine Analyse durchführen, welche Angriffe für ihn relevant sind, und welche er vernachlässigen kann. Diese Analyse der Angriffe hilft ihm, geeignete Gegenmaßnahmen auszuwählen, die sein Risiko der Verwundbarkeit auf ein akzeptables Maß reduzieren. Die Verwundbarkeit und damit der eigene Schutzbedarf ist in der Regel für verschiedene Anwendungen sehr unterschiedlich.

Die eingeführten Gegenmaßnahmen reduzieren die Verwundbarkeit und müssen mit der jeweiligen Sicherheitspolitik des Eigentümers übereinstimmen.

Auch nach der Einführung der Gegenmaßnahmen bleibt eine Rest-Verwundbarkeit bestehen, die mit anderen Maßnahmen weiter eingeschränkt werden kann.

Die folgende Graphik symbolisiert den durch »best practice« maximierten Geschäftserfolg:

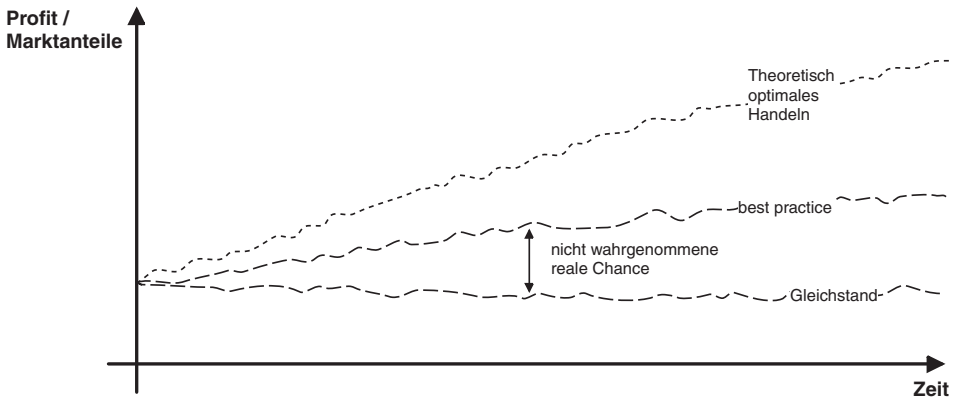


Abb. 1.4: Chancenoptimiertes geschäftliches Handeln

Es besteht weitgehend Einigkeit darüber, dass zum einen die Ungewissheit über das Kommende und zum anderen die negative Valenz des möglichen Ereignisausgangs die zentralen Bestimmungsstücke des Risikos darstellen. Damit ist Risiko immer Chance und Gefahr zugleich: Chance, ein angestrebtes Ziel zu erreichen, z. B. die Vorteile des Internets zu nutzen, d. h. etwas zu gewinnen (Profit, Marktanteile, ...) und Gefahr, dass man etwas Existierendes (Werte) durch das eigene Handeln – z. B. durch Nutzung des Internets – zur Disposition stellt, und dadurch Informationswerte beeinträchtigt werden oder man diese verliert.

Unternehmen und Organisationen sollten die Chancen nutzen, die die Informationstechnik eröffnet – z. B. durch Nutzung des Internets – aber durch die richtige Investition in die geeigneten Gegenmaßnahmen (Firewall-Systeme, VPNs, Intrusion-Detection-Systeme, Anti-Virus-Systeme ...) dafür sorgen, dass das Risiko einer Verwundbarkeit reduziert wird. Hierdurch ist verantwortungsvolles Handeln

neuKap01.fm Seite 38 Freitag, 18. Oktober 2002 3:50 15

möglich und Leistungsfähigkeit bzw. Profit und Marktanteile werden gesteigert: zur betriebswirtschaftlichen und schließlich in summa auch zur volkswirtschaftlichen Blüte.

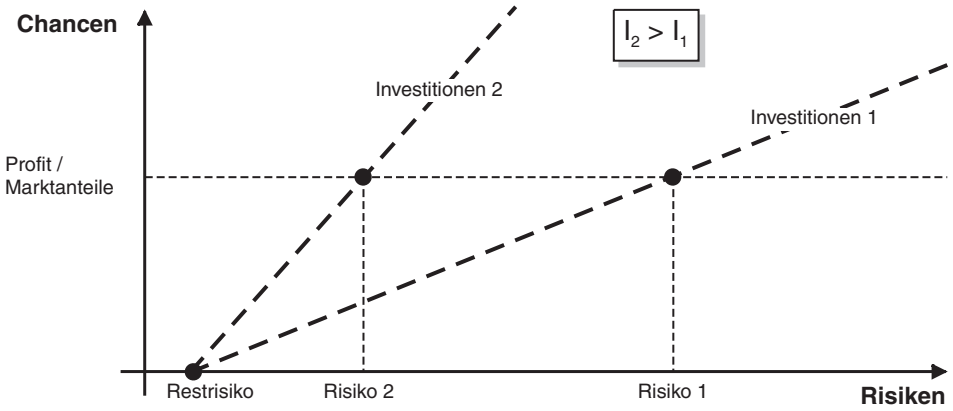


Abb. 1.5: Angemessene Investionen

Zu diesem Thema möchte ich ergänzend auf zwei Bücher von Tim Cole hinweisen: »Erfolgsfaktor Internet – Warum kein Unternehmen ohne Vernetzung überleben wird«, /Cole99a/ sowie: »Managementaufgabe Sicherheit«, /Cole99b/.

1.7 Der Firewall-Markt

In diesem Kapitel werden einige Informationen über den Firewall-Markt dargestellt.

Im Rahmen von E-Commerce, E-Business und Remote-Access-Projekten ist die Ausdehnung der Unternehmensnetze gegenwärtig ein zentraler Aspekt in der IT-Welt. Daran wird sich auch in den kommenden Jahren wenig ändern.

Firewall-Marktzahlen nach einer Studie von Datamonitor

Millionen $	2000	2001	2002	2003	2004	2005	CAGR
US	648	881	1.145	1.442	1.789	2.146	27%
Europa	344	467	654	890	1.153	1.445	33%
Asien	59	82	117	171	241	327	41%
Rest	50	70	101	149	208	279	41%
Gesamt	**1.100**	**1.500**	**2.017**	**2.651**	**3.390**	**4.198**	**31%**

Tabelle 1.1: Firewall-Markt 2000-2005
(aus: Global network security markets to 2005, Datamonitor, 12/2000)

neuKap01.fm Seite 39 Freitag, 18. Oktober 2002 3:50 15

Während der Markt für Software-basierte Firewall-Systeme vor allem in Amerika, aber auch in Europa langsam gesättigt scheint, wächst der Markt für Firewall-Applikationen überproportional. Gerade für die kleinen Unternehmen, die mit immer größerer Kraft ins E-Business vorstoßen, sind Firewall-Systeme die ideale Lösung, um eine »Verteidigungslinie« aufzubauen. Zusammen mit den technisch immer besser ausgestatteten Filialen/Geschäftsstellen sorgen sie für einen starken Wachstumsmarkt.

Ein neuer Markt für Personal Firewalls hat sich durch den Zuwachs an kleinen Büros und Heimarbeitsplätzen aufgetan.

Firewall-Marktzahlen nach einer Studie von Frost & Sullivan 1999

Milliarden $	2000	2001	2002	2003	2004	2005
Growth Rate	78,9	71,4	69,6	69,4	68,2	66,7
Europa	**0,36**	**0,61**	**1,04**	**1,75**	**2,95**	**4,92**

Tabelle 1.2: Software-Firewall-Markt 2000-2005
(aus: European Security Software Markets, Frost & Sullivan, 1999)

Der Markt für Software-Firewalls entwickelt sich weiterhin positiv, auch wenn die Wachstumsraten in den kommenden Jahren zurückgehen werden. Bis zum Jahr 2005 wird auf dem europäischen Markt mit einem Anstieg auf 4,92 Milliarden US$ gerechnet.

Treibende Faktoren für den Firewall-Markt

Ständiges Wachstum des **E-Commerce** setzt Unternehmen, die noch nicht im Web vertreten sind, unter Zugzwang. Unternehmen, die bereits eine Webpräsenz haben, müssen sich Gedanken über die Sicherheit ihrer Transaktionen machen. Dieser Trend wird auch in den kommenden Jahren konstant stark bleiben.

Die **wirklichen und wahrgenommenen Risiken im Internet** werden durch Berichte in der Fachpresse und der allgemeinen Presse in die Öffentlichkeit getragen und den Unternehmen bewusst gemacht. Die Diskussion über Cyberterrorismus und Wirtschaftsspionage per Internet spielt hier eine besondere Rolle. Die Angst vor einem möglichen Angriff von außen trägt wesentlich zum Wachstum des Firewall-Marktes bei.

Geringere Transaktionskosten beim Transfer von digitalen Daten und Informationen machen das Internet im Vergleich zu anderen Übermittlungswegen interessant. Zusätzlich ermöglichen sinkende Providerkosten und Preise für Server-Software und auch Firewall-Systeme einen schnellen und günstigen Eintritt in das Internet.

neuKap01.fm Seite 40 Freitag, 18. Oktober 2002 3:50 15

Ein weiterer Faktor ist die zahlenmäßige Zunahme der **Intranets**. Intranets werden zum Standard bei Unternehmensnetzwerken. Das Wachstum des Firewall-Marktes ist an den Anstieg der internen Verwendung von IP-Netzwerken (Intranet) gekoppelt.

Hemmende Faktoren für den Firewall-Markt

Auch wenn die Gefahren vor Hackerangriffen mittlerweile bekannt sind, ist nicht mehr von der Hand zu weisen, dass die größeren Gefahren oft von innen, d.h. von den eigenen Mitarbeitern, ausgehen. Gegen diese Angriffe sind zentrale Firewall-Systeme aufgrund ihrer Architektur kein geeigneter Schutz (siehe Kap. 13.9, »Personal Firewall«).

Vor allem kleinere und mittelständische Unternehmen investieren lieber in eine günstigere Router-Lösung als in ein sicheres Firewall-System. Diese Router basieren jedoch zumeist auf einer einfachen Packet-Filter-Funktion und bieten somit nicht die Netzwerksicherheit von Stateful-Inspection- oder Application-Gateway-Lösungen. Es liegt in der Verantwortung der Manager von Organisationen, sich im Rahmen eines Risko-Managements mit geeigneten Firewall-Lösungen angemessen zu schützen.

Trends

Firewall-Systeme werden zunehmend mit weiteren Sicherheitslösungen wie Intrusion-Detection-Systemen, Virtual Private Networks und zentralen Viren-Scannern kombiniert. Außerdem werden Firewall-Systeme zunehmend als technische Lösung zum Risiko-Management betrachtet.

Die Integration von Firewall-Systemen in übergreifende Sicherheits- und Netzwerkmanagement-Systeme ist für viele Organisationen von hoher Bedeutung, um das Management bewältigen zu können.

1.8 Fazit

Die internationale wirtschaftliche Ausdehnung vieler Organisationen – man denke z.B. an die Mega-Fusion von Daimler-Benz und Chrysler oder die im Januar 2000 beschlossene größte Fusion der bisherigen Wirtschaftsgeschichte zwischen AOL und Time Warner – braucht vernetzte IT-Strukturen und eine Kommunikationsplattform wie das Internet. Das Internet dringt in viele öffentliche und private Lebensbereiche vor und eröffnet gleichzeitig neue rechtliche, soziale und ethische Probleme, denen wir uns stellen müssen. Politische und juristische Instrumente stehen noch nicht zur Verfügung, um einem Missbrauch wirksam begegnen zu können.

neuKap01.fm Seite 41 Freitag, 18. Oktober 2002 3:50 15

Informationstechnologie kann nur sinnvoll eingesetzt werden, wenn sie sicher und beherrschbar ist. Die Bedrohungen, die aus der neuen Technik resultieren, können wir nicht beeinflussen, aber unsere Verletzbarkeit.

Dafür ist jedoch Voraussetzung, dass für bewährte klassische Sicherheitsmechanismen, wie Pförtner, Brandschutzmauer, handgeschriebene Unterschrift und Briefumschlag, elektronische Äquivalente eingesetzt werden.

neuKap01.fm Seite 42 Freitag, 18. Oktober 2002 3:50 15

neuKap02.fm Seite 43 Freitag, 18. Oktober 2002 3:50 15

Kapitel 2

Ziele von Firewall-Systemen

In diesem Kapitel werden die allgemeinen Ziele eines Firewall-Systems anhand von Analogien dargestellt. Die Idee, die hinter dem Betrieb eines Firewall-Systems steht, und das Konzept des »Common Point of Trust« werden erläutert.

2.1 Analogien zu Firewall-Systemen

Ein Firewall-System ist gleichzeitig »elektronischer Pförtner« und »elektronische Brandschutzmauer« und sichert und kontrolliert den Übergang von einem zu schützenden Netz zu einem unsicheren öffentlichen Netz. Dabei muss ein Firewall-System analog zu herkömmlichen Sicherheitseinrichtungen für physikalische Objekte (Gebäude) zwei Aspekte erfüllen:

- Brandschutzmauer
  Als Erstes ist ein elektronisches Firewall-System wie eine Brandschutzmauer dafür zuständig, einen bestimmten Bereich abzuschotten, damit Schäden, die auf der einen Seite der Mauer auftreten, nicht auf die andere Seite übergreifen.

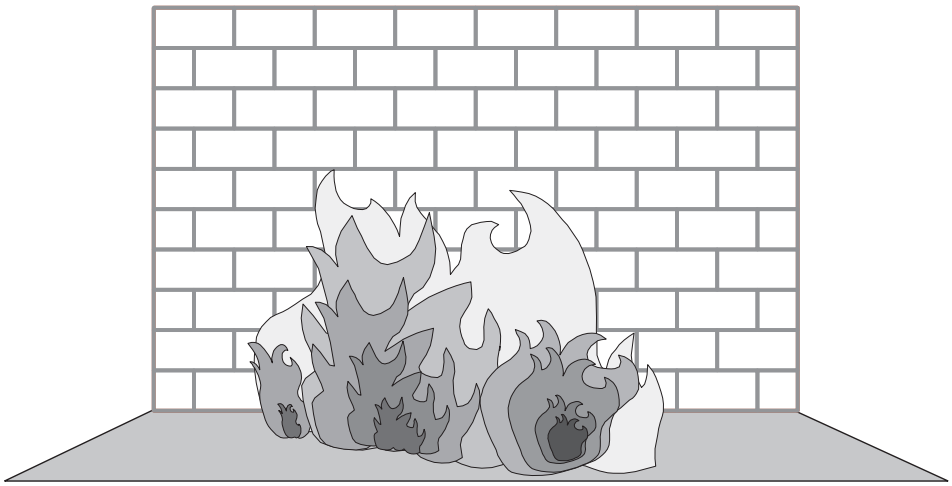


Abb. 2.1: Brandschutzmauer

neuKap02.fm Seite 44 Freitag, 18. Oktober 2002 3:50 15

Entsprechend wird das Gebäude einer Organisation in bestimmte Abschnitte unterteilt, damit ein Feuer, das in einem Abschnitt ausbricht, nicht auf die anderen Teile der Organisation übergreifen kann.

Auf Kommunikationsnetze bezogen bedeutet dies, dass das Firewall-System das zu schützende Netz gegen Gefahren aus dem unsicheren Netz abschottet. Es wird nur ein einziger besonders sicherer Übergang (bewachte Tür durch einen Pförtner) zwischen den beiden Teilnetzen realisiert.

- Pförtner
  Ein Firewall-System hat außerdem analog zu einem Pförtner in einem Gebäude die Aufgabe, den Zugang zum Gebäude einer Organisation zu kontrollieren, indem Personen, die in das Gebäude der Organisation hinein wollen, sich identifizieren und authentisieren müssen. Als Mitarbeiter identifizierte Personen werden nach ihrer Überprüfung hineingelassen. Besucher werden als Besucher registriert, und eine Verbindung zwischen Besuchern und zu besuchenden Angehörigen der Organisation wird hergestellt.

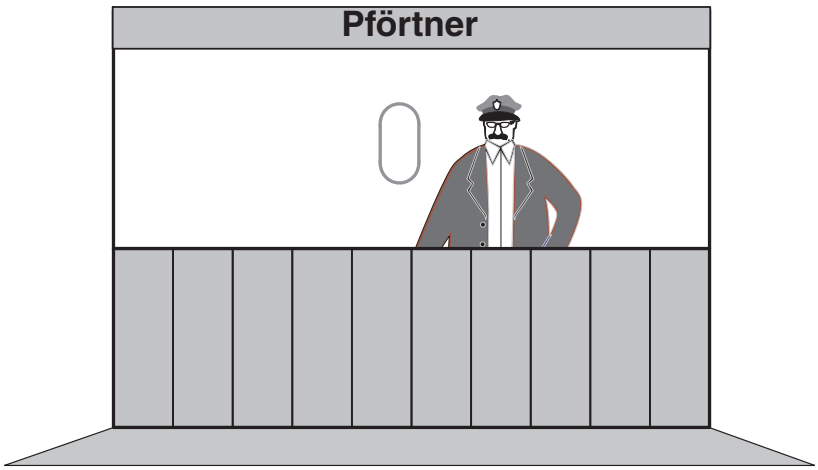


Abb. 2.2: Pförtner

Außerdem wird kontrolliert, welche Gegenstände Mitarbeiter und Besucher mit in das Gebäude der Organisation nehmen, und vor allem, welche sie aus dem Gebäude der Organisation herausnehmen dürfen.

Zusätzlich werden beim Pförtner alle Ereignisse protokolliert, z. B. wann welcher Besucher gekommen und gegangen ist und wen er besucht hat.

Eventuell auftretende Unregelmäßigkeiten können mit diesen Informationen im Nachhinein aufgedeckt werden.

neuKap02.fm Seite 45 Freitag, 18. Oktober 2002 3:50 15

Das elektronische Äquivalent zum Pförtner ist ein Firewall-System, das überprüft, wer aus dem unsicheren Netz auf das zu schützende Netz der Organisation zugreifen darf, und hier kontrolliert, über welche Protokolle und Dienste zugegriffen wird und mit welchen Rechnersystemen kommuniziert werden darf.

In diesem Sinne ist ein Firewall-System gleichzeitig eine elektronische Brandschutzmauer und ein elektronischer Pförtner. Je nach Anforderung des Nutzers stellt das Firewall-System die Sicherheitsmechanismen zur Verfügung, die gebraucht werden, um ein Netz einer Organisation gegen Angriffe aus einem unsicheren Netz zu schützen, und somit Risiken und damit die Verwundbarkeit einer Organisation zu minimieren. Zum sicheren Betrieb eines Firewall-Systems gehören technische, personelle, organisatorische und infrastrukturelle Sicherheitsmechanismen.

Sicherheitsmechanismen sind erforderlich geworden, weil sich die Geschäftsprozesse in unserer Informationsgesellschaft verändert haben. Für die Sicherheit und Beherrschbarkeit der Geschäftsprozesse, die über Kommunikationsnetze abgewickelt werden, müssen Firewall-Systeme integriert werden. Dabei ist ein Firewall-System mehr als ein Produkt, denn mithilfe eines Firewall-Systems ist die Umsetzung einer Sicherheitspolitik in einer Organisation möglich.

Voraussetzung: Sicherheitskonzept

Ähnlich wie für den Pförtner und die Brandschutzmauer gilt auch für den Einsatz eines Firewall-Systems: Nicht das Firewall-System macht sicher, sondern mit einem Firewall-System kann man etwas sicher machen, wenn es richtig betrieben wird.

Das bedeutet, dass Firmen, die ihre Netze schützen wollen, vorher genau wissen sollten, wer oder was wovor geschützt werden und was erlaubt bzw. verboten werden soll. Grundsätzlich ist vor dem Einsatz eines Firewall-Systems eine Sicherheitspolitik zu entwickeln und umzusetzen. Erst wenn die grundlegenden Anforderungen feststehen, kann überprüft werden, wie mithilfe eines Firewall-Systems diese Anforderungen realisiert werden können.

Auch beim Einsatz eines Firewall-Systems muss vorher definiert werden, über welche Protokolle und Hilfsmittel ein Zugriff auf das Netz einer Organisation erlaubt sein soll, so wie ein Pförtner nur bestimmte Besuchertypen ins Gebäude lässt, z. B. solche, die zu Fuß kommen und eventuell noch eine Aktentasche mitbringen, aber nicht solche, die mit dem Auto, Fahrrad oder Roller ins Gebäude der Organisation hineinfahren wollen (siehe Kapitel 11 *Ein Firewall-System ist mehr als ein Produkt*).

Die Reduzierung der Zugriffe, die erlaubt sein sollen, erhöht die Sicherheit und erleichtert die Kontrolle und die Administration eines Firewall-Systems.

Wenn auf der organisatorischen, infrastrukturellen und personellen Ebene entsprechende Sicherheitsmaßnahmen ergriffen werden, bleibt der administrative

neuKap02.fm Seite 46 Freitag, 18. Oktober 2002 3:50 15

Aufwand für den Betrieb des Firewall-Systems überschaubar, und die Fehlerwahrscheinlichkeit wird stark reduziert. Ein überschaubares Sicherheitsmanagement gewährleistet die übersichtliche Anordnung der notwendigen Sicherheitsdienste.

Ein Firewall-System muss in ein individuelles Sicherheitskonzept eingebettet werden. Wird es davon losgelöst installiert, hat es vielleicht eine Alibi-Funktion, kann aber keine Sicherheitsfunktionen garantieren.

2.2 Zielsetzung eines Firewall-Systems

Ein Firewall-System wird als Schranke zwischen das zu schützende Netz und das unsichere Netz geschaltet, sodass der gesamte Datenverkehr zwischen den beiden Netzen nur über das Firewall-System möglich ist. Auf dem Firewall-System werden Sicherheitsmechanismen implementiert, die diesen Übergang sicher und beherrschbar machen. Dazu analysiert das Firewall-System die Kommunikationsdaten, kontrolliert die Kommunikationsbeziehungen und Kommunikationspartner, reglementiert die Kommunikation nach einer Sicherheitspolitik, protokolliert sicherheitsrelevante Ereignisse und alarmiert bei starken Verstößen den Security-Administrator.

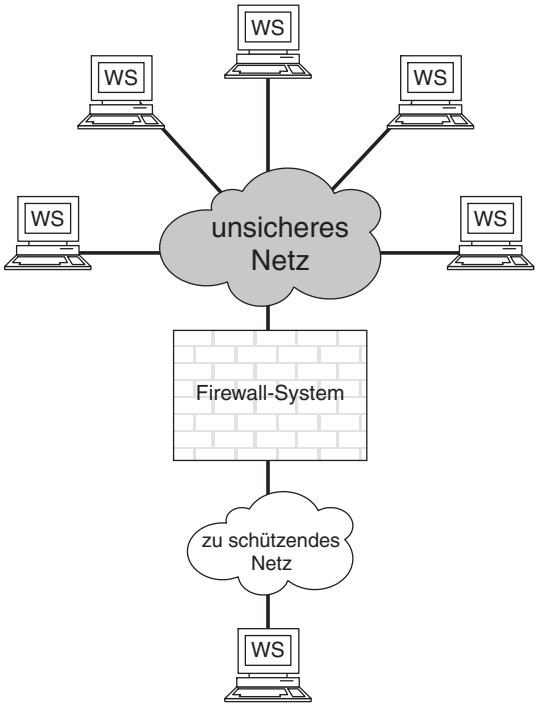


Abb. 2.3: Firewall-System

neuKap02.fm Seite 47 Freitag, 18. Oktober 2002 3:50 15

Ein Firewall-System stellt den »Common Point of Trust« für den Übergang zwischen unterschiedlichen Netzen dar, d.h., der einzige Weg ins interne Netz führt kontrolliert über das Firewall-System.

Firewall-Systeme werden verwendet, um sich an unsichere Netze wie z.B. das Internet anzukoppeln. Firewall-Systeme werden aber auch eingesetzt, um das eigene Netz zu strukturieren und hier Sicherheitsdomänen mit unterschiedlichem Schutzbedarf zu schaffen.

Vorteile des »Common Point of Trust«-Konzeptes

- Kosten:
  Die Realisierung von Sicherheitsmechanismen in einem zentralen Firewall-System ist wesentlich effizienter als die Realisierung von Sicherheitsmechanismen auf jedem einzelnen Rechnersystem, das im zu schützenden Netz steht.
- Umsetzung der Sicherheitspolitik:
  Mithilfe eines zentralen Firewall-Systems kann die Sicherheitspolitik einer Organisation auf einfache Weise zentral durchgesetzt werden. Zum Beispiel werden die Dienste und Protokolle, die über ein Firewall-System möglich sein sollen, an einer zentralen Stelle für alle Benutzer definiert und überprüft.
- Möglichkeiten:
  Eine kryptographische (starke) Authentikation von Benutzern ist nur auf einem Firewall-System zu realisieren und nicht auf jedem einzelnen Rechnersystem im zu schützenden Netz, damit die Benutzer sicher identifiziert und authentisiert werden können. Für heterogene Rechnerlandschaften gibt es zurzeit keine Konzepte und Realisierungen, wie kryptographische Authentikation auf den unterschiedlichen Rechnerbetriebssystemen (VMS, UNIX, Windows, OS/2, Mac OS, ...) praktisch realisiert werden kann. Hier können Kosten eingespart werden.
- Sicherheit durch Abschottung:
  Durch die reduzierte Funktionalität, die ein Firewall-System anbietet, existieren weniger Angriffspunkte für Angreifer aus dem unsicheren Netz. Der Aufwand für Sicherheitsmechanismen konzentriert sich auf das Firewall-System. Dadurch wird erreicht, dass die Rechnersysteme des zu schützenden Netzes nicht mehr von einem Rechnersystem aus dem unsicheren Netz (z.B. Internet) angegriffen werden können, sondern Rechnersysteme von außerhalb durch das Firewall-System abgeblockt werden. Rechnersysteme können nicht mehr zum Ziel von Angreifern aus dem unsicheren Netz werden, wenn sie falsch installiert oder konfiguriert sind. Alle Sicherheitsmechanismen sind in dem Firewall-System konzentriert realisiert.

neuKap02.fm Seite 48 Freitag, 18. Oktober 2002 3:50 15

- Überprüfbarkeit:
  Durch den klaren Übergang (Common Point of Trust) zwischen zwei Netzen ist eine einfache und vollständige Protokolliermöglichkeit vorhanden, da die gesamte Kommunikation über das Firewall-System läuft.

Allgemeine Ziele von Firewall-Systemen

Allgemeine Ziele eines Firewall-Systems werden im Folgenden benannt und definiert:

- Zugangskontrolle auf der Netzwerkebene
  Es wird überprüft, welche Rechnersysteme über das Firewall-System miteinander kommunizieren dürfen.
- Zugangskontrolle auf Benutzerebene
  Das Firewall-System überprüft, welche Benutzer über das Firewall-System eine Kommunikation aufbauen dürfen. Dazu wird die Echtheit (Authentizität) des Benutzers festgestellt.
- Zugangskontrolle auf Datenebene
  Das Firewall-System überprüft, welche Daten eines definierten Benutzers über das Firewall-System übertragen werden dürfen. Dazu wird die Echtheit der Daten festgestellt (Digitale Signatur).
- Rechteverwaltung
  Im Rahmen der Rechteverwaltung wird festgelegt, mit welchen Protokollen und Diensten und zu welchen Zeiten über das Firewall-System eine Kommunikation stattfinden darf.
- Kontrolle auf der Anwendungsebene
  Es wird überprüft, ob Kommandos genutzt oder Dateiinhalte übertragen werden, die nicht zur, durch die Anwendung definierten, Aufgabenstellung gehören.
- Entkopplung von Diensten
  Dienste werden entkoppelt, damit Implementierungsfehler, Schwachstellen und Konzeptionsfehler der Dienste nicht die Möglichkeit für Angriffe bieten.
- Beweissicherung und Protokollauswertung
  Verbindungsdaten und sicherheitsrelevante Ereignisse werden protokolliert und können für die Beweissicherung von Handlungen der Benutzer und für die Erkennung von Sicherheitsverletzungen ausgewertet werden.
- Alarmierung
  Besonders sicherheitsrelevante Ereignisse werden an ein Security Management gesendet, damit bei Sicherheitsverletzungen schnell reagiert werden kann.

neuKap02.fm Seite 49 Freitag, 18. Oktober 2002 3:50 15

- Verbergen der internen Netzstruktur
  Ziel ist es, die Struktur des zu schützenden Netzes gegenüber dem unsicheren Netz zu verbergen. Es soll aus dem unsicheren Netz nicht sichtbar sein, ob im zu schützenden Netz 10, 100, 1 000 oder 10 000 Rechnersysteme vorhanden sind.
- Vertraulichkeit der Nachrichten
  Nachrichten können nicht im Klartext gelesen werden. Dadurch ist die Vertraulichkeit der Daten bei einer Übertragung über unsichere Netze gewährleistet.

Weitere Ziele eines Firewall-Systems

- Das Firewall-System selbst muss gegen Angriffe resistent sein.
- Accounting (IP- und benutzerorientiert)
- Network Address Translation

neuKap02.fm Seite 50 Freitag, 18. Oktober 2002 3:50 15

neuKap03.fm Seite 51 Freitag, 18. Oktober 2002 3:50 15

Kapitel 3

TCP/IP-Technologie für Internet und Intranet

Das Internet, das »Netz der Netze«, verkörpert eine einzigartige, weltumspannende Infrastruktur vernetzter Netzwerke und die Software-Technologien, auf denen diese Netzwerke aufbauen. Die TCP/IP-Technologie (Transmission Control Protocol/Internet Protocol) ist das eigentliche Herz des Internets. Erst die hohe Verwendung der TCP/IP-Protokolle ermöglichte die weltweite Vernetzung der Rechnersysteme bis hin zum kleinsten PC im letzten Winkel dieser Erde /Hamp96/.

Die TCP/IP-Technologie ist kein feststehendes Gebilde, sondern besteht aus unterschiedlichen Diensten und Anwendungen, die im Laufe der Jahre ständig weiterentwickelt wurden. TCP- und IP-Protokoll sind streng genommen nur zwei Komponenten der gesamten Kommunikations-Architektur, haben sich aber als übergeordneter Begriff im Sprachgebrauch durchgesetzt.

3.1 Von den Anfängen bis heute

Ursprünglich hatte das Internet, wie viele Projekte der Hochtechnologie, militärische Zielsetzungen. Die ersten Gedanken machte man sich bereits Ende der Fünfzigerjahre, als die amerikanische *»RAND Corp.«* ein Konzept für ein Kommando- und Überwachungsnetzwerk militärischer Einrichtungen entwickelte. Der Kern dieses Konzepts bestand aus einem dezentralen Aufbau, der auch nach teilweiser Zerstörung der Infrastruktur, z. B. nach einem Atomschlag, die Funktionsfähigkeit der amerikanischen Militäreinrichtungen gewährleisten sollte.

Um im technologischen Wettstreit mit der Sowjetunion die amerikanische Militärtechnologie in eine führende Position zu bringen, rief die US-Regierung unter anderem die *»Advanced Research Projects Agency«* (ARPA) ins Leben. Deren Aufgabe war es, neue und innovative Technologien zu entwickeln. Aus den ursprünglichen Konzepten der »RAND Corp.« entwickelten die ARPA-Ingenieure die paketorientierte Datenübertragung, die die Datenkommunikation in den folgenden Jahren revolutionieren sollte. Ende 1969 wurde zwischen der *»University of California at Los Angeles«*, der *»University of California at Santa Barbara«*, der *»University of Utah«* und dem *»Stanford Research Institute«* (SRI) in Menlo-Park in Kalifornien das erste experimentelle Netz (ARPANET) in Betrieb genommen. Für den Erfolg des ARPANET sorgten vor allem die auf allen angeschlossenen Rechnern

neuKap03.fm Seite 52 Freitag, 18. Oktober 2002 3:50 15

zur Verfügung gestellten Dienstleistungen wie Terminalsitzung (Remote LogIn), Dateiübertragung (File Transfer) und Elektronische Post (Electronic Mail).

Im Jahr 1973 begann die inzwischen in *»Defense Advanced Research Projects Agency«* (DARPA) umbenannte Organisation ein weiteres Projekt, um die zwischenzeitlich neben dem ARPANET entstandenen, unterschiedlichen Übertragungsmechanismen zu verbinden. So entstand auf der Basis des TCP/IP-Konzepts das erste wirkliche Internet. Die Grundzüge dieser Technologie wurden 1974 von *Victor Cerf* (Stanford University) und *Bob Kahn* (DARPA) erstmals in einem veröffentlichten Artikel festgelegt. Ein erstes Testnetz wurde 1977 in Betrieb genommen und in den kommenden Jahren ständig erweitert. 1983 hatte das immer noch experimentelle ARPANET eine derartige Ausdehnung erreicht, dass man beschloss, die Kontrolle über dieses Netz an die *»Defense Communication Agency«* (DCA) abzugeben. Gleichzeitig wurden sämtliche Netzknoten auf das TCP/IP-Protokoll umgestellt und das bisherige Netz in einen militärischen Bereich (MILNET) und einen forschungsorientierten Bereich (ARPANET) aufgeteilt.

In den letzten Jahren hat sich das Internet sehr stark gewandelt. Die Fortschritte der Kommunikationstechnologie und das stetig wachsende Informationsbedürfnis haben das Internet explosionsartig anwachsen lassen. Waren früher fast ausschließlich Universitäten, Institute und deren Wissenschaftler ans Internet angeschlossen, so ist es heute zu einem Informationsforum für die breite Öffentlichkeit geworden. Heute sind schätzungsweise 500 Millionen Benutzer in über 240 Ländern an das Internet angeschlossen (Stand Ende 2001).

Als Anfang der Neunzigerjahre das World Wide Web (WWW) eingeführt wurde, bot sich erstmals die Möglichkeit, unter einer einheitlichen Darstellung unterschiedliche Dienste mit multimedialen Inhalten, wie z. B. Bildern, Tönen, Animationen und Videos, zu transportieren. Einige Strategen erkannten das Potenzial dieses Mediums, und innerhalb weniger Jahre wurde das World Wide Web zu einem globalen Marktplatz, auf dem fast alle großen, aber auch immer mehr mittlere und kleine Organisationen vertreten sind. Die meisten Internetprovider stellen für ihre Kunden heute, bis zu einem gewissen Umfang kostenlos, Platz auf ihren Servern zur Verfügung. Damit bietet sich für jeden privaten Anwender die Möglichkeit, auf einer eigenen Homepage sich selbst, seine Hobbys, Interessen und Neigungen weltweit zu präsentieren und Kontakt mit Gleichgesinnten aufzunehmen.

Die elektronische Post (E-Mail) ist heute im geschäftlichen und privaten Umgang ein fester Bestandteil unserer täglichen Kommunikation geworden. Die meisten Mitarbeiter in Firmen und Behörden sind heute per E-Mail zu erreichen, und auf Visitenkarten ist die Angabe einer E-Mail-Adresse mittlerweile obligatorisch.

neuKap03.fm Seite 53 Freitag, 18. Oktober 2002 3:50 15

Die rasante Entwicklung des Internets hat aber auch Schattenseiten mit sich gebracht. Die TCP/IP-Technologie war nicht für ein solches globales Netz gedacht. Durch die in den Anfangsjahren auf wenige Teilnehmer begrenzte Ausdehnung des Internets waren Sicherheitskonzepte wie Zugriffsberechtigung, Vertraulichkeit der Daten während der Übertragung und Schutz von Netzsegmenten vor unberechtigten Zugriffen nicht in dem Maße erforderlich wie heute. Da sich mittlerweile jeder von fast jedem Ort auf der Welt in das Internet einschalten kann, sind damit natürlich auch Sicherheitsmaßnahmen unumgänglich geworden.

3.2 Vorteile der TCP/IP-Technologie

TCP/IP-Technologie bietet entscheidende Vorteile:

- Für jeden Benutzer besteht die Möglichkeit, auf jede für ihn freigegebene Information innerhalb des gesamten Netzwerks zugreifen zu können. Zusätzlich kann jeder angeschlossene Benutzer mit jedem anderen angeschlossenen Rechnersystem kommunizieren. Es gibt bereits Anwendungen, die weltweites Telefonieren oder Videokonferenzen von einem Rechnersystem zum nächsten ermöglichen. Dadurch wird der Informationsaustausch zwischen den unterschiedlichen Benutzern gewährleistet, der das Internet in Zukunft zu *dem* globalen Informationsforum machen wird.
- Bereits bei der Konzeption Anfang der Siebzigerjahre legte man fest, dass diese Protokolle unabhängig von der verwendeten Netzwerktechnologie sein sollten. Durch diese Forderung ist die Kommunikation zwischen den unterschiedlichen Rechner- und Netzwerktypen, wie z. B. im Internet, möglich geworden. Gleichzeitig bietet es die Möglichkeit, neue technologische Entwicklungen mit bereits vorhandenen Strukturen zu verknüpfen. Durch die permanente Weiterentwicklung der Technik im Computer- und Kommunikationsbereich lässt sich die bewährte Technologie ohne weiteres auf neue Entwicklungen übertragen, ist dann aber immer noch in der Lage, mit älteren Systemen zu kommunizieren.
- Durch die ständige Weiterentwicklung ist das Internet zu einer ausgereiften Technologie geworden, die sich im alltäglichen Einsatz bewährt hat.
- Die Internet-Technologie ist heute weit verbreitet, daher gibt es auch ein breites Angebot kompatibler Netzkomponenten. Da die meisten Software-Varianten auch durch Implementierungen anderer Hersteller ersetzbar sind, bedeutet das eine geringe Herstellerabhängigkeit. Durch die starke Verbreitung innerhalb des Internets werden die Produkte auch zunehmend billiger.
- Die einzelnen Protokollspezifikationen sind standardisiert und für jedermann frei zugänglich. Dadurch sind Implementierungen für neue oder spezielle Systeme jederzeit leicht zu entwickeln oder anzupassen.

neuKap03.fm Seite 54 Freitag, 18. Oktober 2002 3:50 15

3.3 Das OSI-Referenzmodell

Das OSI-Referenzmodell hat eine klare Architektur und eignet sich daher besonders gut für die Darstellung einer Kommunikationsarchitektur und der Prinzipien des Schichtenmodells. Um eine einheitliche Struktur für gegenwärtige und zukünftige Entwicklungen von Netzwerktechnologien festzulegen, einigte man sich auf das so genannte OSI-Referenzmodell (Open System Interconnection), das 1983 von der »International Organisation for Standardization« (ISO) als Standard festgelegt wurde. In diesem Modell wird davon ausgegangen, dass ein Kommunikationsprotokoll aus mehreren Modulen besteht, von denen jedes einzelne Modul während einer Kommunikation unterschiedliche Aufgaben zu erfüllen hat.

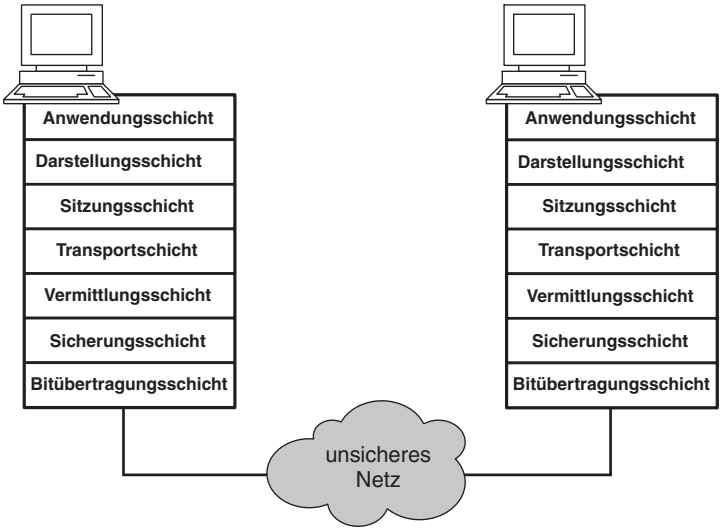


Abb. 3.1: Das OSI-Referenzmodell

Das OSI-Referenzmodell besagt nun, dass bei einer Verbindung z. B. zwischen zwei Rechnersystemen jede Schicht des Rechnersystems A mit der gleichen Schicht des Rechnersystems B kommunizieren kann. Dazu werden den Daten in jeder Schicht bestimmte Bitmuster in einem Header vorangestellt oder einem Trailer am Ende angefügt. Diese Bitmuster enthalten so genannte Protokollinformationen, die z. B. darüber Auskunft geben

- wer die Daten abgesandt hat,
- wer die Daten empfangen soll,
- welchen Weg die Daten während der Übertragung nehmen sollen,
- wie die Daten weiterverarbeitet werden dürfen,
- oder wie sie vom Empfänger behandelt werden sollen.

neuKap03.fm Seite 55 Freitag, 18. Oktober 2002 3:50 15

Jede weitere Schicht übernimmt die Datenpakete der übergeordneten Schicht und fügt, falls dies für den Ablauf der Kommunikation notwendig sein sollte, ihre eigenen Protokollinformationen in einem weiteren Header oder Trailer hinzu. Die Auswertung der Protokolldaten erfolgt beim Empfänger nur auf der jeweils gleichen Schicht, d.h., die Daten einer übergeordneten Schicht werden von einer niedrigeren Schicht nicht interpretiert oder ausgewertet.

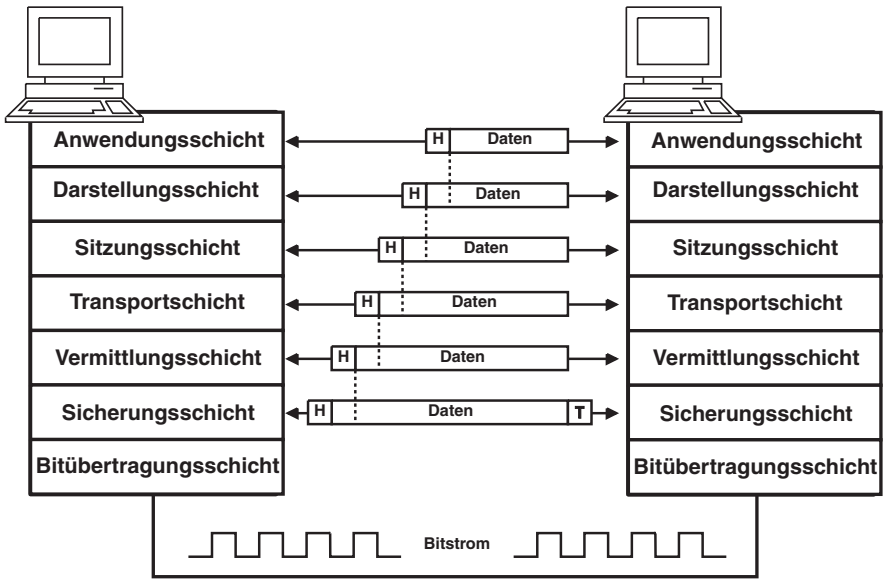


Abb. 3.2: Kommunikation zwischen zwei Rechnern

Im folgenden Abschnitt soll kurz erläutert werden, welche Aufgaben die jeweiligen Schichten übernehmen:

1. Die Bitübertragungsschicht (Physical Layer) legt fest, wie die Daten physikalisch übertragen werden. Zu den Parametern dieser ersten Schicht gehören Informationen über die verwendeten Übertragungsmedien, wie z.B. Kupferkabel, Glasfaser, Infrarot- oder Funkübertragung, und die Spezifikation von Schnittstellen mit Spannungspegeln, Steckverbindern und Datenübertragungsraten.
2. Die Aufgabe der Sicherungsschicht (Data Link Layer) ist die sichere Datenübertragung zwischen zwei benachbarten Stationen, z.B. Router, innerhalb eines Netzwerkes. Dazu werden die zu übertragenden Bits in Rahmen (Frames) zusammengefasst und mit einer Prüfsumme versehen. Wird ein solcher Rahmen unvollständig übertragen oder zerstört, so fordert der Empfänger nach einem Vergleich der Prüfsumme den entsprechenden Rahmen erneut beim Absender an.

neuKap03.fm Seite 56 Freitag, 18. Oktober 2002 3:50 15

3. Die Vermittlungsschicht (Network Layer) legt die Übertragungswege (Routen) für die Daten zwischen zwei Rechnersystemen fest. Dazu werden Informationen wie z. B. Übertragungszeit, Auslastung des Übertragungsweges usw. benutzt, um nach festgelegten Regeln, dem Routing-Protokoll, eine Verbindung herzustellen. Die innerhalb dieser Schicht transportierten Daten werden in Datenblöcken übertragen, die man als Pakete bezeichnet.
4. Die Transportschicht (Transport Layer) stellt eine Art virtueller Verbindung zwischen den beiden Rechnersystemen bereit. Sie sorgt vor allem für eine Korrektur der Übertragungsfehler und ist sehr stark von den untergeordneten Schichten abhängig.
5. Die Sitzungsschicht (Session Layer) dient der Verwaltung von Kommunikationsprozessen. Dabei wird die Verbindung mit einem oder mehreren Kommunikationspartnern kontrolliert und gleichzeitig dafür gesorgt, dass die jeweilige Kommunikation synchron abläuft, d. h., dass bei einem aufgetretenen Fehler die Daten wieder in der richtigen Reihenfolge zusammengefügt werden.
6. In der Darstellungsschicht (Presentation Layer) werden die zu übertragenden Daten in ein einheitliches Format gebracht. Dies ist vor allem bei der Verwendung von unterschiedlichen Zeichensätzen, z. B. ASCII und EBCDIC, notwendig. Zusätzlich können in dieser Schicht weitere Funktionen zur Umwandlung, Verschlüsselung oder Komprimierung der zu übertragenden Daten enthalten sein.
7. Die Anwendungsschicht (Application Layer) beinhaltet schließlich die eigentlichen Anwendungs- und Dienstprogramme für die unterschiedlichen Funktionen, die über die Netzwerkverbindung ausgeführt werden sollen.

3.4 TCP/IP-Protokollarchitektur

Obwohl es keine generelle Vereinbarung über ein spezielles TCP/IP-Schichtenmodell gibt, kann man sagen, dass es aus weniger Schichten aufgebaut ist als das OSI-Referenzmodell. In den folgenden Kapiteln wollen wir uns deshalb auf ein Vier-Ebenen-Modell beziehen.

In diesem Modell gibt es analog zum OSI-Referenzmodell unterschiedliche Kommunikationsebenen, die Daten von der übergeordneten Ebene zur nächsttieferen Ebene weiterreichen. Jede Kommunikationsebene fügt den Daten eigene Kontrollinformationen hinzu, bis sie über das Netz gesendet werden. Der Empfänger reicht diese Daten dann Ebene für Ebene nach oben weiter, wobei jede Ebene nur die für sie relevanten Daten auswertet und diese aus dem Datenpaket entfernt, bevor sie an die nächsthöhere Ebene weitergegeben werden.

neuKap03.fm Seite 57 Freitag, 18. Oktober 2002 3:50 15

Abb. 3.3: Ebenen der TCP/IP-Protokollarchitektur

- Die Netzzugangsebene ermöglicht einem Rechnersystem Daten zu einem anderen Rechnersystem innerhalb des direkt angeschlossenen Netzes (z. B. Ethernet) zu übertragen. Dazu sind genaue Kenntnisse des zugrunde liegenden Netzaufbaus nötig. Die Netzzugangsebene umfasst die zwei unteren Ebenen des OSI-Modells und beinhaltet die Kapselung von IP-Paketen in Netzrahmen (Frames) und die Zuordnung von IP-Adressen zu physikalischen Netzadressen, z. B. MAC-Adressen.
- Die Netzwerkebene definiert den Aufbau von IP-Paketen und bestimmt, auf welchem Weg die Daten durch das Internet übertragen werden (Routing).
- Die Transportebene stellt eine Verbindung zwischen zwei Endpunkten oder Rechnersystemen her. Die wichtigsten Protokolle sind hier TCP und UDP.
- Die Anwendungsebene beinhaltet sämtliche Programme und Dienste, die über die Netzwerkverbindung durchgeführt werden sollen. Dazu gehören vor allem Dienste wie Telnet (Login auf einem anderen Rechnersystem), FTP (Datentransfer zwischen zwei Rechnersystemen), SMTP (E-Mail-Funktionen), HTTP (World Wide Web) usw.

neuKap03.fm Seite 58 Freitag, 18. Oktober 2002 3:50 15

3.5 Internet-Adressen

Wie finden die Daten im Internet ihr Ziel? Ganz klar, jedes Rechnersystem im Internet hat eine bestimmte IP-Adresse und einen Namen.

Bei der Entwicklung der Internet-Adressierung legte man nicht nur hohen Wert auf die Identifizierung jedes angeschlossenen Rechnersystems, sondern auch darauf, an welcher Stelle innerhalb eines Netzwerkes es sich befindet und über welche Übertragungswege die Daten ihr Ziel erreichen können. Dazu bekommt jeder Benutzer im weltweiten Netzwerk eine einmalige 32 Bit oder 4 Byte lange Internet-Adresse (IPv4-Adressierung), bestehend aus einer Netzwerk- und einer Rechnersystem-Identifikation, die als 4 Dezimalzahlen dargestellt werden und jeweils durch einen Punkt getrennt sind.

Beispiel: 11000011 . 10010011 . 00111000 . 11101101 entspricht 195 . 147 . 56 . 237

Diese Adressierung wird in fünf Klassen (Klasse A bis E) aufgeteilt. Jede dieser Klassen unterscheidet sich in der Länge der Netzwerk- und der Rechnersystem-Identifikation (Abb. 3.4). Diese Aufteilung wurde getroffen, da man in den Anfangstagen des ARPANET davon ausging, dass es in Zukunft nur wenige große (Klasse-A-) Netzwerke (z. B. für Militär und Forschung) geben würde. Doch nach einigen Jahren zeigte sich mit der Einführung von lokalen Netzwerken in vielen Organisationen, dass diese Annahme nicht mehr stimmte. Durch die Vergabe von Klasse-A-Adressen wurden die Möglichkeiten schnell begrenzt. Aus diesem Grund führte man zwei weitere Klassen für mittelgroße (Klasse B) und kleine Netze (Klasse C) ein. Den Klasse-D-Adressen fällt eine besondere Bedeutung zu. Sie werden als so genannte Multicast-Adressen bezeichnet. Das bedeutet, dass bestimmte Datenpakete nicht mehr an jedes Rechnersystem einzeln verschickt werden müssen, sondern gleichzeitig an eine ganze Gruppe von Rechnersystemen, denen eine Multicast-IP-Adresse zugeordnet wurde, gesendet werden können. Die IP-Adressen der Klasse E sind für zukünftige Anwendungen reserviert und werden derzeit zu Forschungszwecken verwendet. Sie sollen genutzt werden, um IPv6-Pakete über IPv4-Netze zu routen.

Das starke Wachstum des Internet hat zu einem Mangel an IP-Adressen geführt. Außerdem sind dadurch die Routing-Tabellen der Backbone-Router, die die einzelnen Netze verbinden, zu groß geworden. Aus diesem Grund hat man die starre Aufteilung in nur fünf Netzklassen aufgehoben (vgl. RFC 1517). Die 32 Bit der IP-Adresse können nun beliebig auf Netz-ID und Rechnersystem-ID verteilt werden. Somit ergeben sich 33 mögliche Netzwerk-Klassen. Für die ursprünglichen fünf Klassen, die immer noch am häufigsten vorkommen, werden die alten Bezeichnungen (Klasse A bis E) weiterverwendet.

neuKap03.fm Seite 59 Freitag, 18. Oktober 2002 3:50 15

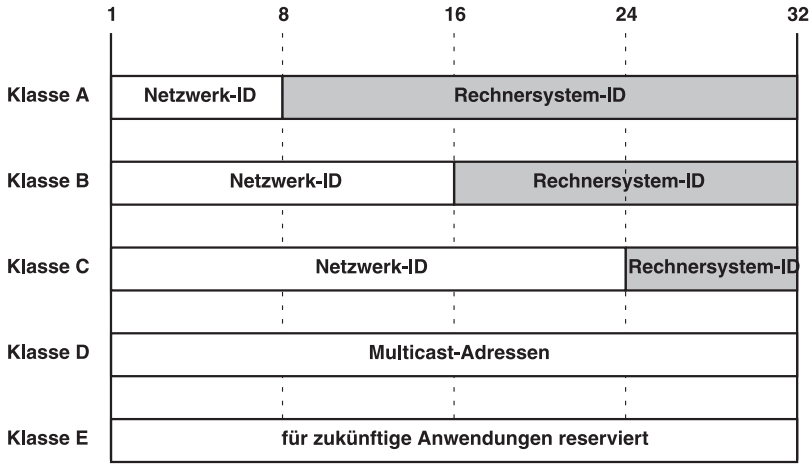


Abb. 3.4: Aufbau von Internetadressen und Einteilung in Klassen

Viele Anwender, die einen Internet-Anschluss über einen Provider haben, sind nur gelegentlich mit dem Internet verbunden. Für diese Rechnersysteme ist es nicht notwendig, eine permanente IP-Adresse zu vergeben. Hier benutzt man die Möglichkeit, IP-Adressen automatisch zu vergeben. Wenn ein Kunde Zugang zum Internet haben möchte, wählt er zunächst einen Einwahlknoten eines Providers in seiner Nähe an. Das Rechnersystem des Providers hat zu diesem Zweck eine Reihe von IP-Adressen reserviert, die dem jeweiligen Anrufer dann automatisch zugeordnet werden und nur für die aktuelle Sitzung gültig sind. Dieses Verfahren nennt man dynamische IP-Adressierung.

Da aufgrund des starken Wachstums des Internets abzusehen war, dass die Anzahl der freien IP-Adressen eines Tages erschöpft sein wird, ist man seit 1995 dabei festzulegen, die Adresslänge zukünftig auf 128 Bit oder 16 Byte (IPv6 oder IPnG next generation) zu verlängern. Natürlich sind die alten IP-Adressen weiterhin gültig und können auch nach dem neuen Standard weiterhin verarbeitet werden. Es muss damit gerechnet werden, dass der fließende Übergang zwischen IPv4 und IPv6 noch sehr lange dauern wird.

Unternehmen verwenden heute meistens nur noch wenige offizielle IP-Adressen, sondern arbeiten mit verborgenen, intern reservierten IP-Adressen, was die Adressenproblematik stark reduziert. (siehe dazu auch Kapitel 12.1 *Network Address Translation*)

Die IP-Adressierung ist für technische Systeme hervorragend geeignet. Im praktischen Umgang hat sich aber gezeigt, dass dieses Verfahren für viele Anwender zu kompliziert und undurchsichtig ist. Wer schon einmal durch das World Wide Web gesurft ist, dem ist sicherlich aufgefallen, dass viele Rechnersysteme nicht über ihre IP-Adressen aufgerufen werden, sondern über einen oder mehrere symbolische Namen.

neuKap03.fm Seite 60 Freitag, 18. Oktober 2002 3:50 15

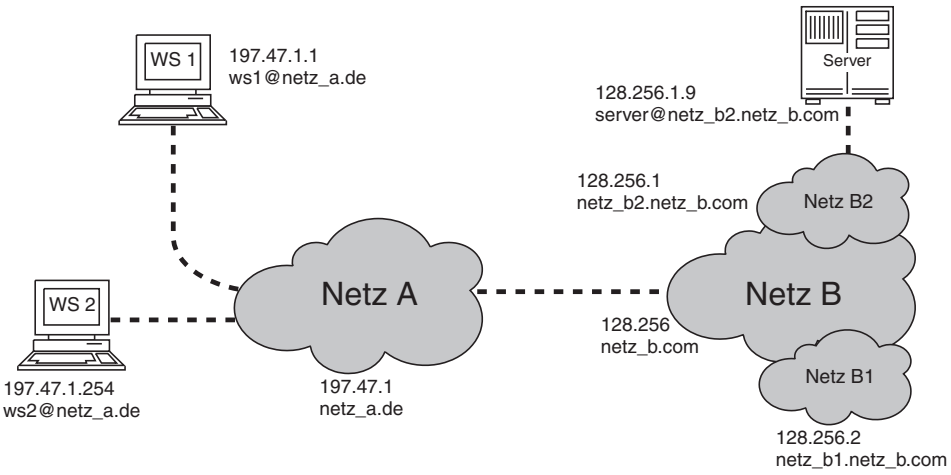


Abb. 3.5: IP- und Domainnamenadressierung

Jedes ans Internet angeschlossene Netz kann zu diesem Zweck neben einem IP-Adressbereich zusätzlich einen Domainnamen erhalten. IP-Netze und DNS-Domains müssen nicht deckungsgleich sein, auch wenn dies meistens der Fall ist. Innerhalb der Domain kann der jeweilige Netzbetreiber für untergeordnete Netze weitere Subdomains erstellen, um sein Netz noch tiefer zu strukturieren. Die Domainnamen werden zentral vom Network Information Center (NIC) und seinen Unterorganisationen (z. B. DENIC in Deutschland) vergeben und verwaltet. Wenn eine Organisation einen eigenen Domainnamen verwenden möchte, so muss sie oder ihr Provider bei der verantwortlichen Unterorganisation des NIC die Zuordnung dieses Namens beantragen. Die Toplevel Domains sind vom Network Information Center fest vorgegeben und in unterschiedliche Nutzerprofile oder lokale Gruppen eingeteilt, z. B.:

- .arpa für spezifische Einrichtungen des ARPANET
- .com für kommerzielle Organisationen aus Industrie und Handel
- .edu für Universitäten und Schulen
- .gov für Regierungsstellen und staatliche Einrichtungen
- .mil für militärische Einrichtungen der US-Streitkräfte
- .org für nicht kommerzielle Einrichtungen
- .de für Einrichtungen in Deutschland
- .uk für Einrichtungen in Großbritannien

Neue, so genannte generic Top Level Domains (gTLD), sind in Vorbereitung:

- .aero für Unternehmen der Luftfahrtindustrie
- .biz für Unternehmen
- .coop für genossenschaftliche Organisationen
- .info für allgemeine WWW-Angebote

neuKap03.fm Seite 61 Freitag, 18. Oktober 2002 3:50 15

- .museum für Museen
- .name für Privatpersonen
- .pro für Ärzte, Anwälte, Steuerberater etc.

Die Vorschläge ».firm«, ».shop« und ».web« wurden verworfen.

Ausführlichere Informationen dazu und eine Sammlung von Links, mit deren Hilfe Sie die Entwicklung verfolgen können, finden Sie unter

```
http://www.denic.de/doc/gtld/index.html
```

3.6 Die Kommunikationsprotokolle

Die folgenden Beschreibungen der am häufigsten im Internet verwendeten Kommunikationsprotokolle und Dienste sollen als Hinweis dienen, welche Informationen jeweils übertragen werden. Diese Informationen sind äußerst wichtig für den Transport der Daten innerhalb und zwischen den Netzen. Gleichzeitig können die übertragenen Daten aber auch manipuliert werden und bei falschem Umgang für enormen Schaden beim Empfänger verantwortlich sein.

Grundsätzlich unterscheidet man zwei verschiedene Arten von Kommunikationsprotokollen. Die verbindungslosen Protokolle kann man mit Telegrammen vergleichen. Die Daten werden vom Absender ins Netz geschickt und können während der Übertragung verloren gehen, dupliziert werden oder verspätet eintreffen, ohne den Absender darüber zu informieren. Man nennt derartige Informationseinheiten auch Datagramme. Diese Art der Kommunikation ist wie der Paketdienst einer Post-Gesellschaft. Man gibt das Paket an einer Stelle ab; wie es dann weitergeleitet wird, darauf hat man keinen Einfluss.

Im Gegensatz dazu bauen die verbindungsorientierten Protokolle eine Kommunikation nach einem bestimmten Schema auf. Zuerst wird eine virtuelle Verbindung zwischen Absender und Empfänger aufgebaut. Nach dem gegenseitigen Austausch von festgelegten Informationen erfolgt dann der eigentliche Datentransfer, und erst wenn beide Seiten den ordnungsgemäßen Empfang der Daten bestätigt haben, wird die Verbindung wieder abgebaut. Hier ist eine Analogie eine Telefonverbindung: Ein Teilnehmer baut die Verbindung auf, und wenn der andere abgenommen hat, kann das Telefonat beginnen.

3.6.1 IP-Protokoll

Das Internet Protocol (IP) ist ein verbindungsloses Protokoll der Netzwerkebene. Ein IP-Header besteht aus mehreren Feldern, die folgende Bedeutung oder Funktionen haben:

- Version: Versionsnummer des verwendeten IP-Protokolls, mit dem das IP-Paket (Datagramm) erstellt wurde.

neuKap03.fm Seite 62 Freitag, 18. Oktober 2002 3:50 15

- Headerlänge: Dieses Feld bestimmt die Länge des IP-Headers in 32-Bit-Einheiten.
- Servicetyp: Man kann die Wichtigkeit eines IP-Paketes mit diesem Feld festlegen und bestimmen, auf welche Art oder welchem Weg dieses IP-Paket übertragen werden soll, z. B. mit geringer Verzögerung, mit hohem Datendurchsatz oder auf einer sicheren Route.
- Gesamtlänge: Die Länge des gesamten IP-Pakets in Bytes.
- Identifikation: Während der Übertragung kann ein IP-Paket in mehrere Fragmente aufgeteilt werden. Dabei wird jedes IP-Paket mit einer Identifikation versehen. Anhand dieser Identifikation und der Quell-Adresse kann ein fragmentiertes IP-Paket beim Ziel-Rechnersystem wieder zusammengefügt werden.
- Flags: Das erste Bit legt fest, ob ein IP-Paket während der Übertragung fragmentiert werden darf. Das zweite Bit ist bei der Zusammensetzung einer fragmentierten Nachricht von Bedeutung. Es bestimmt, ob die enthaltenen Daten aus der Mitte oder vom Ende der ursprünglichen Nachricht stammen.
- Fragment-Offset: Wenn eine Nachricht in mehrere Fragmente zerlegt wird, werden diese Fragmente der Reihe nach durchnummeriert und dann abgeschickt. Da die einzelnen IP-Pakete innerhalb des Netzwerks unterschiedliche Wege nehmen können, treffen die IP-Pakete beim Ziel-Rechnersystem nicht immer in der richtigen Reihenfolge ein. Dieser kann die Teile einer Nachricht erst dann wieder zu einer vollständigen Nachricht zusammensetzen, wenn er sämtliche Teile erhalten hat.
- Time to Live (TTL): Wenn ein IP-Paket vom Quell-Rechnersystem ins Netz geschickt wird, muss das Ziel-Rechnersystem nicht unbedingt erreichbar sein. In einem derartigen Fall würde das IP-Paket solange im Netz kursieren, bis das Ziel-Rechnersystem irgendwann bereit ist, das IP-Paket zu empfangen. Damit dies nicht passiert, wird vom Quell-Rechnersystem für jedes IP-Paket eine Lebensdauer in Sekunden festgelegt. Jedesmal, wenn das IP-Paket von einer Zwischenstation, z. B. einem Router oder einem Netzknoten, weitergeleitet wird, wird der Wert dieses Feldes herabgesetzt. Hat das Feld den Wert Null erreicht, wird das IP-Paket gelöscht bzw. nicht mehr weitergeleitet.
- Protokoll: In diesem Feld wird protokolliert, welche weiteren Protokolle in das IP-Paket eingebettet sind, z. B. TCP, UDP, ICMP, usw.
- Header-Prüfsumme: Um die Unversehrtheit eines Headers zu gewährleisten, wird aus den vorhandenen Feldern eine Prüfsumme errechnet und vom Quell-Rechnersystem in dieses Feld eingetragen. Wenn das IP-Paket weitergeleitet wird oder beim Ziel-Rechnersystem angekommen ist, wird die Prüfsumme neu berechnet und mit dem eingetragenen Wert verglichen.
- Quell-Adresse: Dieses Feld enthält die IP-Adresse des Quell-Rechnersystems (Absender).
- Ziel-Adresse: Dieses Feld enthält die IP-Adresse des Ziel-Rechnersystems (Empfänger).

neuKap03.fm Seite 63 Freitag, 18. Oktober 2002 3:50 15

- IP-Optionen: Dieses Feld dient hauptsächlich dem Testen von Netzwerken und der Fehlersuche. Hier können bestimmte Optionen festgelegt werden, die z. B. Einschränkungen oder Informationen zur Weiterleitung der Daten enthalten. So können hier etwa Informationen für das Source Routing eingefügt werden, d. h., jede Zwischenstation einer Verbindung wird vor der Übertragung detailliert festgelegt.

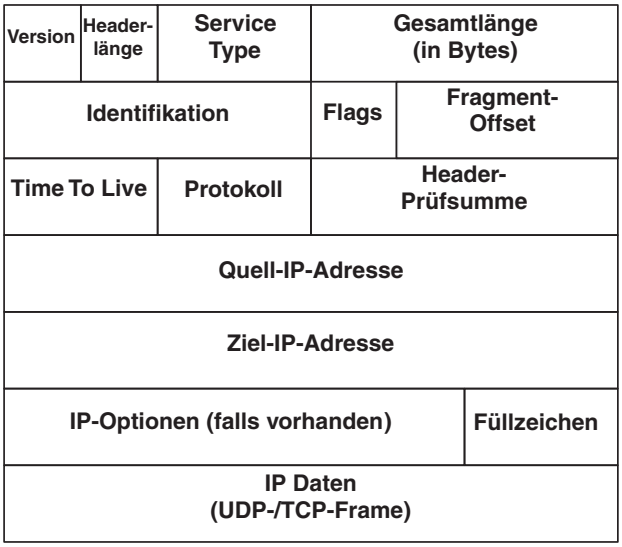


Abb. 3.6: Header eines IP-Datenpaketes

3.6.2 Routing Protokolle

In einem komplexen Netzwerk wie dem Internet gibt es viele verschiedene Möglichkeiten, wie Daten von der Quelle an ihr Ziel gelangen. Den Prozess, bei dem die Verbindungswege innerhalb der Netze festgelegt werden, nennt man Routing.

Zu diesem Zweck gibt es an der Verbindungsstelle von zwei oder mehreren Netzen spezielle Rechnersysteme (Router oder Gateways), die nach festgelegten Regeln bestimmen können, welchen Weg die Daten nehmen sollen. Jeder Router benutzt zur Festlegung der Wege eigene Routingtabellen. Darin sind alle direkt angeschlossenen Rechnersysteme und die Verbindungsstellen zu benachbarten Netzen enthalten. Diese Tabellen können sich in Abhängigkeit von verschiedenen Faktoren, wie z. B. der Netzauslastung oder der Verfügbarkeit bestimmter Rechnersysteme oder Netze, jederzeit ändern. Dieses Verfahren nennt man dynamisches Routen.

neuKap03.fm Seite 64 Freitag, 18. Oktober 2002 3:50 15

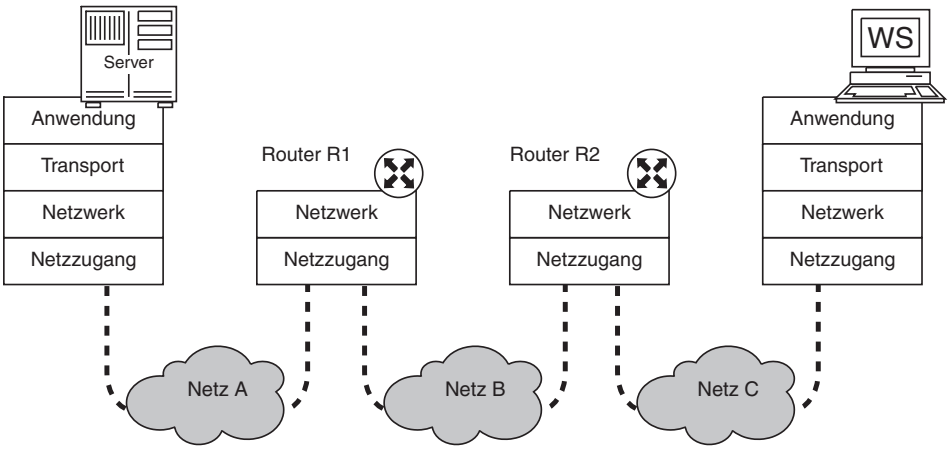


Abb. 3.7: Routing über verschiedene Netze

Routing Protokolle wie RIP (Routing Information Protocol) oder OSPF (Open Shortest Path First) dienen dazu, diese Veränderungen der Routen an die beteiligten Systeme weiterzuleiten. Ein Angreifer hat die Möglichkeit, falsche RIP-Informationen zu erzeugen und dadurch unerwünschte Routen bzw. Zwischenstationen einzufügen. Eine dieser Zwischenstationen kann es ihm dann ermöglichen, die Informationen abzuhören oder zu manipulieren.

Als wesentlich sicherer hat sich dagegen die Methode des statischen Routings erwiesen. Bei diesem Verfahren wird nicht jedem einzelnen Router die Entscheidung überlassen, welchen Weg die Daten zu nehmen haben, sondern der Übertragungsweg wird vorher detailliert festgelegt und in die Datenpakete mit eingefügt. Das statische Routing ist wegen der Dynamik im Internet nicht möglich. Im zu schützenden Intranet kann es eine höhere Sicherheit gewährleisten.

Im Gegensatz zu Rechnersystemen, in denen die Daten alle Protokollebenen durchlaufen, werden die Daten bei Routern nur bis zur Netzwerkebene weitergereicht.

3.6.3 ICMP

In einem verbindungslosen Protokoll besteht keine Möglichkeit, den Absender zu informieren, ob das Datenpaket die vorgesehene Lebensdauer (Time To Live) überschritten hat, ob der Empfänger nicht erreichbar ist oder die Daten unterwegs verloren oder zerstört wurden. Dennoch braucht man eine Möglichkeit, derartige Informationen zwischen Rechnersystemen auszutauschen. Aus diesem Grund wurde das Internet Control Message Protocol (ICMP) in das IP-Protokoll integriert, das ein unverzichtbarer Bestandteil der Internet-Protokolle ist und in keiner Internet-Anwendung fehlen darf.

neuKap03.fm Seite 65 Freitag, 18. Oktober 2002 3:50 15

Router oder Rechnersysteme werten diese Nachrichten meist automatisch aus und veranlassen bestimmte Aktionen oder Umkonfigurationen. Ein Angreifer wird dadurch in die Lage versetzt, durch Absenden falscher ICMP-Informationen Einfluss auf das System zu nehmen, bzw. bestimmte Reaktionen zu erzeugen, die es ihm später ermöglichen, die Funktionsfähigkeit zu beeinträchtigen oder ins System einzubrechen (siehe Kapitel 4.5 *Angriffsmethoden und prinzipielle Gegenmaßnahmen auf der Grundlage der TCP/IP-Protokolle*).

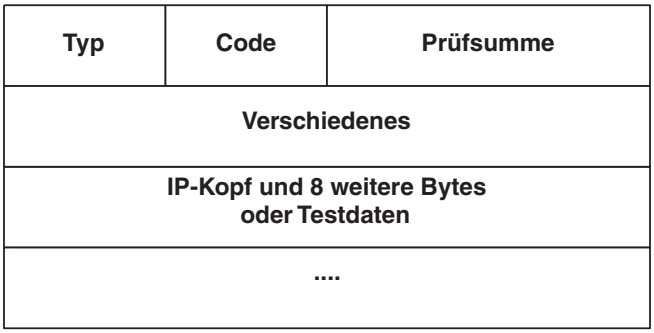


Abb. 3.8: Header eines ICMP-Datenpaketes

Das ICMP-Datenpaket enthält Fehler- und Diagnoseinformationen. Es wird intern vom IP angestoßen und verarbeitet. Obwohl die ICMP-Nachrichten in ein IP-Datenpaket gekapselt werden, bilden sie kein höheres Protokoll, wie z. B. TCP oder UDP, sondern sind ein direkter Bestandteil des IP-Protokolls. Das IP-Protokoll kann in der Praxis nicht ohne das ICMP-Protokoll verwendet werden. Diese Nachrichten werden nur von dem Rechnersystem abgesendet, das den Fehler versendet oder ausgelöst hat, und direkt an den ursprünglichen Absender der Daten zurückgeschickt.

Man unterscheidet verschiedene Typen von ICMP-Nachrichten. Diese werden durch eine Ziffer im Header eines ICMP-Paketes (Typ) gekennzeichnet und können je nach ICMP-Datentyp unterschiedliche Daten enthalten. Die wichtigsten sind:

- Echo Reply (0): Diese Nachricht wird ausgelöst, sobald eine EchoRequest-Nachricht von einem anderen Rechnersystem empfangen wurde. Im Datenfeld dieses Paketes werden Testdaten versendet, die unter anderem Aufschluss über Betriebsbereitschaft, Laufzeit usw. geben.
- Destination Unreachable (3): Wenn eine Nachricht nicht an ihr beabsichtigtes Ziel gelangt, wird diese Nachricht an den Absender zurückgesandt. Ein Grund dafür kann sein, dass ein Netzwerk, ein Host, ein Protokoll oder ein Port nicht erreichbar waren. Oder während der Übertragung wäre eine Fragmentierung

neuKap03.fm Seite 66 Freitag, 18. Oktober 2002 3:50 15

des gesendeten Datenpakets nötig gewesen. Dies wurde aber durch das Setzen des Fragmentierungsbits im Header des IP-Pakets verboten. Ein weiterer Grund ist, dass ein bestimmtes Rechnersystem, das vom Absender in der Source-Routing-Option eingetragen wurde, nicht erreichbar war. Die Meldung Destination Unreachable kann z.B von einem Angreifer dazu missbraucht werden, alle Verbindungen zwischen den beteiligten Rechnersystemen zu unterbrechen.

- Source Quench (4): Wenn ein Router nicht über die entsprechende Kapazität verfügt, um die empfangenen Daten direkt weiterzuleiten, sendet er an den Absender diese Nachricht. Dieser muss dann die Aussenderate von weiteren Nachrichten verringern.
- Redirect (5): Wenn ein Router erkennt, dass der Absender, statt direkt an den nächsten Router zu senden, einen unnötigen Umweg nimmt, sendet er diese Nachricht an den Absender. Das Datenfeld enthält die IP-Adresse des direkt erreichbaren Routers und wird vom Absender in dessen eigene Routingtabelle eingetragen. Dieses Vorgehen kann von einem Angreifer missbraucht werden, um unerwünschte Routen zu konfigurieren und die Daten unterwegs abzuhören oder zu manipulieren.
- Echo Request (8): Diese Nachricht wird ausgesendet, um zu überprüfen, ob der beabsichtigte Empfänger erreichbar ist. Zusammen mit der Echo-Reply-Antwort auf diese Nachricht lassen sich Rückschlüsse über Betriebsbereitschaft, Laufzeit usw. ziehen.
- Time exceeded (11): Wenn ein IP-Datenpaket seine Lebensdauer (Time to Life) überschreitet, bevor es sein Ziel erreicht hat, wird es verworfen. Der Absender erhält dann von dem Rechnersystem, das diesen Vorgang ausgeführt hat, diese Meldung.
- Parameter Problem (12): Wenn ein IP-Datenpaket aufgrund fehlerhafter Angaben im Header verworfen wurde, erhält der Absender des Paketes diese Nachricht.

Ein Beispiel für die Benutzung von ICMP-Nachrichten ist der Befehl PING, der auf den meisten Rechnersystemen verwendet wird. Dieser Befehl wird auf der Benutzerebene erzeugt und sendet eine oder mehrere ICMP-Nachrichten an den Empfänger. Dabei werden die Befehle EchoRequest und EchoReply verwendet, und der Absender erhält Informationen über:

- die IP-Adresse des Empfängers, und ob das Rechnersystem erreichbar ist,
- die MAC-Adresse des nächsten Routers bzw. Rechnersystems,
- Routing-Einträge,
- Laufzeit der Daten,
- Datenverluste.

neuKap03.fm Seite 67 Freitag, 18. Oktober 2002 3:50 15

3.6.4 Portnummern

Ein wichtiger Begriff, der im Zusammenhang mit den Kommunikationsprotokollen auf der Transportebene immer wieder auftaucht, sind die so genannten Ports. Ein Rechnersystem, z. B. ein Server, muss in der Lage sein, mit mehr als einem anderen Rechnersystem gleichzeitig zu kommunizieren. Anderenfalls würde der Server während einer aufgebauten Verbindung für alle anderen Rechnersysteme nicht erreichbar sein. Bestimmte Anwendungen erfordern auch den gleichzeitigen Aufbau von zwei oder mehr Verbindungen, z. B. eine für eine Übertragung von Kommandos und eine für die Datenübertragung. Zu diesem Zweck verfügt jedes Rechnersystem über so genannte Portnummern, die zusammen mit der Netzwerk-Identifikation und der Rechnersystem-Identifikation einen Kommunikationsendpunkt (Port) bilden. Dieser Aufbau ist in etwa vergleichbar mit einer Telefonnummer. Die Netzwerk-Identifikation lässt sich mit der Vorwahl vergleichen, die Rechnersystem-Identifikation mit der Rufnummer und die Portnummer mit der Nebenstelle.

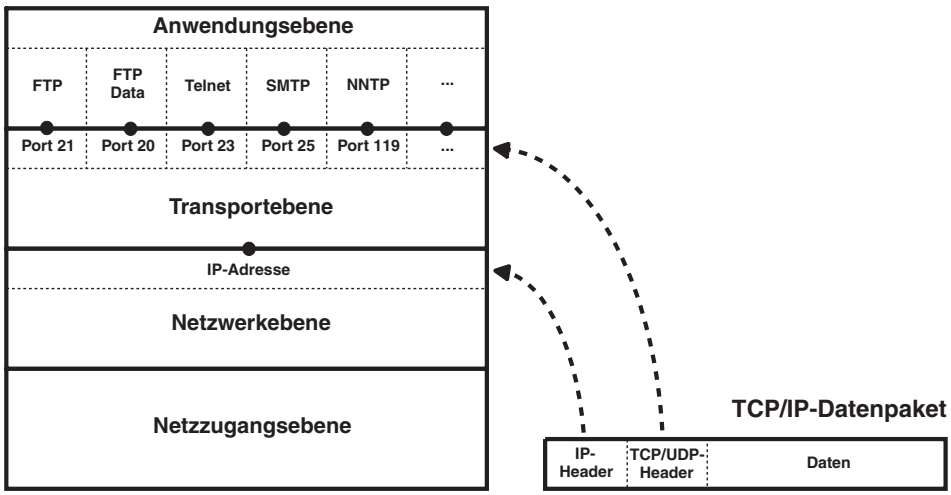


Abb. 3.9: Eindeutige Identifizierung des Kommunikationsendpunktes durch IP-Adresse und Portnummer

Da eine Portnummer aus 16 Bit aufgebaut wird, wäre ein Rechnersystem mit einer IP-Adresse rein theoretisch in der Lage, gleichzeitig 65 535 Verbindungen zu anderen Kommunikations-Endpunkten herzustellen. Dies ist in der Praxis aber nicht der Fall, da die unterschiedlichen Kommunikationsprotokolle wie TCP oder UDP unterschiedliche Adressräume verwenden, die zwar identische Portnummern haben können, aber physikalisch nicht übereinstimmen.

neuKap03.fm Seite 68 Freitag, 18. Oktober 2002 3:50 15

Die Dienste der Anwendungsschicht (z. B. Telnet oder FTP) erfordern, wie wir später sehen werden, eine bestehende virtuelle Verbindung zwischen zwei Rechnersystemen. Um diese Verbindung überhaupt aufbauen zu können, muss dem aktiven, Kontakt aufnehmenden Rechnersystem (Client) aber zumindest ein Port bekannt sein, auf dem der entsprechende Dienst des passiven Rechnersystems (Server) erreichbar ist.

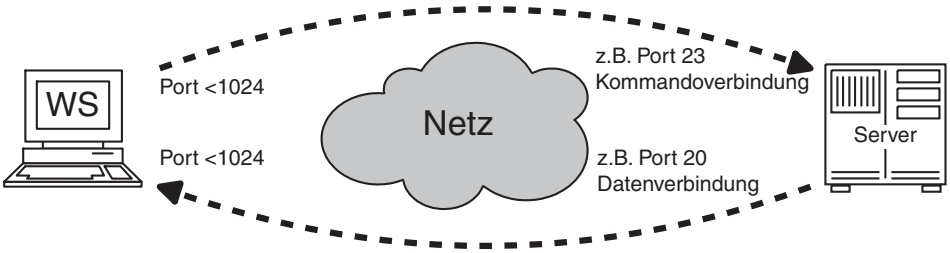


Abb. 3.10: Verbindung zwischen zwei Rechnern (z. B. FTP-Verbindung)

Zu diesem Zweck wurden bestimmte Portnummern (well-known-ports) definiert, die standardmäßig für die entsprechenden Dienste zur Verfügung stehen. Der Client kann dem Server dann über diesen Port seine eigene verwendete Portnummer mitteilen, und einem Verbindungsaufbau steht damit nichts mehr im Wege.

Dienst	Portnummer	Protokoll
echo	7	UDP oder TCP
ftp-data	20	TCP
ftp	21	TCP
telnet	23	TCP
smtp	25	TCP
dns	53	UDP
tftp	69	UDP
finger	79	TCP
http	80	TCP
nntp	119	TCP

Tabelle 3.1: Auszug aus der Liste mit well-known-ports

neuKap03.fm Seite 69 Freitag, 18. Oktober 2002 3:50 15

3.6.5 UDP

Das User Datagram Protocol (UDP) ist ein verbindungsloses Kommunikationsprotokoll der Transportebene. Es benutzt das untergeordnete IP-Protokoll, um Nachrichten von einem Rechnersystem zum anderen zu transportieren. In Ergänzung zum IP-Protokoll kann es aber zwischen mehreren Anwendungsdiensten (Ports) des Empfängers unterscheiden.

Der entscheidende Vorteil von UDP ist der geringe Overhead. Dadurch eignet es sich z. B. zur Übertragung von kleinen Datenmengen. Hier ist es einfacher, die Daten bei einem aufgetretenen Fehler einfach noch einmal zu übertragen, als eine garantiert fehlerfreie Verbindung aufzubauen. Dazu braucht man einen Frage-Antwort-Dialog zwischen zwei Rechnersystemen. Wenn nach einer bestimmten Zeit keine Antwort vom Ziel-Rechnersystem kommt, wird das Datenpaket noch einmal auf den Weg geschickt. Eine weitere Möglichkeit ist, einer übergeordneten Anwendung die Sicherungsfunktionen zu überlassen. In diesem Fall ist es unnötig, die Datenübertragung doppelt zu überwachen.

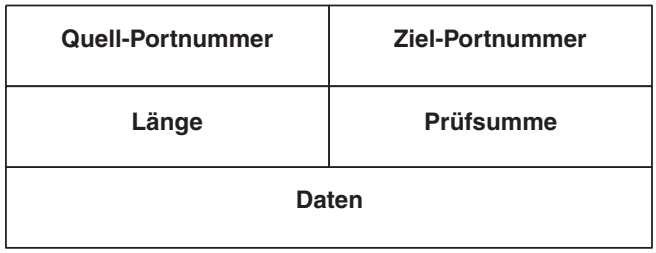


Abb. 3.11: Header eines UDP-Datenpaketes

- Das UDP-Protokoll erzeugt keinerlei Transportquittungen oder andere Sicherheitsmaßnahmen, um die Korrektheit der Übertragung zu bestätigen. Es werden keine Informationen an das Quell-Rechnersystem zurückgegeben.
- Wenn die Daten auf dem Weg zum Ziel-Rechnersystem in mehrere Fragmente aufgeteilt wurden, können die Daten unterschiedliche Wege nehmen. So können Daten im Ziel-Rechnersystem in vertauschter Reihenfolge ankommen. Das UDP-Protokoll gibt die Daten unsortiert an die übergeordnete Anwendung weiter.
- Wenn die Daten schneller eintreffen, als das Ziel oder ein Rechnersystem im Netz sie verarbeiten kann, z.B wenn es überlastet ist, können die Daten verloren gehen. Es gibt keinerlei Informationen, die den Datenfluss zwischen den Rechnersystemen steuern oder kontrollieren.
- Der Header enthält zwei 16-Bit-Portnummern, die unabhängig von den beim TCP-Protokoll benutzten Portnummern sind.

neuKap03.fm Seite 70 Freitag, 18. Oktober 2002 3:50 15

- Grundsätzlich ist diese Form der Datenübertragung nicht vertrauenswürdig und sehr leicht zu manipulieren. Auf exponierten Rechnersystemen, die öffentlich zugänglich sind, sollte das UDP-Protokoll vermieden werden, es sei denn, eine übergeordnete Ebene (Anwendungsebene) übernimmt die Sicherungsfunktionen.

3.6.6 TCP

Das Transmission Control Protocol (TCP) ist nach dem IP-Protokoll das wichtigste Transportprotokoll. Das TCP-Protokoll ist ein verbindungsorientiertes Kommunikationsprotokoll der Transportebene, d.h., bevor die Daten von der Quelle zum Ziel geschickt werden, wird eine virtuelle Verbindung hergestellt, die in beide Richtungen (duplex) funktioniert. Die Daten werden in Form von festgelegten Paketen übertragen und die korrekte Übertragung durch unterschiedliche Verfahren sichergestellt.

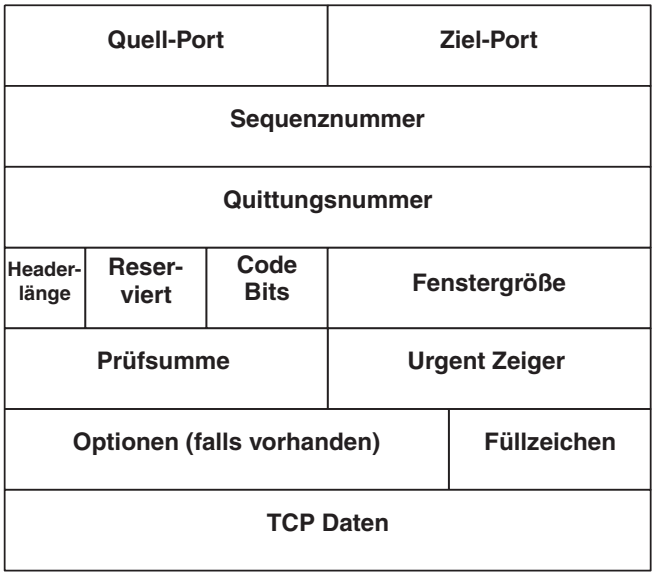


Abb. 3.12: Header eines TCP-Datenpaketes

- Der Header eines TCP-Datenpaketes enthält u.a. zwei 16-Bit-Portnummern, die zur Identifikation der Kommunikationsendpunkte von Quelle und Ziel dienen. Über die standardisierte Zuordnung (well-known-ports) können die unterschiedlichen Dienste der Anwendungsschicht Verbindung miteinander aufnehmen.
- Beim Aufbau einer Verbindung generiert jede TCP-Einheit eine Anfangs-Sequenznummer. Diese Nummern werden ausgetauscht und gegenseitig

neuKap03.fm Seite 71 Freitag, 18. Oktober 2002 3:50 15

bestätigt. Jedes gesendete Datensegment enthält eine fortlaufende Sequenznummer, wobei Duplikate ausgeschlossen werden. Anhand dieser Sequenznummern können die Daten beim Ziel, unabhängig vom Zeitpunkt des Eintreffens der Segmente, in der korrekten Reihenfolge zusammengesetzt werden.

- Die Quittungsnummer wird vom Ziel-Rechnersystem an das Quell-Rechnersystem der Daten übermittelt. Die Quittungsnummer ist immer um eins höher als die letzte Sequenznummer, die korrekt empfangen wurde. Anhand dieser Nummer kann das Quell-Rechnersystem die Pakete, die noch für eine eventuell erforderliche Wiederholung vorhanden sind, aus seinem Datenpuffer löschen.
- Das Feld Headerlänge bestimmt die Länge des Protokollkopfes in 32-Bit-Worten und damit den Anfang der Nutzdaten.
- Die Codebits oder Flags lösen bestimmte Reaktionen im TCP-Protokoll aus. Auf die genaue Bedeutung soll hier aber nicht weiter eingegangen werden.
- Ein Quell-Rechnersystem darf nicht mehr Daten abschicken, als ein Ziel-Rechnersystem verarbeiten oder weiterleiten kann. Dazu gibt das Ziel-Rechnersystem im Feld »Fenstergröße« an, wie viel Daten es zur sofortigen Verarbeitung in seinem Puffer zwischenspeichern kann.
- Jedes Datensegment enthält eine Prüfsumme, die aus dem Header und den Nutzdaten gebildet wird. Das Ziel-Rechnersystem errechnet aus den erhaltenen Daten ebenfalls eine Prüfsumme und vergleicht diese mit dem Datenfeld im Header des Datensegmentes. Stimmen die Werte überein, so schickt das Ziel-Rechnersystem eine positive Bestätigung an das Quell-Rechnersystem. Ein beschädigtes Datensegment wird zunächst ignoriert und nach einer angemessenen Wartezeit erneut angefordert.
- Für einige Dienste wurde ein Mechanismus konzipiert, mit dem der Server dazu veranlasst werden kann, dringende Anweisungen auszuführen, obwohl noch nicht alle Eingabedaten verarbeitet wurden. Diesem Zweck dient der Dringlichkeitszeiger (Urgent Data), der auf das Datenbyte vor der dringenden Meldung verweist (z. B. die Übertragung eines Ctrl-C-Zeichens bei einer Telnet-Session).
- Normalerweise wird in einem TCP-Paket als Option nur die maximale Segmentgröße (Maximum Segment Size) verwendet. Damit teilt das Quell-Rechnersystem dem Ziel-Rechnersystem die maximale Größe der zu sendenden Datensegmente mit. Die weiteren Optionen sind No Operation und End of Option List.
- Das Feld »Füllzeichen« wird dazu benutzt, die Länge des Optionsfeldes auszugleichen, damit die Gesamtgröße des Headers immer ein Vielfaches eines 32-Bit-Wortes ergibt.

Jedes Segment enthält eine Zeitüberwachung, d. h., dass ein Ziel-Rechnersystem nach einer bestimmten Zeit eine Quittung über die enthaltenen Pakete an das Quell-Rechnersystem zurückschicken muss. Wenn ein Quell-Rechnersystem nach

neuKap03.fm Seite 72 Freitag, 18. Oktober 2002 3:50 15

Ablauf der Quittungszeit keine Antwort erhalten hat, wird das entsprechende Datensegment erneut gesendet.

Damit haben wir die Protokolle der Transportschicht abgehandelt. In den folgenden Kapiteln wollen wir uns die Protokolle und Dienste der Anwendungsschicht genauer betrachten.

3.6.7 DNS

Um Rechnersystem-Namen entsprechende IP-Adressen zuordnen zu können, musste man in den Anfängen des Internets eine Liste der Rechnersystem-Namen von einem zentralen Server regelmäßig per Datenübertragung auf jedem Rechnersystem aktualisieren. Durch die rasante Ausbreitung des Internets ist diese Methode nicht mehr praktikabel. Aus diesem Grund wurde der Domain Name Service (DNS) entwickelt. Damit wurden die Rechnersystem-Namen nicht mehr auf jedem einzelnen Rechnersystem registriert, sondern auf speziell für diesen Dienst bereitgestellten Servern innerhalb jedes Teilnetzwerkes. Die einzelnen Rechnersysteme senden bei Bedarf Abfragen (Queries) an diese Namen-Server, die als Antwort die entsprechende IP-Adresse oder den dazugehörigen Rechnersystem-Namen liefern.

Um dieses System benutzen zu können, ist jedes Internet-Teilnetzwerk dazu verpflichtet, einen Domain-Namens-Server zu betreiben oder betreiben zu lassen, auf dem sich so genannte Zonen-Datenbanken befinden. In diesen Datenbanken befinden sich unter anderem zwei Tabellen, mit der einem bestimmten Rechnersystem-Namen die dazugehörige IP-Adresse zugeordnet werden kann und umgekehrt.

Prinzipiell muss beachtet werden, dass alle vom DNS zur Verfügung gestellten Informationen missbraucht werden können, da diese Informationen nicht durch kryptographische Verfahren geschützt werden. Um Zugriff auf ein Rechnersystem eines Netzes zu erhalten, benötigt ein Eindringling zunächst dessen IP-Adresse, die er entweder durch blindes Probieren oder einfacher durch Auswertung der DNS-Informationen erhalten kann. Mittels dieser Informationen kann der Eindringling dann beispielsweise eine Adressfälschung (IP-Spoofing) vornehmen und damit Zugriff auf Rechnersysteme innerhalb des zu schützenden Netzes erhalten.

3.6.8 Telnet

Das Telnet-Protokoll erlaubt einem Benutzer (Client), eine Terminalsitzung auf einem entfernten Rechnersystem (Server) durchzuführen. Dazu wird zuerst eine TCP-Verbindung zwischen Client und dem Port 23 des Servers aufgebaut. Anschließend wird eine LogIn-Prozedur durchgeführt, in der sich der Benutzer durch die Angabe des Benutzernamens und des Passwortes identifizieren und authentisieren muss.

neuKap03.fm Seite 73 Freitag, 18. Oktober 2002 3:50 15

Abb. 3.13: Beispiel einer Telnet-Sitzung

Bei dieser Authentikation über den Telnet-Dienst wird das Passwort im Klartext übertragen. Deshalb besteht die Gefahr, dass sich ein Angreifer auf dem Übertragungsweg in eine autorisierte Telnet-Verbindung eingeschaltet hat, um sicherheitsrelevante Informationen (z. B. Passwörter) abzuhören, oder um eigene Befehle in die Telnet-Verbindung einzugeben.

Anschließend kann der Angreifer sich unter Angabe der vorher abgehörten Identität auf dem Server anmelden (Maskerade-Angriff), um für ihn relevante Daten auszuspionieren, zu manipulieren oder zu löschen.

3.6.9 FTP

Das File Transfer Protocol (FTP) ermöglicht den Austausch und die Übertragung von beliebigen Dateien, ähnlich einem Datei-Manager, zwischen entfernten Rechnersystemen. Bei der Nutzung von FTP werden zwei unterschiedliche Verbindungen genutzt. Der Client baut als Erstes von einem beliebigen Port eine Verbindung zum Port 21 des Servers auf. Über diese Verbindung sendet der Client dem Server die Kommandos. Mit dem Kommando »port« teilt der Client dem Server mit, über welchen Port er die Daten übertragen soll. Der Server baut nun anhand dieser Angaben eine TCP-Verbindung vom Port 20 zum angegebenen Port des Client auf und überträgt die angeforderten Daten.

Um den Austausch von Befehlen zwischen Rechnersystemen mit verschiedenen FTP-Servern zu ermöglichen, wurden für FTP eine Reihe von standardisierten Kommandos definiert. Diese sind nicht identisch mit den Kommandos der Benutzeroberfläche. Der FTP-Client übersetzt die Kommandos der Benutzeroberfläche in die entsprechenden Standardbefehle für die Kommunikation. Für ein Firewall-System sind die standardisierten Kommandos relevant, da nur diese tatsächlich über eine TCP/IP-Verbindung übertragen werden.

Während der Client die Kommandoverbindung zum Port 21 des Servers aufbaut, ist der Server für den Aufbau des Datenkanals von seinem Port 20 zu einem beliebigen Port des Clients verantwortlich. Dies stellt eine Sicherheitslücke dar, da sich ein Angreifer selbst als Server ausgeben oder eigene Daten in die Kommunikation mit dem Server einfügen kann. Damit bekommt er die Möglichkeit, gefährliche Programme wie z. B. Viren oder Trojanische Pferde in das Rechnersystem einzuschleusen, die anschließend Daten ausspionieren oder zerstören können.

neuKap03.fm Seite 74 Freitag, 18. Oktober 2002 3:50 15

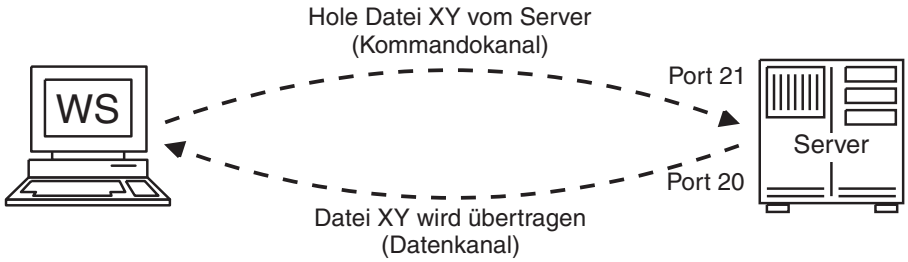


Abb. 3.14: Beispiel einer FTP-Verbindung

Eine Abhilfe ist hier die passive Methode (siehe Kapitel 5.2.4 *Überprüfungen auf der Transportebene*).

3.6.10 SMTP

Das Simple Mail Transport Protocol (SMTP) ist ein einfaches Protokoll für die Übertragung von elektronischen Nachrichten (E-Mails) durch das Internet/Intranet. Das E-Mail-System besteht aus zwei Komponenten: dem Message Transfer Agent (MTA) und dem Mail User Agent (UA). Der Message Transfer Agent wird vom jeweiligen Internetprovider oder Intranetbetreiber installiert und hat die Aufgabe, die elektronische Post über die Teilnetzwerke an ihren Bestimmungsort weiterzuleiten. Der Mail User Agent ist nichts anderes als die E-Mail-Software, mit der der Benutzer je nach Programm seine elektronische Post verfassen, versenden und empfangen kann. Die elektronische Post wird auf dem Message Transfer Agent solange gespeichert, bis der Benutzer sie mithilfe seiner Software auf das lokale Rechnersystem lädt.

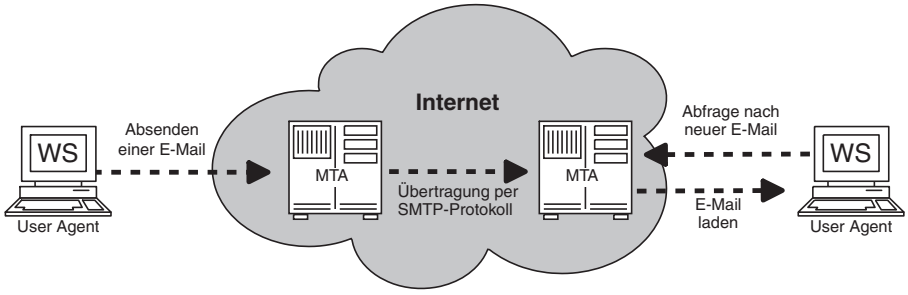


Abb. 3.15: Funktionsweise des E-Mail-Dienstes

Der Übertragungsmodus der Nachrichten durch das Internet mithilfe des SMTP-Protokolls ist sehr einfach aufgebaut und wird im Klartext durchgeführt. Es ist bisher nicht möglich, die Identität des Absenders zu überprüfen. Dadurch ist es mög-

neuKap03.fm Seite 75 Freitag, 18. Oktober 2002 3:50 15

lich, Nachrichten mit beliebigem oder gefälschtem Absender (Mail-Spoofing) über das Internet zu verbreiten. Einziger Schutz für den Anwender ist die Verwendung von kryptographischen Verfahren, wie z. B. der digitalen Signatur mit Verschlüsselung (siehe Kapitel 7 *Firewall-Systeme und Verschlüsselung*).

Ein weiterer Schwachpunkt des E-Mail-Systems ist das Programm Sendmail als die am weitesten verbreitete Umsetzung eines Message Transfer Agent unter Verwendung des SMTP-Protokolls. Die Komplexität und umfassende Leistungsfähigkeit macht Sendmail gleichzeitig sehr fehleranfällig und schwer zu konfigurieren. Dadurch wurden in den letzten Jahren immer wieder Sicherheitslücken entdeckt, mit denen Daten von Angreifern kopiert, manipuliert oder zerstört werden konnten.

3.6.11 HTTP

Wenn ein Anwender von seinem Rechnersystem aus eine Reise ins Internet unternimmt, benötigt er dafür ein spezielles Programm (Browser), das unter anderem die Darstellung von so genannten HTML-Dokumenten ermöglicht. HTML (Hyper Text Markup Language) ist ein Standard, der den Aufbau und das Format der für das World Wide Web charakteristischen Seiten definiert. Dabei muss es sich nicht nur um Textinformationen handeln. Es können gleichzeitig auch Grafiken, Töne oder Animationen und Videos übertragen werden. Um diese Informationen im Internet übertragen zu können, wurde ein spezielles Kommunikationsprotokoll entwickelt, das Hypertext Transfer Protokoll (HTTP).

Das HTTP-Protokoll arbeitet nicht Session-orientiert, d. h., die Übertragung eines HTML-Dokuments erfolgt unabhängig von einem zuvor übertragenen HTML-Dokument. Dazu wird, wie bei anderen Kommunikationsprotokollen der Anwendungsschicht (z. B. FTP oder Telnet), zunächst eine virtuelle Verbindung (TCP) zwischen Client und Server aufgebaut. Diese bleibt aber nicht über mehrere Anforderungen des Clients hinweg bestehen, sondern wird sofort nach dem Versenden der Antwort vom Server wieder abgebaut.

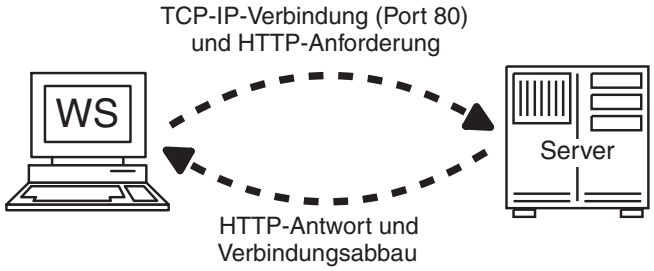


Abb. 3.16: Prinzip einer HTTP-Verbindung

neuKap03.fm Seite 76 Freitag, 18. Oktober 2002 3:50 15

Wenn ein Benutzer eine beliebige Seite auf einem Server aufruft, so liest der Browser zunächst das HTML-Dokument und baut den Text entsprechend der angegebenen Formatierungen (Größe, Farbe, Schriftart usw.) auf. Wenn eine WWW-Seite zusätzliche Informationen enthält, z. B. Grafiken, Geräusche oder Videos, so ist im HTML-Dokument der genaue Ort dieser Datei verzeichnet. Der Browser baut dann über das HTTP-Protokoll eine erneute Verbindung auf und holt sich die Grafik, Klangdatei, Video oder sonstige Information vom Server. Nach dem Abschluss der Übertragung wird diese Information vom Browser auf dem Rechnersystem des Anwenders direkt dargestellt bzw. wiedergegeben. Die meisten Browser kann man so konfigurieren, dass sie nur die gewünschten Informationen darstellen. Wenn z. B. nur eine sehr langsame Verbindung ins Internet vorhanden ist, so kann man auf die Darstellung von großen Daten, wie z. B. Grafiken, verzichten und nur die Textinformationen darstellen (siehe Abb. 3.17 und 3.18).

Abb. 3.17: Ansicht eines HTML-Dokumentes im Browser

neuKap03.fm Seite 77 Freitag, 18. Oktober 2002 3:50 15


```
<HR>

<H3><A NAME="Hacker besuchen CIA"></A>Hacker &quot;besuchen&quot; CIA</H3>

<DL>
<DD><P><A HREF="http://www.odci.gov/cia"><IMG SRC="../images/cia.gif"
ALT="CIA" HSPACE=5 HEIGHT=95 WIDTH=96 ALIGN=LEFT></A>
</P>

<P>Eine Gruppe schwedischer Hacker ist in den Internet-Rechner des amerikanischen
Geheimdienstes CIA eingedrungen und hat die Web-Seiten nach ihren Vorstellungen
ge&auml;ndert. Die Central Intelligence Agency wurde dabei kurzerhand in &quot;Central
Stupi dity Agency&quot;  (Zentrale Beh&ouml;rde f&uuml;r Dummheit) umbenannt. Au&szlig;erdem
wurden &quot;Hotlinks&quot; zu verschiedenen Sex- und Musikangeboten gelegt. Kurze Zeit
nach dem &quot;Anschlag&quot; war die Internet-Adresse der CIA nicht mehr zu erreichen.
Bereits im  August manipulierten unbekannte Hacker die Eingangsseite des amerikanischen
Justizministeriums und ver&auml;nderten den Titel in &quot;U.S. Departement of
Injustice&quot; (US-Ministerium f&uuml;r Ungerechtigkeit). </P>

<P><I>Quelle: compact 12/96</I></P>
</DL>

<P><A HREF="#Inhaltsverzeichnis">[Zur&uuml;ck zum Inhaltsverzeichnis]</A>
<A HREF="#Seitenende">[Zum Seitenende]</A></P>

<HR>

<H3><A NAME="Schutz gegen Lauscher und Spione"></A>Schutz gegen Lauscher
und Spione</H3>

<DL>
<P><IMG SRC="../images/tgv.gif" ALT="CIA" HSPACE=5 HEIGHT=92 WIDTH=150 ALIGN=LEFT>
<IMG SRC="../images/ice.gif" ALT="CIA" HSPACE=5 HEIGHT=96 WIDTH=150 ALIGN=RIGHT>
</P>

<P>Satte 3,5 Milliarden Mark h&auml;tte <I>Siemens</I> vor drei Jahren           der dicke
Auftrag aus Korea eingebracht, statt dessen gab es aber nur Zoff und Theater. Denn
nachdem der franz&ouml;sische Anbieter <I>GEC Alsthom</I> den M&uuml;nchnern den
Auftrag weggeschnappt hatte, lancierte <I>Siemens</I> einen ungeheuerlichen Vorw           urf:
&quot;Der franz&ouml;sische Geheimdienst las und lauschte mit und gab s&auml;mtliche
Informationen an den TGV-Hersteller weiter.&quot; ...</P>

<P><I>Quelle: impulse 10/96</I></P>
</DL>

<P><A HREF="#Inhaltsverzeichnis">[Zur&uuml;ck zum Inhaltsverzeichnis]</A>
<A HREF="#Seitenende">[Zum Seitenende]</A></P>
```

Abb. 3.18: Ansicht eines HTML-Dokumentes im Quellcode

Cookies und aktive Inhalte

Ein wichtiges Thema, das immer wieder für Aufregung sorgt, ist die Verwendung von aktiven Elementen, so genannten Java-Applets, ActiveX-Controls oder JavaScript-Befehlen. Diese Elemente sind kleine eigenständige Programme, die per HTTP-Protokoll auf das Rechnersystem des Anwenders geladen und ausgeführt werden.

Die Gefahr besteht darin, dass diese aktiven Elemente nicht nur irgendwelche grafischen Abläufe darstellen können, sondern unter Umständen auch Zugriff auf elementare Systemressourcen haben. So können sie Dateien oder Verzeichnisse löschen, Manipulationen an Daten ausführen oder Informationen sammeln und eigenständig über das Internet verschicken. Näheres zu diesem Thema finden Sie im Kapitel *13.2 Java und und seine Verwandten*.

neuKap03.fm Seite 78 Freitag, 18. Oktober 2002 3:50 15

Nicht ganz so gefährlich sind die so genannten Cookies, Datenstrukturen, die vom Web-Server auf den Client geladen und dort zur weiteren Verwendung zwischengespeichert werden. Der Cookie-Mechanismus wurde von der Netscape Corporation entwickelt, da das HTTP-Protokoll zustandslos ist: Jedesmal, wenn ein Browser die URL einer Internet-Seite beim Web-Server abfragt, wird dieser Vorgang als neue Aktion bewertet. Die Tatsache, dass es sich bei dieser Anfrage vielleicht nur um die letzte von vielen Abfragen dieser Art handelt, wenn der Anwender durch das Internet surft, wird vom HTTP-Protokoll nicht registriert.

Auf der einen Seite sorgt diese Eigenschaft des Protokolls dafür, dass das weltweite Netz effizienter wird, andererseits aber macht diese Eigenschaft es aber außerordentlich schwierig, z.B. virtuelle Einkaufswagen im Internet zu realisieren, da es hierbei erforderlich ist, dass die Aktionen des Anwenders für einen längeren Zeitraum nachgehalten werden müssen.

Cookies können nur eingesetzt werden, um Informationen zu speichern, die zu einem bestimmten Zeitpunkt vorgelegen haben. Hierzu ein Beispiel: Wenn man einen Antrag ausfüllt, auf dem die Lieblingsfarbe angegeben wird, dann kann diese Information vom Server zu einem Cookie verarbeitet und an den Browser des Anwenders geschickt werden. Wenn diese Site beim nächsten Mal vom Anwender aufgerufen wird, gibt der Browser das Cookie zurück und ermöglicht es dem Server somit, die Hintergrundfarbe der Seite entsprechend der Lieblingsfarbe des Benutzers zu ändern.

Cookies können jedoch auch für andere, umstrittene Zwecke eingesetzt werden: Jedesmal, wenn ein Browser eine Seite im Internet aufruft, werden Spuren über den Anwender hinterlassen, die mit der Zeit immer umfassender werden. Unter diesen vielen unterschiedlichen Informationen, die gesammelt werden, befinden sich z.B. auch Name und IP-Adresse des Computers, der Name des benutzten Browsers, das Betriebssystem des Rechners, die URL der besuchten Internet-Seiten. Ohne Cookies ist es fast unmöglich, diese Spuren systematisch zu verfolgen und genaue Informationen über den Anwender und seine Angewohnheiten zu sammeln. Mit der Hilfe von Cookies wird es zum Kinderspiel, diese elektronischen Spuren systematisch zu sammeln und auszuwerten.

Schon beim Design des Cookie-Mechanismus durch die Entwickler von Netscape wurden Fehler gemacht, die einen sorgfältigen Umgang mit Cookies vom Benutzer verlangen. Cookies werden im Normalfall nicht nur an denjenigen Server zurückgeschickt, von dem sie ursprünglich auf den Client geladen wurden, sondern auf alle Rechner derselben Domäne. Damit soll gewährleistet werden, dass auch Cluster von Web-Servern bei vielbesuchten Anbietern einwandfrei über Cookies zu steuern sind. Zur Entscheidung, ob ein Rechner zur Domäne des Cookiesenders gehört, werden schlicht und einfach die Punkte im Namen von rechts nach links gezählt: Rechner1.utimaco.de gehört zur selben Domäne wie Rechner2.utimaco.de, weil sich die Namen nur links vom zweiten Punkt unter-

neuKap03.fm Seite 79 Freitag, 18. Oktober 2002 3:50 15

scheiden. Dieser Mechanismus, der im Übrigen auch im Internet Explorer von Microsoft implementiert ist, funktioniert aber nicht in Ländern mit erweiterten Domänenstrukturen. Der Rechner Rechner1.company1.co.uk gehört natürlich nicht zur selben Domäne wie Rechner2.company2.co.uk, die Cookies werden aber dennoch an diesen geschickt.

Cookies sollten also niemals grundsätzlich aktiviert, sondern entweder ganz deaktiviert oder mit den Option »nur an den sendenden Rechner zurückschicken« aktiviert werden.

Ein weiterer Vorteil von HTML-Dokumenten ist die Angabe von URLs (Uniform Resource Locator), Adressen, auf denen weitere Informationen enthalten sind. Dies müssen aber nicht weitere HTML-Dokumente sein, sondern sie können auch jedes weitere beliebige Datenformat enthalten. Ein URL enthält folgende Informationen:

- das zu benutzende Protokoll, um auf die entsprechende Information zugreifen zu können,
- die genaue Internet-Adresse des Servers mit Angabe der Portnummer,
- Pfad und Dateinamen, an dem die Information gespeichert ist.

Durch diese Angaben ist es ohne weiteres möglich, innerhalb einer WWW-Seite zu anderen Diensten der Anwendungsebene, z. B. FTP, Telnet, E-Mail usw., zu wechseln, um die entsprechenden Dienste auszuführen.

Ein Firewall-System, das dem Schutz eines Netzes dient, muss in der Lage sein, die Befehle eines HTTP-Paketes zu analysieren und durch Filter einzuschränken. Die übertragenen Daten müssen unterschieden und auf bestimmte Informationen untersucht werden können.

3.6.12 NNTP

Das Internet bietet durch seine enorme Größe eine Fülle von unterschiedlichen Informationen. Da die Entwicklung auf fast allen Wissensgebieten schnell fortschreitet, ist man darauf angewiesen, ständig auf dem neuesten Wissensstand zu sein. Eine Möglichkeit dazu bieten die so genannten Newsserver.

Manche Newsserver haben sich wegen der Vielzahl an Informationen auf bestimmte Themengebiete spezialisiert.

Um die Newsserver ständig auf dem aktuellen Stand zu halten, tauschen diese untereinander in regelmäßigen Abständen neu eingegangene Beiträge aus. Innerhalb des Internets erfolgt dieser Datenaustausch mittels eines eigenständigen Protokolls. Das Network News Transfer Protocol (NNTP) wird benutzt, um neue Beiträge an den nächsten Newsserver zu versenden. Dieser überträgt die aktuellen Informationen dann weiter zum nächsten usw. Diesen Vorgang bezeichnet man als »News Feed«. Da einige dieser Server die Informationen nicht nur an einen,

neuKap03.fm Seite 80 Freitag, 18. Oktober 2002 3:50 15

sondern gleich an mehrere Server weiterleiten, kann sich eine neue Information innerhalb weniger Tage innerhalb des gesamten Internets ausgebreitet haben.

Das heute benutzte NNTP-Protokoll verfügt über einen Mechanismus, mit dem es möglich ist, nur jene Artikel zu übertragen, die auf dem Rechnersystem des Empfängers noch nicht vorhanden sind.

neuKap04.fm Seite 81 Freitag, 18. Oktober 2002 3:51 15

Kapitel 4

Bedrohungen im Netz

Im folgenden Kapitel werden die potenziellen Bedrohungen, die in Netzen wie dem Internet und in Intranets wirken, beschrieben. Außerdem werden gezielte Angriffe dargestellt, die auf der TCP/IP-Technologie beruhen, und prinzipielle Möglichkeiten, diesen mithilfe von Firewall-Systemen entgegenzuwirken.

4.1 Angriffsmöglichkeiten in Kommunikationssystemen

Die stärksten Bedrohungen der IT-Systeme zielen auf das Kommunikationssystem, d.h. auf die Nachrichten, die über Kommunikationssysteme wie Internet und Intranet ausgetauscht werden. Zunächst werden die verschiedenen Angriffsarten definiert und anschließend die Schäden kategorisiert, die durch Angriffe entstehen können.

Auf eine Nachricht (ein oder mehrere IP-Pakete) reagiert ein Empfänger mit einem bestimmten Verhalten (Abb. 4.1).

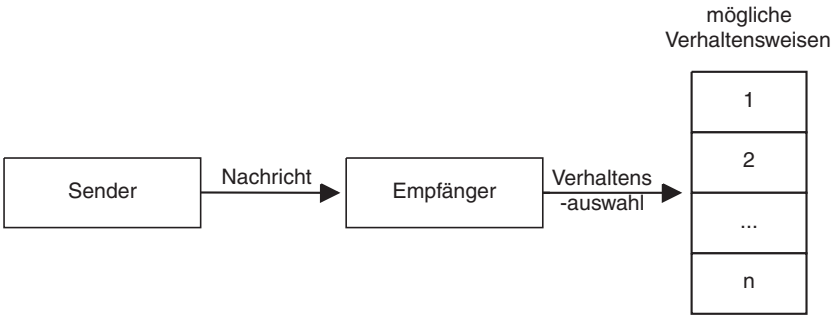


Abb. 4.1: Reaktionsmöglichkeiten des Empfängers einer Nachricht

Ein Angreifer, der die Kommunikationsverbindung abhört, kann das Verhalten des Empfängers und des Senders interpretieren. Der Angreifer kann die Reaktionen des Empfängers zielgerichtet beeinflussen, wenn er die Möglichkeit hat, die Nachricht zu wiederholen, zu verändern, zu löschen oder zu ergänzen.

Aus dieser Überlegung heraus werden grundsätzlich zwei Bedrohungsarten unterschieden: passive Angriffe und aktive Angriffe.

neuKap04.fm Seite 82 Freitag, 18. Oktober 2002 3:51 15

4.1.1 Passive Angriffe

Bei passiven Angriffen werden die übertragenen Nachrichten und der Betrieb des Kommunikationssystems nicht geändert. Passive Angriffe sind Bedrohungen, die vom Angreifer bewusst und gezielt durchgeführt werden, um sich unerlaubt Informationen zu beschaffen.

Passive Angriffe können z. B. mit Klemmen oder Induktionsschleifen an der Leitung oder durch das Abfangen der Signale von Richtfunk und Satellitenverbindungen durchgeführt werden.

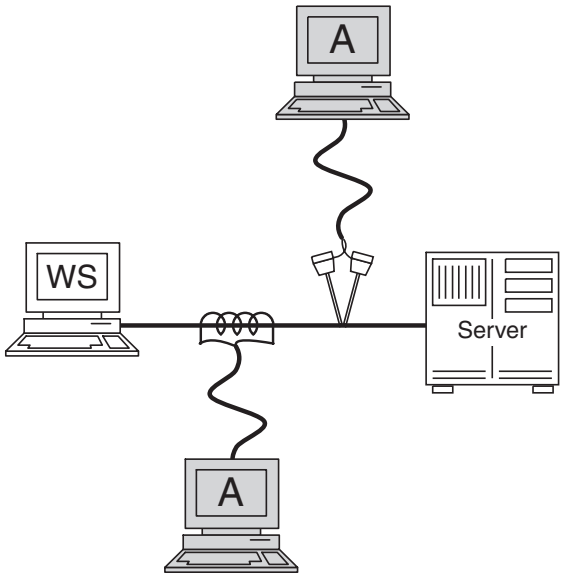


Abb. 4.2: Passive Angriffe auf Nachrichten oder auf das Kommunikationssystem

Wir unterscheiden folgende passive Angriffsarten:

- Abhören von Daten
  Ein Abhörer gelangt unmittelbar in den Besitz der Nachricht und kann sie zu seinem Zweck verwerten. Zum Beispiel kann ein Angreifer bei einer IP-Verbindung zwischen einem Telnet Server und einem Telnet-Client während der LogIn-Prozedur die Identität und das Passwort eines Teilnehmers abhören und später mit diesem Passwort unerlaubt Zutritt zum Server-System erlangen. Weitere Beispiele sind das Abhören von vertraulichen Informationen, wie Entwicklungsunterlagen von neuen Produkten, oder das Abhören von Daten, die unter das Datenschutzgesetz fallen. Diese Angriffe sind bei der Verwendung von frei zugänglichen LAN-Anschlüssen problemlos durchführbar.

neuKap04.fm Seite 83 Freitag, 18. Oktober 2002 3:51 15

- Abhören der Teilnehmer-Identitäten
  Der Lauscher erfährt, welche Teilnehmer (Benutzer oder Rechnersysteme) untereinander eine Datenverbindung aufbauen und Daten austauschen. Allein aus der Kenntnis, wer mit wem zu welchem Zeitpunkt Nachrichten ausgetauscht hat, sind oft Rückschlüsse auf den Inhalt der Nachricht oder das Verhalten der Teilnehmer möglich. Wenn z. B. jemand auf die WWW-Seiten eines Waschmaschinenherstellers zugreift, kann man vermuten, dass er eine Waschmaschine kaufen will.

- Verkehrsflussanalyse
  Auch wenn die Daten verschlüsselt sind, ist es einem Abhörer möglich, durch eine »Verkehrsflussanalyse« gewisse Informationen zu erhalten, wie z. B. Größenordnungen, Zeitpunkte, Häufigkeit und Richtung des Datentransfers. Diese Informationen können für bestimmte spezielle Anwendungen interessant sein, z. B. für Börsen-Transaktionen oder militärische Operationen.

Spezielle Gefahren beim Einsatz lokaler Netze

Besonderen passiven Angriffen sind lokale Netze ausgesetzt, da sie im allgemeinen Broadcastmedien verwenden, d. h., dass alle Nachrichten an alle Teilnehmer gesendet werden und davon ausgegangen wird, dass die Teilnehmer nur die Nachrichten verwenden, die für sie bestimmt sind. In der Praxis werden zusätzliche Steckdosen eingerichtet, um flexibel für Umzüge, zusätzliche Rechnersysteme etc. zu sein. Diese zusätzlichen Steckdosen sind nicht blockiert, solange sie nicht benutzt werden, und können daher jederzeit missbraucht werden, um Analysegeräte anzuschließen und den gesamten Nachrichtenstrom mitzuverfolgen.

Lokale Netze sind aber auch so konzipiert, dass im laufenden Betrieb zusätzliche Steckdosen und Rechnersysteme montiert werden können, ohne den Verkehr zu stören. Diese Flexibilität und Robustheit ist aus Sicht der Datensicherheit von Nachteil. Beide Gefahren beinhalten das unbefugte, unbemerkte Anschließen zusätzlicher Rechnersysteme. Aber auch die Stationen befugter Teilnehmer können dazu verwendet werden, den gesamten Nachrichtenstrom abzuhören.

Mit einfachen Hilfsmitteln wie Protokollanalysatoren (z. B. LAN-Watch) können möglicherweise von jedem Rechnersystem im LAN alle Pakete mitgelesen werden.

Da viele Organisationen die Systemadministration der Rechnersysteme remote durchführen, können »root«-Passworte mitgelesen werden, mit deren Hilfe weitere Angriffe durchgeführt werden können.

Protokollmitschnitt einer Telnet-Session

Im folgenden Protokollmitschnitt einer Telnet-Session ist die Phase des Login festgehalten. Die Software, die den Protokollmitschnitt realisiert hat, kann auf jedem normalen PC laufen, der ans LAN angeschlossen ist. An das Rechnersystem, mit

neuKap04.fm Seite 84 Freitag, 18. Oktober 2002 3:51 15

dem der Mitschnitt durchgeführt wurde, werden keine besonderen Anforderungen gestellt.

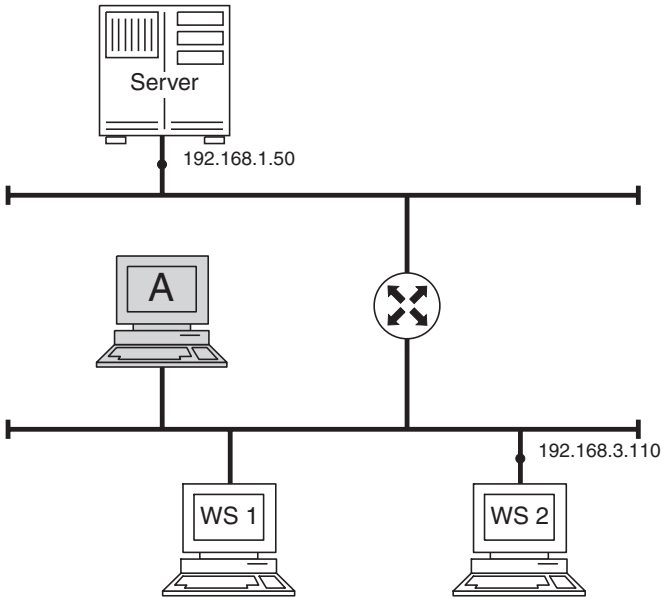


Abb. 4.3: Passiver Angriff mithilfe eines Protokollanalysators

Der Benutzer der Workstation 2 hat ein Login mit dem Server durchgeführt. Als Benutzeridentifikation wurde »Nutzer1« eingegeben. Diese Eingabe wurde vom Server zur Kontrolle zurückgesendet, aus diesem Grund sind die einzelnen Buchstaben doppelt im Protokollmitschnitt zu sehen. Das Passwort, das der Benutzer »Nutzer1« verwendet hat, lautet »1beutlin« (siehe Tab. 4.1). Die Buchstaben des Passworts werden vom Server nicht zurückgesendet, sodass sie nur einmal zu sehen sind (diese Eigenschaft erleichert die Suche nach dem Passwort in Protokollmitschnitten). Wenn dieses Programm morgens verwendet wird, während sich alle Mitarbeiter an diesem Server einloggen, können alle Passworte festgehalten werden.

Es muss betont werden, dass mangelhafte Vertraulichkeit ein großes Problem beim Betrieb lokaler Netze ist, da hiermit auch die mangelhafte Sicherheit der üblichen Zugangs- und Zugriffskontrollen auf Server-Systeme und jegliche Betriebsmittel im lokalen Netz zusammenhängt.

Weitere Gefahrenpunkte in lokalen Netzen, an denen Nachrichten abgehört werden können, sind Brücken, Router und Brouter sowie Gateways.

neuKap04.fm Seite 85 Freitag, 18. Oktober 2002 3:51 15

Ziel	Quelle	Nachricht
192.168.3.110	192.168.1.50	Telnet :logIn:
192.168.1.50	192.168.3.110	Telnet :n
192.168.3.110	192.168.1.50	Telnet :n
192.168.1.50	192.168.3.110	Telnet :u
192.168.3.110	192.168.1.50	Telnet :u
192.168.1.50	192.168.3.110	Telnet :t
192.168.3.110	192.168.1.50	Telnet :t
192.168.1.50	192.168.3.110	Telnet :z
192.168.3.110	192.168.1.50	Telnet :z
192.168.1.50	192.168.3.110	Telnet :e
192.168.3.110	192.168.1.50	Telnet :e
192.168.1.50	192.168.3.110	Telnet :r
192.168.3.110	192.168.1.50	Telnet :r
192.168.1.50	192.168.3.110	Telnet :1
192.168.3.110	192.168.1.50	Telnet :1
192.168.1.50	192.168.3.110	Telnet :.
192.168.3.110	192.168.1.50	Telnet :..
192.168.3.110	192.168.1.50	Telnet :Password:
192.168.1.50	192.168.3.110	Telnet :1
192.168.1.50	192.168.3.110	Telnet :b
192.168.1.50	192.168.3.110	Telnet :e
192.168.1.50	192.168.3.110	Telnet :u
192.168.1.50	192.168.3.110	Telnet :t
192.168.1.50	192.168.3.110	Telnet :l
192.168.1.50	192.168.3.110	Telnet :i
192.168.1.50	192.168.3.110	Telnet :n
192.168.1.50	192.168.3.110	Telnet :.
192.168.3.110	192.168.1.50	Telnet :..
192.168.3.110	192.168.1.50	Telnet :Last logIn: Tue Apr 29 14:05:20 from merry..

Tabelle 4.1: Mitschnitt einer Telnet-Sitzung

4.1.2 Aktive Angriffe

Neben der Gefahr, abgehört zu werden, besteht die Möglichkeit von aktiven Angriffen, die den Nachrichtenstrom und/oder den Betrieb der Kommunikation verfälschen. Aktive Angriffe werden z. B. durch Auftrennen der Übertragungsleitungen oder mithilfe der Emulation von Übertragungsprotokollen durchgeführt.

neuKap04.fm Seite 86 Freitag, 18. Oktober 2002 3:51 15

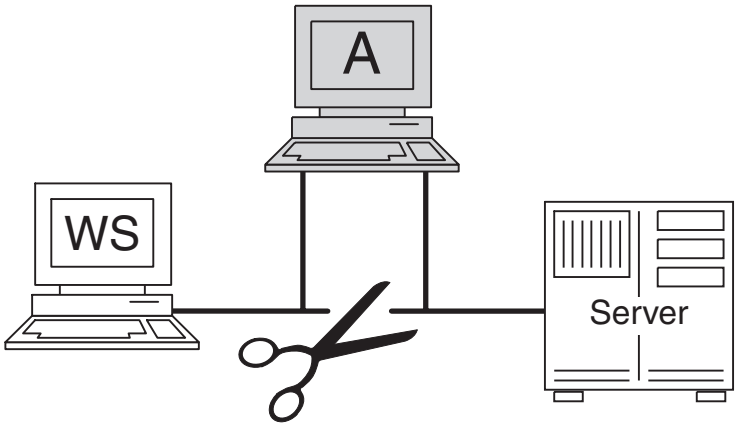


Abb. 4.4: Aktive Angriffe

Bei »Aktiven Angriffen« wird grob unterschieden zwischen Bedrohungen durch Dritte und Bedrohungen durch den Kommunikationspartner.

Bedrohungen durch Dritte sind z. B.:

- Wiederholen oder Verzögern von Informationen
  Durch Wiederholen oder Verzögern von Informationen kann der Empfänger irritiert oder zu einer falschen Aktion veranlasst werden. Beispiel: Mehrfache Überweisung eines Geldbetrages oder Wiederholung eines abgefangenen LogIns.
- Einfügen und Löschen bestimmter Daten
  Um ein System zu manipulieren, fügt ein Angreifer bestimmte Nachrichten oder Daten innerhalb der Nachrichten ein oder löscht sie. Ein Empfänger kann durch Unterdrückung oder zusätzlichen Empfang entscheidender Informationen zu einem falschen Verhalten veranlasst werden. Beispiel: In der E-Mail »Kaufen Sie *keinesfalls* neue Aktien« wird das Wort *»keinesfalls«* während der Übertragung gelöscht, sodass der Empfänger die Instruktion »Kaufen Sie neue Aktien« erhält.
- Modifikation von Daten
  Modifikation von Daten bedeutet, dass die Veränderung der Daten von den Kommunikationspartnern nicht erkannt wird. Durch Ändern der Daten während der Datenübertragung ist es dem Angreifer möglich, falsche Aktionen zu veranlassen /PoRi95/. Beispiel: Die Veränderung einer Kontonummer bei einer Geldüberweisung führt dazu, dass ein anderer als der intendierte Empfänger das Geld bekommt.

neuKap04.fm Seite 87 Freitag, 18. Oktober 2002 3:51 15

- Boykott des Kommunikationssystems (Denial of Service)
  Wenn der Umfang von eingefügten oder unterdrückten Daten zu groß wird oder realzeitorientierte Daten zu lange verzögert werden, kann hierdurch das gesamte Kommunikationssystem boykottiert werden. Beispiel: Durch permanenten Verbindungsaufbau zu einem bestimmten Server kann dieser blockiert und isoliert werden.

Bedrohungen durch den Kommunikationspartner sind z. B.:

- Vortäuschung einer falschen Identität (Maskerade-Angriff)
  Wenn sich ein Teilnehmer für einen anderen ausgibt, kann er sich Informationen erschleichen, die für diesen anderen Teilnehmer bestimmt waren, oder Aktionen auslösen, die nur der andere Teilnehmer veranlassen darf. Beispiel: Ein Teilnehmer verschafft sich unerlaubt Zugang zur einer Datenbank.

- Leugnen einer Kommunikationsbeziehung
  Der steigende Einsatz von Datenkommunikation zur Abwicklung vertraglich relevanter Vorgänge erfordert, dass sowohl der Sender einer Nachricht nicht leugnen kann, der Sender zu sein, als auch der Empfänger nicht abstreiten kann, die Nachricht erhalten zu haben.

  Beispiele:
  Bestellung von Waren über das Internet bei einem Händler oder Abschluss von Verträgen über das Internet.

Trittbrettfahrer (Man in the middle)

So genannte Trittbrettfahrer hängen sich z. B. an einen Knoten (Router oder Rechnersystem) im Internet und verfolgen einen Verbindungsaufbau mit. Die Verbindung wird dann nach der Authentikation des Benutzers für eigene Zwecke genutzt. Mit dieser Methode können Rechnersysteme, auf die eigentlich kein Zugriff möglich ist, manipuliert und Authentikationsprozesse (auch kryptographische Methoden) unterlaufen werden.

Beschreibung eines Angriffs

Der Benutzer der Workstation 1 möchte einen Dienst des Servers X im Internet nutzen. Dazu baut der Benutzer eine Verbindung zum Server X auf und führt dort den notwendigen LogInvorgang (Identifikation und Authentikation) durch. Ein Angreifer (Rechnersystem A), der sich aktiv in die Kommunikationsverbindung im Internet eingeklinkt hat, verfolgt diese Prozedur und wartet, bis der Server die Bestätigung des erfolgreichen Login sendet. Diese Bestätigung gibt er nicht an die Workstation 1 weiter, sondern sendet z. B. einen Verbindungsabbau. Der Angreifer trennt die Workstation 1 ab, ohne dass diese den Angriff »bemerkt«. Nun kann der Angreifer die authentisierte Verbindung als Trittbrettfahrer für sich und seine Ziele nutzen (siehe Abb. 4.5). Diese Angriffsmethode kann auch bei kryptographischen Authentikationsverfahren durchgeführt werden.

neuKap04.fm Seite 88 Freitag, 18. Oktober 2002 3:51 15

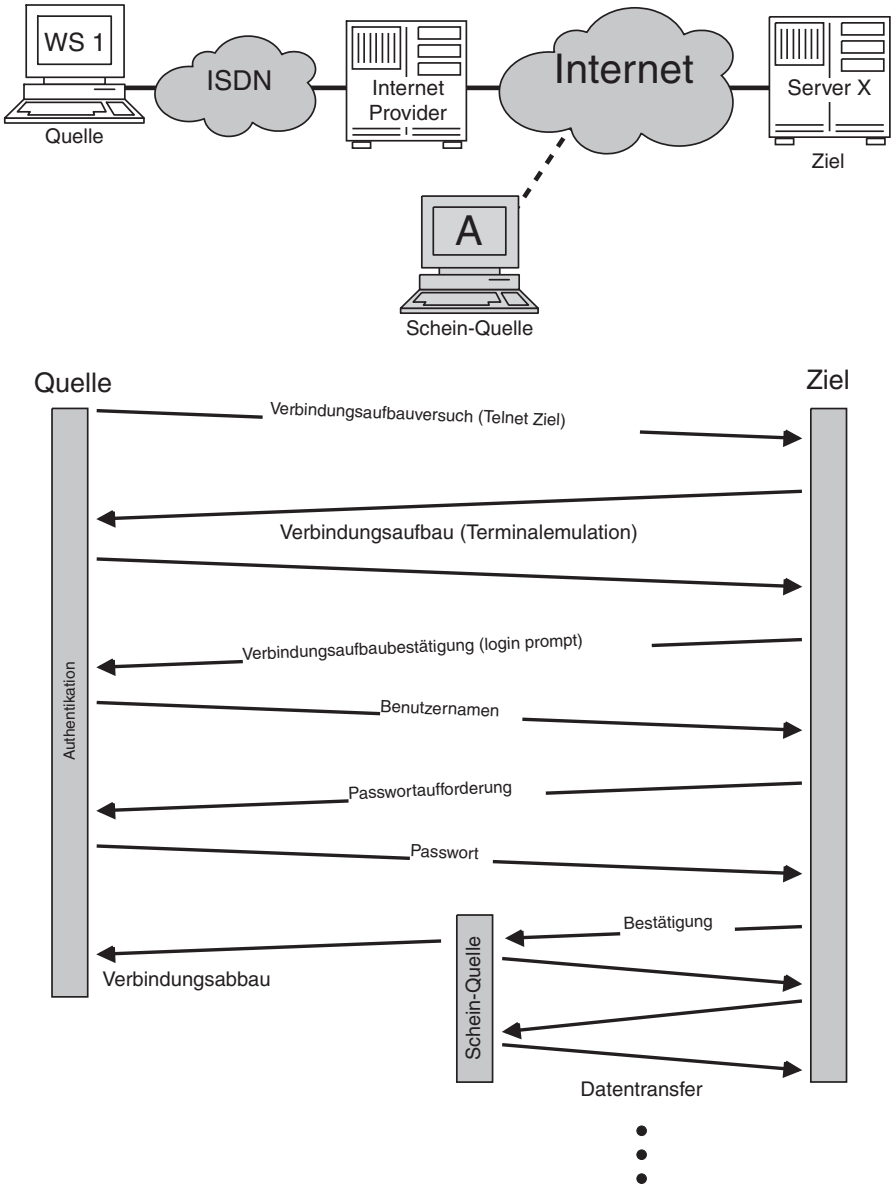


Abb. 4.5: Trittbrettfahrer

4.1.3 Zufällige Verfälschungsmöglichkeiten

Neben den Gefahren, die Kommunikationssystemen durch absichtliche passive und aktive Angriffe drohen, gibt es auch unbeabsichtigte Verfälschungsmöglichkeiten.

neuKap04.fm Seite 89 Freitag, 18. Oktober 2002 3:51 15

Unbeabsichtigte Verfälschungsmöglichkeiten sind z. B.:

- Fehlrouting von Informationen
  In den Routern im Internet/Intranet können Informationen auf einen falschen Weg geraten und an einen fremden Teilnehmer ausgeliefert werden. Ein solches Fehlrouting kann bereits beim Verbindungsaufbau erfolgen, sodass die Verbindung zu einem falschen Teilnehmer hergestellt wird.

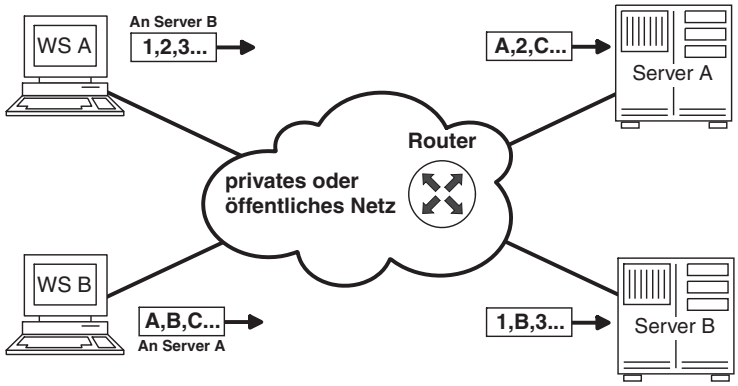


Abb. 4.6: Fehlrouting von Informationen

- Übertragungsfehler
  Übertragungsfehler können durch Übersprechen von Nachbarkanälen oder durch Wählgeräusche verursacht werden. Die Bitfehlerwahrscheinlichkeiten bei Datenübertragungswegen liegen zwischen 10^{-4} bis 10^{-7}. Auch hier können Fehler bei der Kommunikation über TCP/IP-basierte Netze auftreten, die sicherheitskritisch sind.

- Software-Fehler
  99 % aller Software ist nicht verifiziert. Das bedeutet, dass in allen Software-Paketen Fehler sind, die in bestimmten Situationen zu Fehlreaktionen führen können.

  Beispiel: Die Software wählt durch einen internen Fehler einen falschen Teilnehmer an und sendet diesem vertrauliche Daten.

- Hardware-Fehler durch Umwelteinflüsse
  Umwelteinflüsse wie die elektromagnetische Emission können mit einem bestimmten Wahrscheinlichkeitsgrad die Ursache dafür sein, dass in einem Rechnersystem Bits umkippen, wodurch ein falsches Verhalten zu erwarten ist. Beispiel: Durch das Umkippen eines Bits (z. B. im Router) wird ein vertrauliches IP-Paket auf einem anderen logischen Kanal zu einem anderen Teilnehmer gesendet.

neuKap04.fm Seite 90 Freitag, 18. Oktober 2002 3:51 15

- Fehlbedienung
  Der Benutzer löst versehentlich Aktionen aus, die er nicht auslösen wollte.

  Beispiel: Der Benutzer wählt aus Versehen einen anderen Teilnehmer an und sendet diesem vertrauliche Informationen.

Fazit: Zufällige Verfälschungsmöglichkeiten können wie aktive Angriffe praktisch nicht verhindert werden. Wenn wir sie aber kennen und beim Aufbau unserer Kommunikationssysteme berücksichtigen, können wir den möglichen Schaden begrenzen.

4.2 Weitere Aspekte potenzieller Bedrohungen bei der Kommunikation über das Internet

In Deutschland gilt für alle Anbieter von Telekommunikationsdienstleistungen das Fernmeldegeheimnis. Dies bedeutet, dass Anbieter von Telekommunikationsdienstleistungen darlegen müssen, wie ihre Kommunikationssysteme (Knoten, Netzwerkmanagement usw.) abgesichert werden, um eine Manipulation von außen zu verhindern. Daher kann davon ausgegangen werden, dass im Fall einer Kommunikation über Netze in Deutschland und in anderen europäischen Ländern von den Telekommunikationsdienstleistern ein hohes Maß an Sicherheit gewährleistet wird.

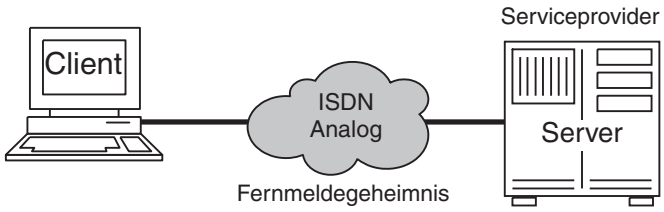


Abb. 4.7: Fernmeldegeheimnis

Beim Anschluss an das Internet, in dem die Kommunikation über Provider möglicherweise sogar weltweit weitergeleitet wird, verlassen wir diesen geschützten Bereich, da in anderen Ländern Vorschriften bezüglich des Fernmeldegeheimnisses nicht oder in nicht ausreichender Form existieren. Es kann also nicht davon ausgegangen werden, dass außerhalb Deutschlands der gleiche rechtliche und technische Schutz gewährleistet ist.

Kommunikationswege der IP-Pakete im Internet

Da z. B. Mails unter Umständen über viele Netzknoten geleitet werden, worauf die Benutzer keinen Einfluss haben, ist ein organisierter Angriff nicht zu unterschätzen.

neuKap04.fm Seite 91 Freitag, 18. Oktober 2002 3:51 15

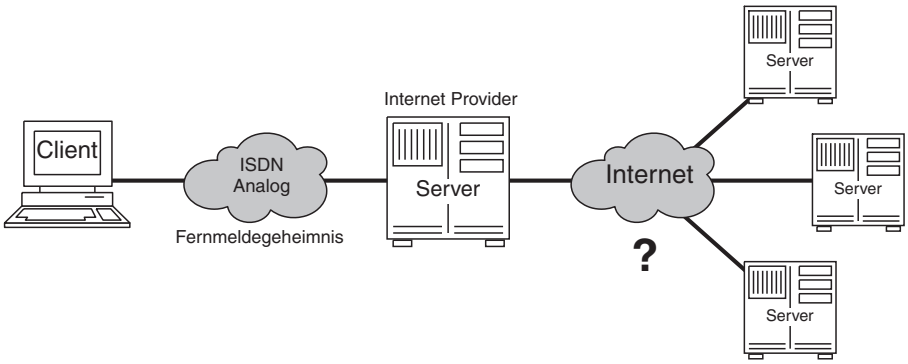


Abb. 4.8: Internet und das Fernmeldegeheimnis

Die Abbildung 4.9 zeigt, welchen »abenteuerlichen« Weg die IP-Pakete einer Mail genommen haben, die von der Utimaco-Niederlassung Aachen zu einem Institut der RWTH gesendet wurde, das nur 3 Kilometer entfernt liegt.

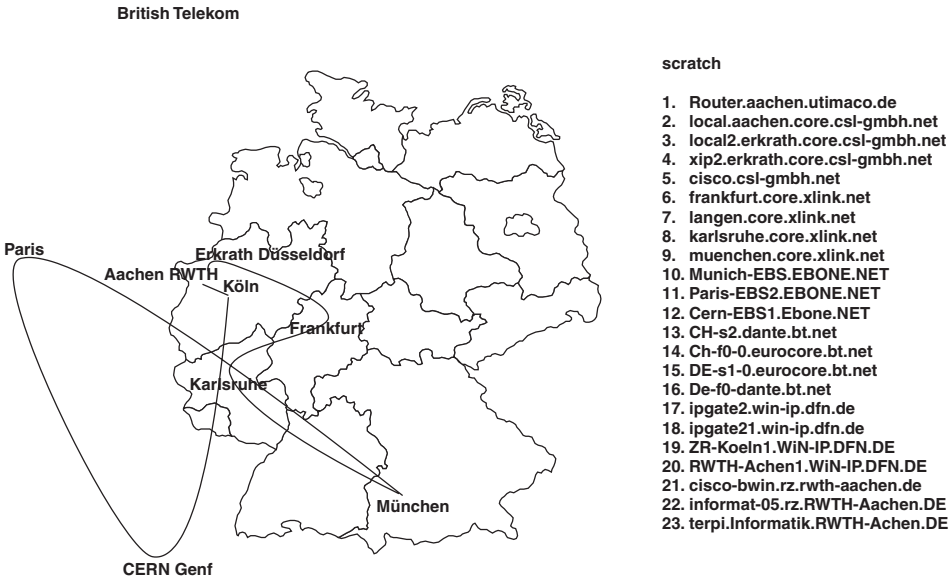


Abb. 4.9: Weg der IP-Pakete einer Mail

Diese Mail ist über 23 Router gelaufen, die sie empfangen und weitergesendet haben. Hierbei handelt es sich um ein harmloses Beispiel. Abhängig vom jeweiligen Internet-Provider werden manche IP-Pakete sogar über die USA geroutet.

neuKap04.fm Seite 92 Freitag, 18. Oktober 2002 3:51 15

4.2.1 Angriffstools aus dem Internet

Im Internet sind eine Reihe von Tools (z. B. ISS, SATAN) abrufbar, mit denen auf TCP/IP-Technologie basierenden Systemen eine Analyse der Netzschwachstellen, aber auch gezielte Angriffe möglich sind. Mithilfe dieser Tools kann jeder Benutzer, auch wenn er nicht über spezielles Fachwissen verfügt, solche Angriffe durchführen.

4.2.2 Implementierungsfehler in Anwendungen und fehlerhafte Konfigurationen

Anwendungen wie »sendmail« wiesen in der Vergangenheit Implementierungsfehler auf, die es ermöglichten, auf einem entfernten IT-System beliebige privilegierte Kommandos auszuführen. Mithilfe dieser privilegierten Kommandos wurden dann Angriffe durchgeführt.

Für jeden Dienst, der über einen Netzzugang ermöglicht werden soll, existiert ein Daemon-Prozess, der falsch konfiguriert oder fehlerhaft sein kann, wodurch wiederum Angriffe durchgeführt werden können /CERT95/.

4.3 Wie hoch ist das Risiko?

Bei der Betrachtung der oben dargestellten potenziellen Bedrohungen stellt sich die Frage, wie groß die Eintrittswahrscheinlichkeit von Angriffen ist. Bei der Einschätzung des Angriffsrisikos spielen drei Faktoren eine wesentliche Rolle: Die lokalen Gegebenheiten, der Wert bzw. die Verwertbarkeit der Daten und die Frage, wie hoch technischer und materieller Aufwand für einen Angreifer sind.

In Bürogebäuden mit mehreren Firmen verlaufen die Datenleitungen oft durch die Räumlichkeiten anderer Firmen, oder sie sind im Hausanschlussraum für jedermann zugänglich. Daher ist es kein Problem, eine geeignete Stelle zu finden, an der die Datenleitung angezapft werden kann (Abb. 4.10).

Mögliche Angriffspunkte liegen auf den Fluren, in Kabelschächten, in der Tiefgarage und an den Einspeisungspunkten von Versorgungsunternehmen, z. B. den Telefonanschlusskästen, die oft gleich neben den frei zugänglichen Mülltonnen stehen. Die leichte und für potenzielle Angreifer relativ risikolose Zugänglichkeit der Datenleitungen erhöht die Gefahr, besonders dann, wenn der Wert der Daten einen Angriff auf das Rechnersystem lohnenswert erscheinen lässt.

Technisch ist das Anzapfen solcher Leitungen selbst für Laien kein Problem. Die Kosten für ein Analysegerät, mit dem die Kommunikationsdaten intelligent analysiert werden können, liegen zwischen 2 500 EUR und 5 000 EUR. Außerdem stehen im Internet zunehmend kostenlose Angriffstools zur Verfügung, mit denen intelligente Angriffe auf Rechnersysteme durchgeführt werden können.

neuKap04.fm Seite 93 Freitag, 18. Oktober 2002 3:51 15

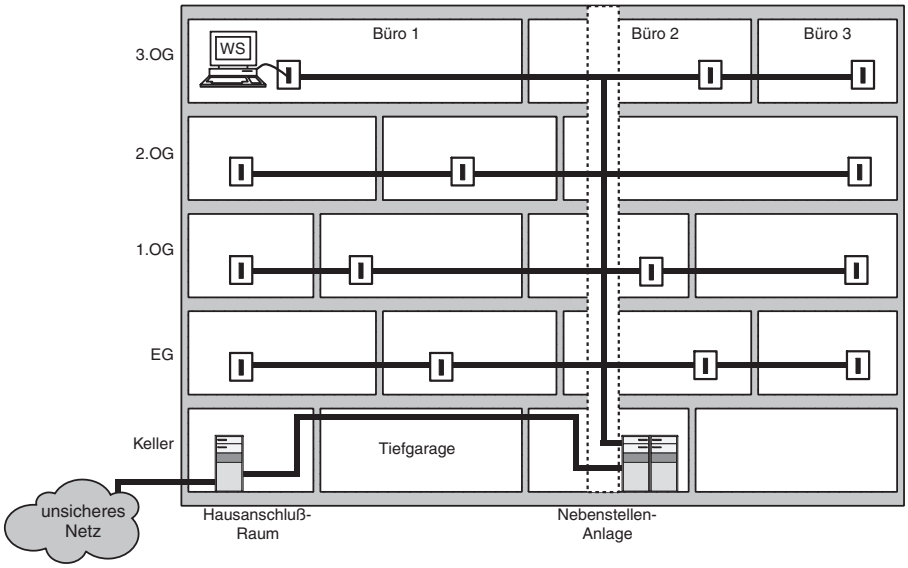


Abb. 4.10: Lokale Gegebenheiten, die das Angriffsrisiko erhöhen

Fazit:

Die jeweiligen lokalen Gegebenheiten, die technische Machbarkeit und die relativ niedrigen Beschaffungskosten für Analysegeräte machen das Angriffsrisiko sehr hoch, besonders wenn der Angreifer sich davon ein lohnendes Geschäft versprechen kann.

Seit Jahren wächst der Bereich Computerkriminalität überdurchschnittlich, siehe Kapitel 16, *Computerkriminalität – Fakten und Zahlen*. Da in den nächsten Jahren immer mehr Geschäftsprozesse über Rechner- und Kommunikationssysteme abgewickelt werden, wird dieser Trend anhalten, wenn keine angemessenen Sicherheitsmaßnahmen eingeführt werden.

4.4 Schadenskategorien und Folgen

Um mögliche Schäden besser einschätzen zu können, werden nachfolgend einige typische Schadenskategorien erläutert /BSI99/. Diese beziehen sich auf die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit.

4.4.1 Verstoß gegen Gesetze/Vorschriften/Verträge

Verstöße dieser Art können aus dem Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit resultieren. Die Schwere eines solchen Schadens ist dabei oftmals abhängig davon, ob es sich nur um einen Bagatellverstoß handelt, oder ob aus

neuKap04.fm Seite 94 Freitag, 18. Oktober 2002 3:51 15

dem Vorgang rechtliche Konsequenzen für die Organisationen entstehen können. Zu den relevanten Gesetzen, Vorschriften und Verträgen gehören:

- Grundgesetz
- Bürgerliches Gesetzbuch
- Strafgesetzbuch (2. Wirtschaftskriminalitätsgesetz)
- Bundesdatenschutzgesetz und Datenschutzgesetze der Länder
- Sozialgesetzbuch
- Handelsgesetzbuch
- Personalvertretungsgesetz
- Betriebsverfassungsgesetz
- Urheberrechtsgesetz
- Patentgesetz
- Produkthaftungsgesetz
- Organisationsanweisungen und Dienstvorschriften
- Dienstleistungsverträge im Bereich Datenverarbeitung
- Verträge, die die Wahrung von Betriebsgeheimnissen vereinbaren
- Betriebsvereinbarungen
- EU-Recht
- Völkerrecht, bi- und multilaterale Abkommen

4.4.2 Beeinträchtigung der persönlichen Unversehrtheit

Die Fehlfunktion eines Rechnersystems kann unmittelbar die Verletzung, die Invalidität oder den Tod von Personen nach sich ziehen. Die Höhe des Schadens ist am direkten persönlichen Schaden zu messen.

Beispiel:

- Verletzung einer Person durch Fehlfunktionen einer Produktionsmaschine nach einer Software-Manipulation über das Internet

4.4.3 Beeinträchtigung der Aufgabenerfüllung

Gerade der Verlust der Verfügbarkeit eines Rechnersystems oder der Integrität von Daten kann die Aufgabenerfüllung in einer Organisation erheblich beeinträchtigen. Die Schwere des Schadens richtet sich hierbei nach der zeitlichen Dauer der Beeinträchtigung und nach dem Umfang der Einschränkungen der angebotenen Dienstleistungen.

Beispiele:

- verzögerte Bearbeitung von Verwaltungsvorgängen
- verspätete Lieferung aufgrund verzögerter Bearbeitung von Bestellungen
- falsche Liefermenge aufgrund falscher Steuerungsdaten
- unzureichende Qualitätssicherung durch Ausfall eines Messsystems

neuKap04.fm Seite 95 Freitag, 18. Oktober 2002 3:51 15

4.4.4 Negative Außenwirkung

Durch den Verlust eines Grundwertes in einem Rechnersystem können verschiedene negative Außenwirkungen entstehen, z. B.:

- Renommeeverlust einer Organisation,
- Beeinträchtigung der wirtschaftlichen Beziehungen zusammenarbeitender Organisationen,
- Vertrauensverlust gegenüber einer Organisation,
- verlorenes Vertrauen in die Arbeitsqualität einer Organisation,
- Zuspielen vertraulicher Daten an die Presse oder die Konkurrenz,
- Einbuße der Konkurrenzfähigkeit.

Die Höhe des Schadens orientiert sich an der Schwere des Vertrauensverlustes und am Verbreitungsgrad der Außenwirkung.

Ursachen für solche Schäden können vielfältiger Natur sein:

- Handlungsunfähigkeit einer Organisation durch IT-Ausfall,
- fehlerhafte Veröffentlichungen durch manipulierte Daten,
- Fehlbestellungen durch mangelhafte Lagerhaltungsprogramme,
- Verstoß gegen die Schweigepflicht durch Vertraulichkeitsverlust von Daten.

Der mögliche Schaden durch eine negative Außenwirkung kann in vielen Organisationen sehr hoch sein.

4.4.5 Finanzielle Auswirkungen

Unmittelbare oder mittelbare finanzielle Schäden können durch den Verlust der Vertraulichkeit schutzbedürftiger Daten, die Veränderung von Daten oder den Ausfall eines Rechnersystems entstehen.

Beispiele:

- unerlaubte Weitergabe von Forschungs- und Entwicklungsergebnissen
- Manipulation finanzwirksamer Daten in einem Abrechnungssystem
- Ausfall eines IT-gesteuerten Produktionssystems und dadurch bedingte Umsatzverluste
- Einsichtnahme in Marketingstrategiepapiere oder Umsatzzahlen
- Produktionsstop aufgrund eines Rechnerausfalls

Die Höhe des Gesamtschadens wird bestimmt durch die direkt entstehenden finanziellen Schäden und die daraus resultierenden pekuniären Folgeschäden.

neuKap04.fm Seite 96 Freitag, 18. Oktober 2002 3:51 15

4.5 Angriffsmethoden und prinzipielle Gegenmaßnahmen auf der Grundlage der TCP/IP-Protokolle

Mithilfe der TCP/IP-Technologie ist im Prinzip jeder Benutzer in der Lage, mit jedem anderen eine Kommunikationsverbindung aufzunehmen. Hier verbergen sich viele Probleme, die mithilfe von Firewall-Systemen eingeschränkt oder verhindert werden können.

In diesem Abschnitt sollen mithilfe einiger Beispiele mögliche Angriffe auf Rechnersysteme in einem zu schützenden Netz dargestellt werden und welche prinzipiellen Möglichkeiten bestehen, den Angriffen mithilfe eines Firewall-Systems entgegenzuwirken.

4.5.1 Idee eines Angriffs

Ein Angreifer versucht gezielt und absichtlich, auf ein oder mehrere Rechnersysteme in einem zu schützenden Netz zuzugreifen, um

- an bestimmte Informationen zu gelangen, die nicht für ihn bestimmt sind,
- Aktionen auszulösen, die er nicht auslösen darf, oder
- Ressourcen zu nutzen, die er nicht nutzen darf.

Dies tut ein Angreifer,

- um mit den Informationen Geld zu verdienen (z. B. Entwicklungsdaten)
- oder ohne materielle Gewinnabsicht.

Letzteres hat Gründe, die meist in den Formenkreis »gestörte Persönlichkeit« fallen. Stichworte: um dem (Zufalls)-Opfer zu schaden, aus Zerstörungswut, ähnlich wie Vandalismus oder Brandstiftung (Nero-Syndrom); aus purer Langeweile (»just for fun«), bei Unterforderung an der Arbeitstätte, wie z. B. die bulgrischen Programmierer, die Virenprogramme schrieben; aus Geltungsbedürfnis, um fehlendes Selbstbewusstsein, fehlende Anerkennung oder versagte Liebe zu kompensieren; aus reiner Spielleidenschaft, bis hin zur Spielsucht und der Jagd nach dem ultimativen Hacking oder Virusprogramm, das seinen »Schöpfer« in die Schlagzeilen bringt, oft aus jugendlichem Übermut (»Script-Kiddies«, die »erprobte« Hack-Listings adaptieren), um fame (Ruhm) zu erlangen, ähnlich wie Sprayer, die traces (Spuren) legen und mit ihren tags (Zeichen) in einer uns unverständlichen Subkultur – hier: der »Hacker-Gemeinde« – leben; aus vorgeblich ideellen oder politischen Gründen (Kampf »gegen das Establishment« oder Intoleranz gegen bestimmte Weltanschauungen).

Im Folgenden werden einige Angriffe beschrieben, bei denen auf Rechnersysteme in einem zu schützenden Netz zugegriffen werden kann.

neuKap04.fm Seite 97 Freitag, 18. Oktober 2002 3:51 15

4.5.2 Analyse des Netzes mithilfe von Scannerprogrammen

Mit so genannten Scannerprogrammen ist ein Angreifer in der Lage festzustellen, aus welchen IP-Adressen (Rechnersystemen), welchen Benutzern und welchen Diensten das zu schützende Netz besteht.

Analyse des Netzes und der Rechnersysteme

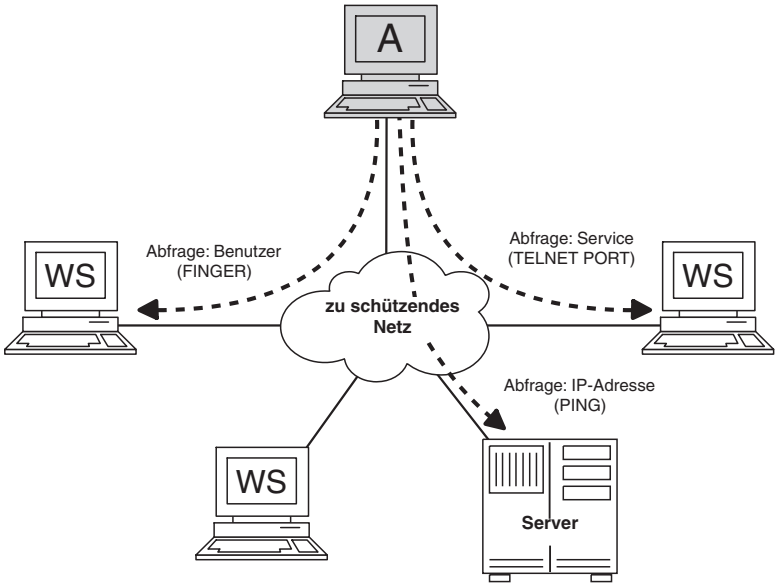


Abb. 4.11: Analyse des Netzes mithilfe von Scannerprogrammen

- Rechnersysteme: Die aktiven IP-Adressen eines Netzes können z. B. mithilfe des »ping«-Befehls analysiert werden. Ein Angreifer sendet den »ping«-Befehl an alle möglichen IP-Adressen eines Adressbereiches. Bei einem Klasse-C-Netz bedeutet dies, es wird an die IP-Adresse A.B.C.1 bis A.B.C.254 ein »ping«-Befehl gesendet. An den empfangenen Antworten kann abgelesen werden, hinter welcher IP-Adresse sich ein real angeschlossenes Rechnersystem befindet.
- aktive Benutzer: Mit dem Befehl »finger« ist ein Angreifer in der Lage, festzustellen, welche Benutzer zum jeweiligen Zeitpunkt an einem bestimmten Rechnersystem aktiv sind, ob sie schon die empfangenen Mails gelesen haben usw.
- aktive Dienste: Durch Ansprechen der einzelnen Ports kann ein Angreifer analysieren, für welche Dienste ein Daemon-Prozess auf dem entsprechenden Rechnersystem installiert ist.

neuKap04.fm Seite 98 Freitag, 18. Oktober 2002 3:51 15

- Schwachstellenanalyse auf den einzelnen Rechnersystemen: Mit weiteren Hilfsprogrammen (z. B. »ISS«, »SATAN«) kann dann der Angreifer gezielt eine Schwachstellenanalyse durchführen. Hier wird überprüft, ob z. B. durch Konfigurationsfehler der Daemon-Prozesse der aktiven Dienste oder die Verwendung fehlerhafter alter Versionen ein Angriff auf das Rechnersystem möglich ist.

Ausnutzung der festgestellten Schwachstellen

Der nächste Schritt des Angreifers ist die konsequente Ausnutzung der festgestellten Schwachstellen.

Wie kann ein Firewall-System helfen?

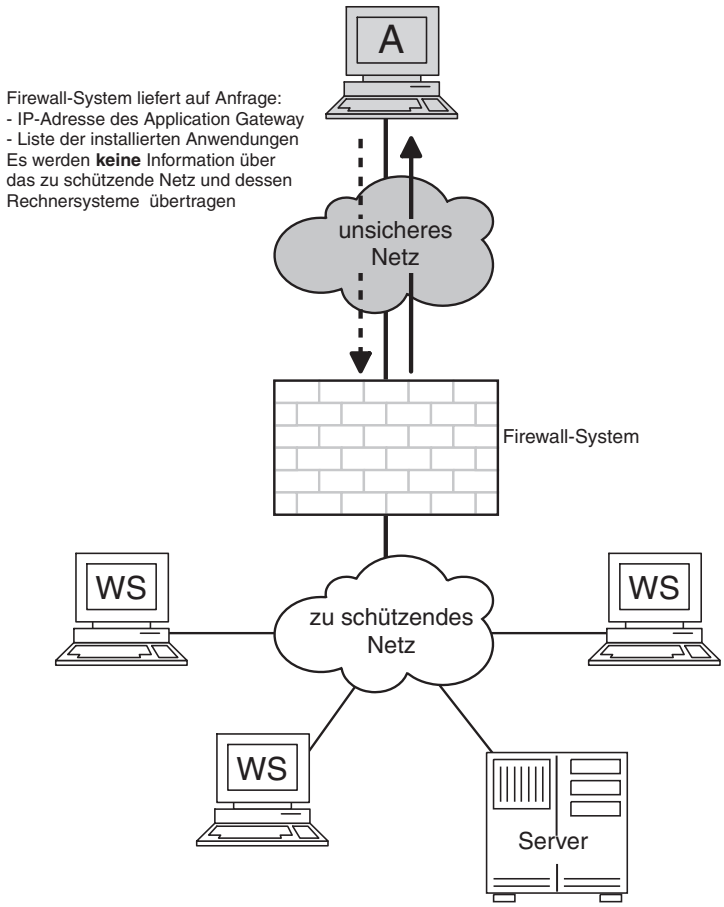


Abb. 4.12: Firewall-System mit dem Sicherheitsdienst »Verbergen der internen Netzstruktur«

neuKap04.fm Seite 99 Freitag, 18. Oktober 2002 3:51 15

Durch die Integration eines Firewall-Systems, das den Dienst »Verbergen der internen Netzstruktur« gewährleistet, kann die Analyse des zu schützenden Netzes verhindert werden. Ein Angreifer kann dann nur noch die IP-Adressen des Firewall-Systems analysieren und feststellen, welche Dienste über das Firewall-System, nach einer erfolgreichen Authentikation, möglich wären.

In diesem Fall ist es dem Angreifer nicht mehr möglich festzustellen, wie viele Rechnersysteme im zu schützenden Netz angeschlossen sind (1, 10, 100 oder 1 000?) und welche Dienste auf den Rechnersystemen aktiviert sind.

4.5.3 Password-Snooping und IP-Maskerade

Die Eigenschaften der verwendeten TCP/IP-Protokolle und Dienste (z. B. Telnet, FTP), dass Namen/Passworte im Klartext übertragen werden und jeder in der Lage ist, jede beliebige IP-Adresse anzunehmen, bilden ein großes Risiko.

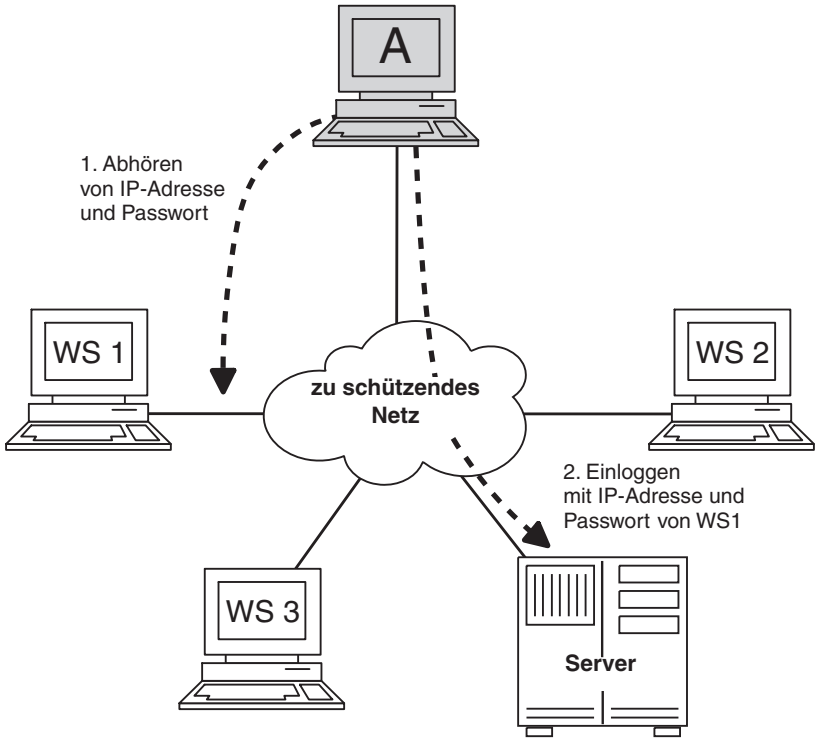


Abb. 4.13: Password-Snooping und IP-Maskerade

neuKap04.fm Seite 100 Freitag, 18. Oktober 2002 3:51 15

Analyse

In einem ersten Schritt liest der Angreifer mithilfe eines Analysegerätes (z. B. LAN-Watch, Feline, ...) die IP-Adresse sowie das Passwort, das bei einer berechtigten Kommunikation einen Dienst freischaltet, mit.

Das Lesen von Passworten kann auch mithilfe von Snifferprogrammen durchgeführt werden.

Nutzung von IP-Adresse und Passwort

Nachdem die berechtigte Kommunikation beendet wird, nimmt der Angreifer die IP-Adresse des »rechtmäßigen« Rechnersystems an (IP-Maskerade). Anschließend startet er die Kommunikation mit den Rechnersystemen, auf denen er unberechtigt arbeiten möchte. Danach nutzt der Angreifer das mitgelesene Passwort, um Zugang zu dem Rechnersystem mit dem entsprechenden Dienst zu erlangen.

Nun kann der Angreifer nach Belieben mit den Rechten des Benutzers, dessen Passwort er mitgelesen hat, seinen Angriff durchführen (siehe Abb. 4.13).

Wie kann ein Firewall-System helfen?

Durch die Integration eines Firewall-Systems mit dem Sicherheitsdienst »Zugangskontrolle auf Benutzerebene« wird ein *einheitliches* kryptographisches Authentikationsverfahren für den Zugriff auf alle internen Rechnersysteme im zu schützenden Netz zur Verfügung gestellt.

Durch die Verwendung eines kryptographischen Authentikationsprotokolls wird die Authentikation des Benutzers gegenüber dem Firewall-System erreicht, demgegenüber sich nur ein berechtigter Benutzer kryptographisch beweisen kann. Ein Benutzer kann sich kryptographisch nur korrekt beweisen, wenn er über den passenden geheimen Schlüssel verfügt.

Dieses Verfahren beruht darauf, dass das Mitlesen der dazu notwendigen Informationen (Zufallszahl und Kryptogramm) einem Angreifer nicht dazu verhilft, später mit diesen Informationen einen Zugriff über das Firewall-System in das zu schützende Netz zu erlangen (siehe Kapitel 8 *Authentikationsverfahren*).

Durch die eindeutige Identifikation und Authentikation eines Benutzers können auch die Logbuchdaten, die ein Firewall-System während der Kommunikation erzeugt, diesem Benutzer eindeutig zugeordnet werden.

neuKap04.fm Seite 101 Freitag, 18. Oktober 2002 3:51 15

up ...

neuKap04.fm Seite 102 Freitag, 18. Oktober 2002 3:51 15

... up ... update

Nutzen Sie den UPDATE-SERVICE des mitp-Teams bei vmi-Buch.

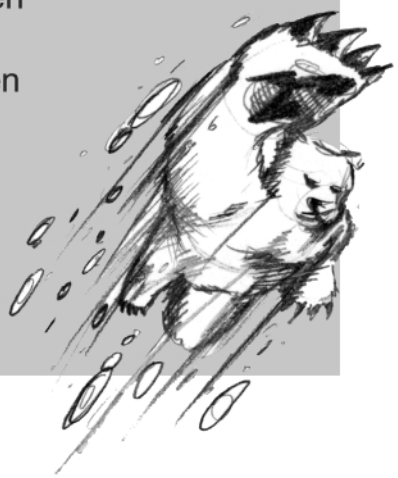
Registrieren Sie sich JETZT!

Unsere Bücher sind mit großer Sorgfalt erstellt. Wir sind stets darauf bedacht, Sie mit den aktuellsten Inhalten zu versorgen, weil wir wissen, dass Sie gerade darauf großen Wert legen. Unsere Bücher geben den top-aktuellen Wissens- und Praxisstand wieder.

Um Sie auch über das vorliegende Buch hinaus regelmäßig über die relevanten Entwicklungen am IT-Markt zu informieren, haben wir einen besonderen Leser-Service eingeführt.

Lassen Sie sich professionell, zuverlässig und fundiert auf den neuesten Stand bringen.
Registrieren Sie sich jetzt auf www.mitp.de oder **www.vmi-buch.de** und Sie erhalten zukünftig einen E-Mail-Newsletter mit Hinweisen auf Aktivitäten des Verlages wie zum Beispiel unsere aktuellen, kostenlosen Downloads.

Ihr Team von mitp



neuKap04.fm Seite 103 Freitag, 18. Oktober 2002 3:51 15

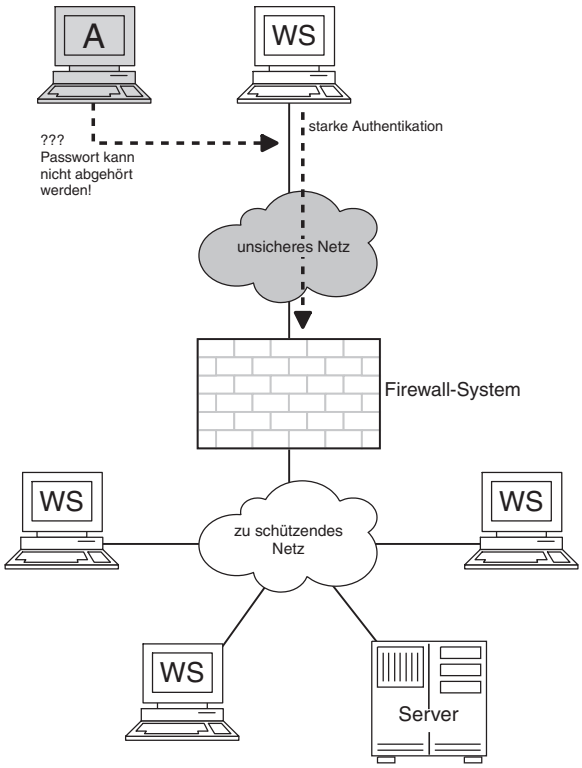


Abb. 4.14: Firewall-System mit dem Sicherheitsdienst »Zugangskontrolle auf Benutzerebene«

4.5.4 Nutzung einer falschen Konfiguration

Für jeden Dienst, der über einen Netzzugang ermöglicht werden soll, existiert ein Daemon-Prozess, der falsch konfiguriert oder installiert sein kann, sodass er es ermöglicht, auf dem entfernten Rechnersystem beliebige privilegierte Kommandos ausführen zu lassen, mit denen ein Angriff durchgeführt werden kann.

Durchführung des Angriffs

Der Angreifer nutzt die Tatsache, dass eine falsche Konfiguation vorliegt, um z. B. an die »root«-Rechte eines Rechnersystems zu gelangen, um damit seine Ziele zu erreichen. Zum Beispiel ein WWW-Server, der mit »root«-Rechten und fehlerhaften CGI-Scripten läuft.

neuKap04.fm Seite 104 Freitag, 18. Oktober 2002 3:51 15

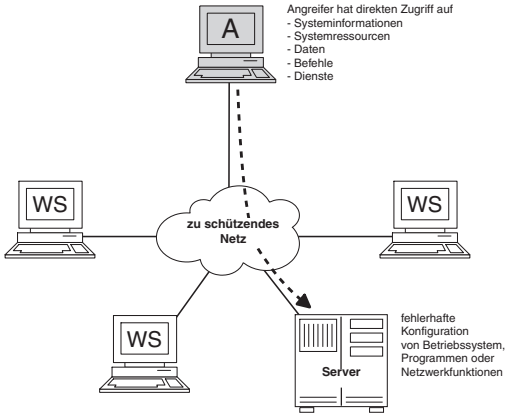


Abb. 4.15: Nutzung einer falschen Konfiguration

Wie kann ein Firewall-System helfen?

Durch die Integration eines Firewall-Systems mit Proxies (Stellvertreter) ist der direkte Zugriff nur auf Dienste mit einfacher Funktionalität (Proxy) des Firewall-Systems möglich. Dadurch wird verhindert, dass auf falsch konfigurierte Rechnersysteme im zu schützenden Netz direkt zugegriffen werden kann.

Fehlerhaft konfigurierte Rechnersysteme im zu schützenden Netz werden durch das Firewall-System mit Application-Gateway und Proxy entkoppelt.

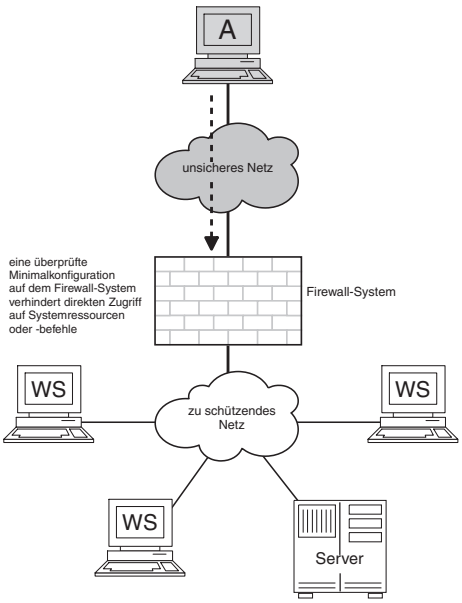


Abb. 4.16: Firewall-System mit einfacher Proxy-Funktionalität

neuKap04.fm Seite 105 Freitag, 18. Oktober 2002 3:51 15

4.5.5 Hopping (Telnet)

Hopping ist das unerlaubte »Weiterhüpfen« von einem remoten Rechnersystem auf ein weiteres Rechnersystem des zu schützenden Netzes. Dabei werden die Möglichkeiten des remoten Rechnersystems für den Zugriff auf das weitere Rechnersystem genutzt.

In vielen Anwendungen wie z. B. bei Servicearbeiten ist es sinnvoll, remote auf Rechnersysteme zuzugreifen. Es muss aber verhindert werden, dass von einem Rechnersystem aus unerlaubt auf weitere Rechnersysteme des zu schützenden Netzes zugegriffen werden kann.

Bei einem interaktiven Hopping wird interaktiv eine »Remote-Kette« aufgebaut. Dabei wird z. B. bei Telnet die entsprechende Meldung von einem Rechnersystem zum anderen geschleift, wobei aber nur beim Endsystem die Bildschirmausgabe erfolgt.

Beschreibung des Angriffes

Der Angreifer (Benutzer) greift mit den entsprechenden Rechten auf die Workstation 2 zu. Dann baut der Angreifer unerlaubt eine Verbindung von der Workstation 2 mit dem Server auf, um z. B. an wichtige Informationen zu gelangen. Eine direkte Verbindung ist nicht erlaubt.

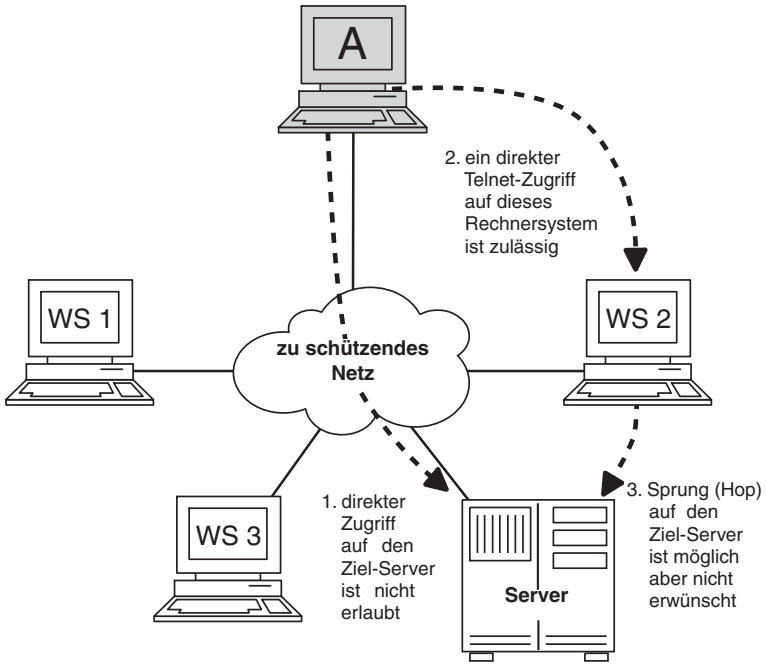


Abb. 4.17: Hopping-Angriff

neuKap04.fm Seite 106 Freitag, 18. Oktober 2002 3:51 15

Wie kann ein Firewall-System helfen?

Durch die Integration eines Firewall-Systems mit dem Sicherheitsdienst »Monitoring einer Telnet-Session« wird erkannt, ob ein Hopping-Angriff durchgeführt wird. Durch die Auflösung der Verbindung, Protokollierung des sicherheitsrelevanten Ereignisses und, falls eingestellt, durch die Sendung einer spontanen Meldung an das Security Management wird auf den Angriff reagiert.

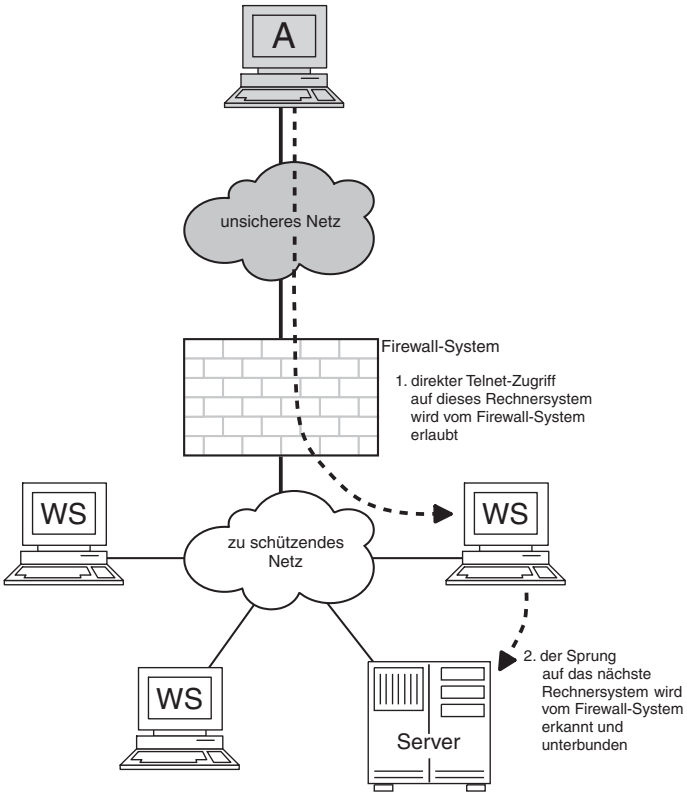


Abb. 4.18: Firewall-System mit dem Sicherheitsdienst »Monitoring einer Telnet-Session«

4.5.6 Nutzung von Implementierungsfehlern in Anwendungen wie z. B. sendmail

Die Programme, die im Bereich der TCP/IP-Kommunikation verwendet werden, sind sehr komplex. In der Vergangenheit hat sich gezeigt, dass sie Programm- und Funktionsfehler enthalten, die immer wieder für Angriffe missbraucht werden konnten. Prinzipiell ist es auch nicht möglich, Programme mit mehr als zehntausend Zeilen so weit auszutesten, dass nachweislich in keinem Betriebszustand

neuKap04.fm Seite 107 Freitag, 18. Oktober 2002 3:51 15

Fehler auftreten können. Aus diesem Grund muss auch in Zukunft immer wieder damit gerechnet werden, dass die Programme Sicherheitsrisiken aufweisen, die für Angriffe verwendet werden können.

Beispiel:

Komplexe Anwendungen, wie z. B. »sendmail«, wiesen in der Vergangenheit Implementierungs- und Designfehler auf, die es ermöglichten, auf dem entfernten Rechnersystem beliebige privilegierte Kommandos ausführen zu lassen, mit denen Angriffe durchgeführt werden konnten.

Beschreibung des Angriffes

Ein Angreifer nutzt den Befehl »debug«, damit er ein Programm auf dem entsprechenden Rechnersystem starten kann. Damit ist er in der Lage, Informationen von Rechnersystemen des zu schützenden Netzes auszulesen.

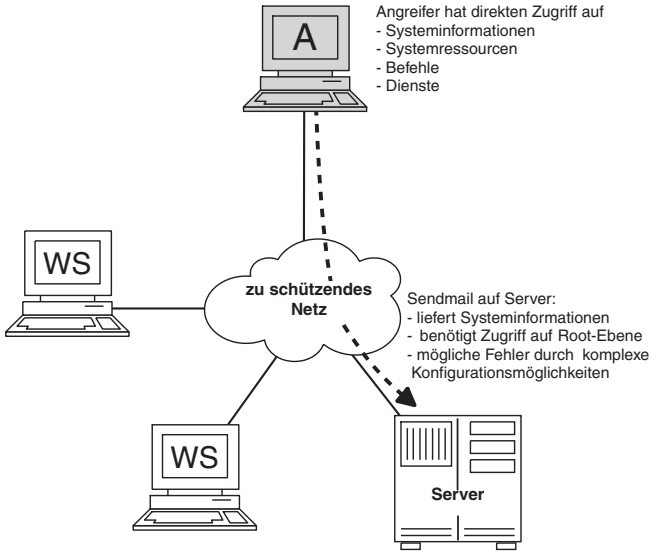


Abb. 4.19: Nutzung von Implementierungsfehlern in Anwendungen

Wie kann ein Firewall-System helfen?

Durch die Integration eines Firewall-Systems mit dem Sicherheitsdienst »Entkopplung von unsicheren Diensten« wird verhindert, dass ein Angreifer von außen einen entsprechenden Angriff durchführt.

Fehlerhafte Programme auf den Rechnersystemen im zu schützenden Netz werden dann durch das Firewall-System entkoppelt, d. h., sie sind nicht direkt erreichbar, sondern nur über Stellvertreter (Proxies).

neuKap04.fm Seite 108 Freitag, 18. Oktober 2002 3:51 15

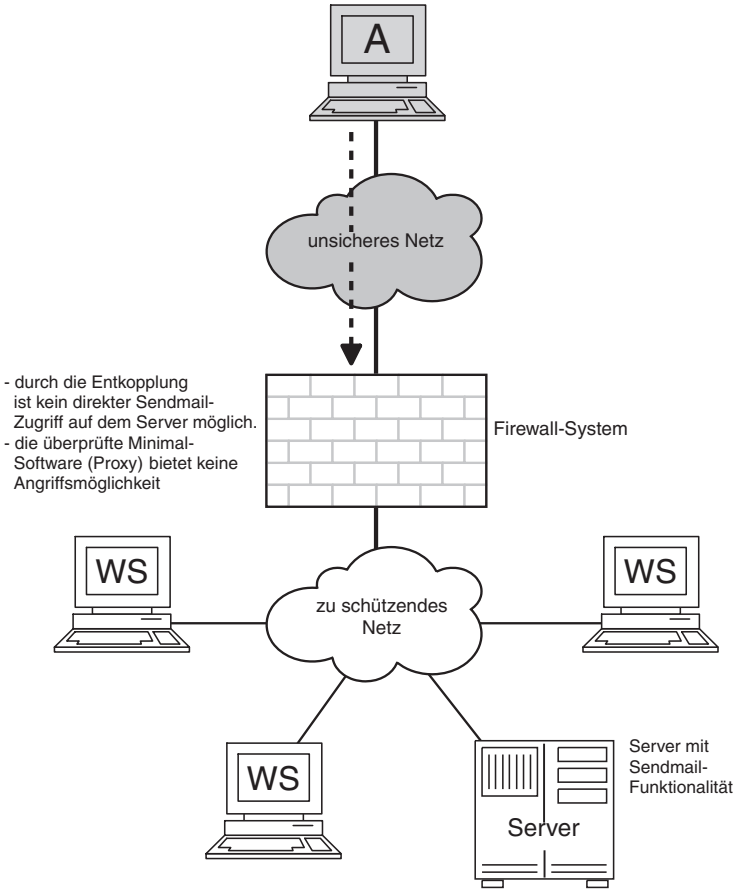


Abb. 4.20: Firewall-System mit dem Sicherheitsdienst »Entkopplung von unsicheren Diensten«

4.5.7 IP-Adressen-Spoofing

Beschreibung des Angriffes

Bei diesem Angriff verfälscht der Angreifer die Absender-IP-Adresse der IP-Pakete, die er unerlaubt in das zu schützende Netz senden möchte, mit einer vorhandenen internen IP-Adresse des zu schützenden Netzes. Der Zugangsrechner überprüft in diesem Beispiel nicht, ob das IP-Paket von außen oder von innen kommt.

Dadurch kann von außen eine Kommunikation mit einem Rechnersystem des zu schützenden Netzes durchgeführt werden.

neuKap04.fm Seite 109 Freitag, 18. Oktober 2002 3:51 15

In der Vergangenheit hatten viele Firewall-Systeme Probleme mit dieser Angriffsform, möglicherweise auch heute noch.

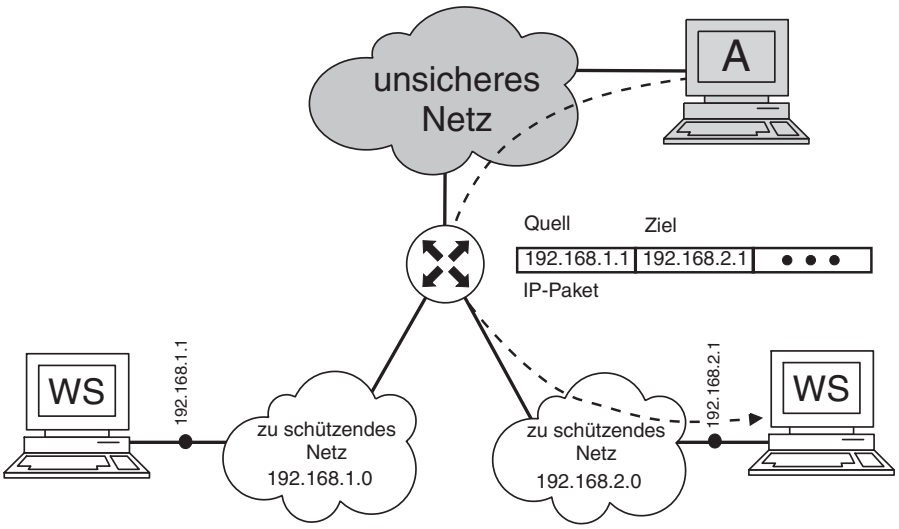


Abb. 4.21: IP-Adressen-Spoofing

Wie kann ein Firewall-System helfen?

Durch die Integration eines Firewall-Systems mit dem Sicherheitsdienst »Eindeutige Erkennung der Seite, von der ein IP-Paket empfangen wurde, und entsprechende Rechteverwaltung«, kann der Angriff IP-Adressen-Spoofing einfach verhindert werden.

4.5.8 ICMP-Angriffe

Als integrativer Bestandteil des TCP/IP-Protokollstacks dient das ICMP-Protokoll unter anderem dazu, bei auftretenden Netzwerkproblemen dem Absender der IP-Pakete Fehlermeldungen anzuzeigen. Der Absender kann dann auf den Fehler reagieren. Bei vielen Implementationen wird auf bestimmte Meldungen sofort, aus dem TCP/IP-Stack entsprechend automatisch reagiert. Ein Angreifer, der falsche ICMP-Protokollelemente sendet, ist damit in der Lage, gezielt Rechnersysteme des zu schützenden Netzes zu manipulieren.

Das Ziel von ICMP-Angriffen kann z. B. sein:

- Die Beeinträchtigung der Funktionsfähigkeit von IP-Netzwerken, z. B. durch das Einfügen der Kommandos »Fragmentation Needed«, »Destination Unreachable« oder »Source Quench« oder
- die Veränderung der Vermittlungspfade durch das Kommando »Redirect«.

neuKap04.fm Seite 110 Freitag, 18. Oktober 2002 3:51 15

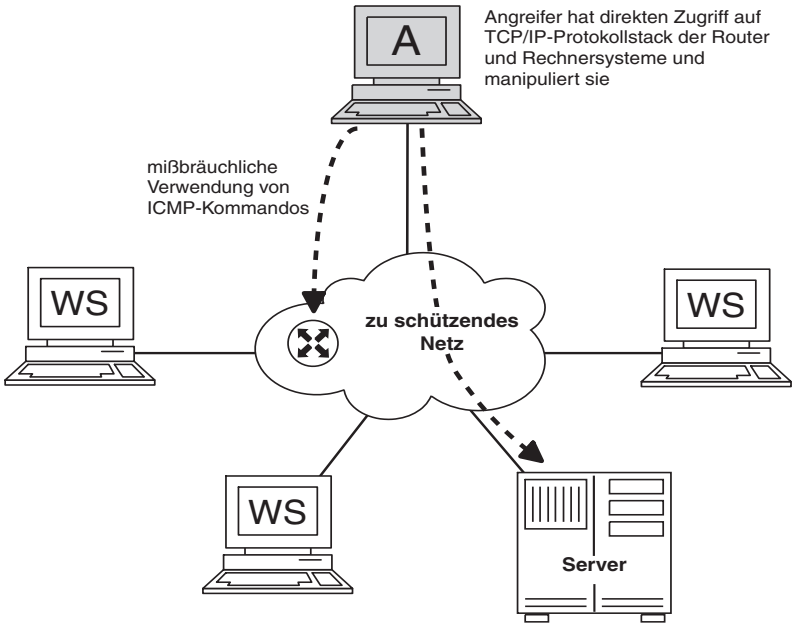


Abb. 4.22: ICMP-Angriffe

Beschreibung von möglichen ICMP-Angriffen

- Missbräuchliche Verwendung des Kommandos »Destination Unreachable«
  Falls IP-Pakete nicht an den gewünschten Empfänger vermittelt werden können, sendet das letzte Rechnersystem im Vermittlungssystem das ICMP-Kommando »Destination Unreachable« an den Sender der IP-Pakete. In der Regel reagiert der Sender mit dem Abbruch der Verbindung zum Empfänger. Ein Angreifer ist also in der Lage, durch das Senden von falschen »Destination Unreachable«-Kommandos bestehende TCP/IP-Verbindungen zum Abbruch zu veranlassen.
- Missbräuchliche Verwendung des Kommandos »Fragmentation Needed«
  Durch das Senden des ICMP-Kommandos »Fragmentation Needed« ist ein Angreifer in der Lage, in beliebigen Rechnersystemen die Fragmentierung von IP-Pakten zu veranlassen, wodurch die Daten in kleine Pakete fragmentiert (zerlegt) werden. Durch diesen Angriff wird eine Erhöhung der Netzlast provoziert.
- Missbräuchliche Verwendung des Kommandos »Source Quench«
  Mithilfe des ICMP-Kommandos »Source Quench« kann die Übertragungsrate des Rechnersystems des Senders reduziert werden. Ein Angreifer ist in der Lage, durch das missbräuchliche, exzessive Versenden von künstlich erzeugten Source-Quench-Paketen die Kommunikation empfindlich zu stören.

neuKap04.fm Seite 111 Freitag, 18. Oktober 2002 3:51 15

- Missbräuchliche Verwendung des Kommandos »Redirect«
  Ein Angreifer ist durch das Senden von gezielten ICMP-Kommandos »Redirect« in der Lage, die Routing-Tabellen der Router eines Netzes so zu verändern, dass die IP-Pakete einer Kommunikationsverbindung über andere Rechnersysteme übertragen werden, um dort die Daten manipulieren oder lesen zu können.

Wie kann ein Firewall-System helfen?

Durch die Integration eines Firewall-Systems mit dem Sicherheitsdienst »Rechteverwaltung von ICMP-Kommandos« wird verhindert, dass ein Angreifer von außen die oben beschriebenen Angriffe durchführen kann.

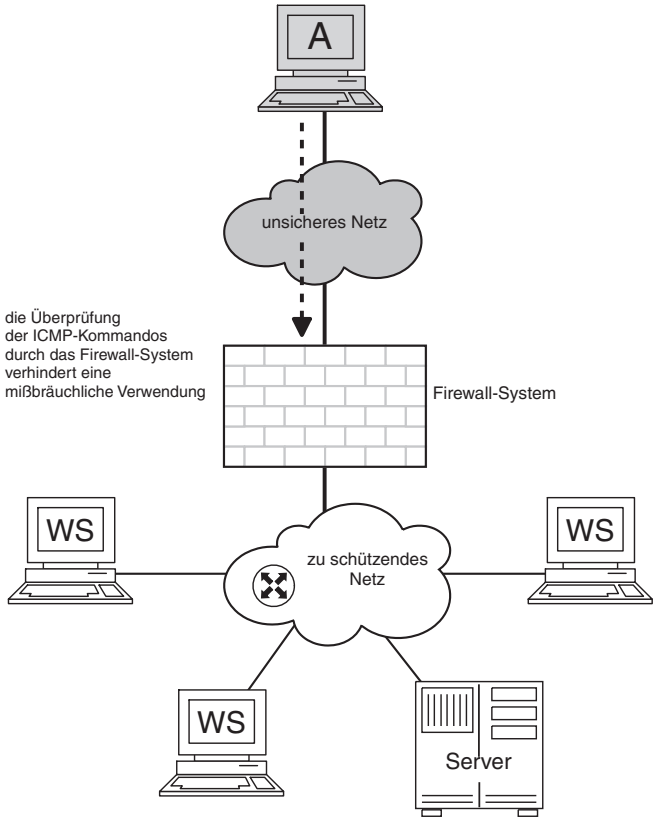


Abb. 4.23: Firewall-System mit dem Sicherheitsdienst »Rechteverwaltung von ICMP-Kommandos«

neuKap04.fm Seite 112 Freitag, 18. Oktober 2002 3:51 15

4.5.9 Internet-Routing-Angriffe

Im IP-Header können mithilfe des »Optionsfeldes« verschiedene Zusatzfunktionen genutzt werden. Dabei kann mit den Optionen »*Loose Source Routing*« und »*Strict Source Routing*« ein Angreifer durch Vorgeben der Route von außen Angriffe auf das zu schützende Netz durchführen.

Beschreibung des Angriffes

Bei der Option »Strict Source Routing« werden alle zu durchlaufenden Vermittlungsknoten in einer vorgegebenen Reihenfolge angegeben. Dadurch ist ein Angreifer in der Lage, die Kommunikation über ein bestimmtes – z. B. sein eigenes – Rechnersystem übertragen zu lassen, um dort die Daten lesen oder manipulieren zu können.

Wie kann ein Firewall-System helfen?

Durch die Integration eines Firewall-Systems mit dem Sicherheitsdienst »Rechteverwaltung der Optionen des IP-Protokolles« wird verhindert, dass ein Angreifer von außen den oben beschriebenen Angriff durchführen kann.

Weitere gezielte Angriffe, die auf der Schwäche der TCP/IP-Technologie beruhen, siehe z. B. auch /Kyas96b/.

4.6 Ergebnisse der KES/Utimaco-Studien

Die KES/Utimaco-Studien der Jahre 1996, 1998 und 2000 zeigen, wie der Status der Informationssicherheit in der betrieblichen Wirklichkeit in Deutschland ist. Die wichtigsten Ergebnisse finden sich konzentriert in /Görtz99/, wo folgende Fragen mit Blockdiagrammen aufgeschlüsselt sind:

- Welche Gefahren haben zu Beeinträchtigungen der IT-Sicherheit geführt?
- Wie ist die aktuelle Risikosituation in Unternehmen?
- Welche Probleme behindern die Verbesserung der Informationssicherheit?
- Wer ist für die Probleme der betrieblichen Informationssicherheit verantwortlich?
- Welche Maßnahmen werden zum Schutz der Kommunikation in öffentlichen Netzen angewandt?

4.7 Zusammenfassung

Mit dem enormen Anwachsen von Kommunikationsnetzen wie Internet und Intranet in der modernen Informationsgesellschaft wächst auch das Risiko, dass Daten manipuliert oder gestohlen werden können und damit ein Schaden auftritt.

Wir sind zwar nicht in der Lage, die Bedrohungen zu beeinflussen, aber wir können dafür sorgen, dass unsere Verletzbarkeit reduziert wird.

neuKap04.fm Seite 113 Freitag, 18. Oktober 2002 3:51 15

Aus diesem Grund wird es in Zukunft immer wichtiger, unsere Kommunikationssysteme sicherer zu gestalten, damit eine vertrauenswürdige und beherrschbare Kommunikation realisiert werden kann.

Immer größere Bedeutung erlangen dabei aktive Abwehrmechanismen wie Security Audit-Systeme (siehe Kapitel 13.6) und Intrusion-Detection/Response-Systeme (siehe Kapitel 13.7). Denn schließlich können große Organisationen unmöglich ihren IT-Betrieb herunterfahren, nur weil jemand z. B. an den Ports »fingert«.

Allerdings verbleibt trotz aller Sicherungsmaßnahmen immer noch ein kleines Restrisiko. Jede Organisation tut gut daran, Notfallpläne für den »Fall der Fälle« auszuarbeiten, in dem Verfahren und Zuständigkeiten festgelegt werden. Diese Pläne sollten von Zeit zu Zeit auch in einem Manöver getestet werden, um im Ernstfall Panik und damit unter Umständen zusätzlichen Schaden zu verhindern.

Ein abschließender Hinweis

In diesem Kapitel wurden prinzipiell die Gefahren aus dem Netz erklärt. Dies musste ohne Anspruch auf Vollständigkeit und Detailtiefe geschehen, sonst hätte es den Rahmen dieses Fachbuchs über Firewall-Systeme überschritten. Jeder Interessierte sollte sich bei Bedarf weiter informieren, z. B. in Newsgroups oder www-Foren.

Besonders aktuell ist der 14-täglich verschickte »Security Newsletter« aus dem INTEREST-Verlag. Er ist im Abonnement des »Organisationshandbuchs Netzwerksicherheit« enthalten und kann mit einem E-Mail-Warndienst kombiniert werden (siehe: `www.interest.de`).

neuKap04.fm Seite 114 Freitag, 18. Oktober 2002 3:51 15

neuKap05.fm Seite 115 Freitag, 18. Oktober 2002 3:51 15

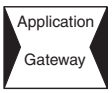
Kapitel 5

Elemente eines Firewall-Systems

In diesem Kapitel wird beschrieben, mit welchen Grundelementen ein Firewall-System aufgebaut werden kann. Es soll gezeigt werden, wie technische Sicherheitsmechanismen für Firewall-Elemente realisiert werden können, welche konkreten Möglichkeiten bestehen, um Sicherheit zu gewährleisten, wie die Architektur von Firewall-Elementen ist, wie sie wirken und wo ihre Grenzen sind.

Bei Firewall-Elementen wird unterschieden zwischen Elementen, die aktiv in die Kommunikation zwischen dem zu schützenden und dem unsicheren Netz eingreifen, und dem Element Security Management, das für die Verwaltung des aktiven Firewall-Elements verantwortlich ist, in dem die Sicherheitspolitik einer Organisation in Form eines Regelwerks definiert wird.

In der Praxis haben sich die aktiven Firewall-Elemente Packet Filter und Application Gateway mit speziellen Varianten und Kombinationen herauskristallisiert, die einen unterschiedlichen Ansatz bei der Einbindung in das Kommunikationssystem und in den Möglichkeiten der Analyse und Protokollierung haben.

Firewall-Element	Bedeutung
Symbol Packet Filter	Packet Filter analysieren und kontrollieren die übertragenen Pakete von der Netzzugangs-, der Netzwerk- bis zur Transportebene und bei zustandsorientiertem Packet Filter evtl. bis zur Anwendungsebene.
 Symbol Application Gateway	Application Gateways analysieren und kontrollieren die Pakete auf der Anwendungsebene und haben mehr Möglichkeiten bei der Protokollierung von Handlungen.
Symbol Security Management	Das Security Management steuert und verwaltet die aktiven Firewall-Elemente.
Alle weiteren Symbole finden Sie im Anhang C, der Legende.	

neuKap05.fm Seite 116 Freitag, 18. Oktober 2002 3:51 15

5.1 Aktive Firewall-Elemente

Im Folgenden wird als Erstes der prinzipielle Aufbau der aktiven Firewall-Elemente, die in die Kommunikationsschnittstelle zwischen dem unsicheren Netz und dem zu schützenden Netz eingefügt werden, dargestellt.

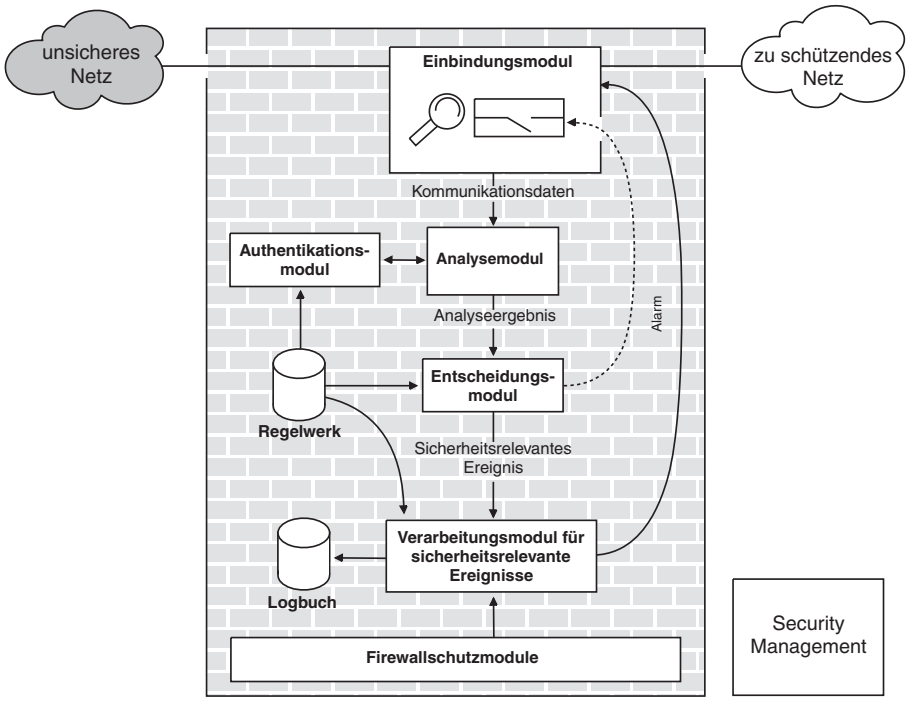


Abb. 5.1: Aufbau eines aktiven Firewall-Elementes

5.1.1 Architektur von aktiven Firewall-Elementen

Alle aktiven Firewall-Elemente brauchen folgende Komponenten, damit sie die Sicherheitsdienstleistungen erbringen können, für die sie eingesetzt werden.

Einbindungsmodul

Das Einbindungsmodul realisiert die Einbindung des aktiven Firewall-Elementes in das Kommunikationssystem. Beim Packet Filter ist dies oberhalb der Netzzugangsebene, beim Application Gateway für die Proxies oberhalb der Ports (Transportebene). Die Einbindung in das Kommunikationssystem muss so realisiert werden, dass die Kommunikationsdaten nicht am Einbindungsmodul vorbeifließen können, ohne einer Analyse und einer Entscheidung unterzogen worden zu sein. Aus diesem Grund ist die Einbindung besonders sicherheitskritisch. Bei Soft-

neuKap05.fm Seite 117 Freitag, 18. Oktober 2002 3:51 15

ware-Lösungen, die auf Standard-Betriebssystemen aufbauen, ist diese Einbindung besonders problematisch (siehe Kapitel 9.2.1 *Was bietet eine Software-Lösung?*).

Analysemodul

Im Analysemodul werden die Kommunikationsdaten den Möglichkeiten des aktiven Firewall-Elements entsprechend analysiert. Die Ergebnisse der Analyse werden an das Entscheidungsmodul weitergeleitet. Vor allem die Tiefe der Analyse, d.h. wie weit und umfangreich analysiert wird, ist sicherheitskritisch und stellt ein besonderes Qualitätsmerkmal eines aktiven Firewall-Elementes dar. Die unterschiedlichen aktiven Firewall-Elemente (Packet Filter und Application Gateway) analysieren auf unterschiedlichen Kommunikationsebenen.

Entscheidungsmodul

Im Entscheidungsmodul werden die Analyseergebnisse ausgewertet und mit den im Regelwerk festgelegten Definitionen der Sicherheitspolitik verglichen. Hier wird anhand von Access-Listen überprüft, ob ankommende Kommunikationsdaten passieren dürfen oder nicht. Falls ja, wird das Einbindungsmodul zum Durchlass aktiviert. Falls nein, werden die Kommunikationsdaten nicht durchgelassen; das Ereignis wird als sicherheitsrelevant eingestuft und entsprechend protokolliert.

Verarbeitungsmodul für sicherheitsrelevante Ereignisse

In diesem Verarbeitungsmodul werden alle sicherheitsrelevanten Ereignisse verarbeitet, die im aktiven Firewall-Element erzeugt werden. In Abhängigkeit vom Regelwerk wird ein sicherheitsrelevantes Ereignis mit den dazugehörigen Protokolldaten je nach Einstellung in ein Logbuch geschrieben oder über den Alarmmechanismus als Warnmeldung an ein Security Management weitergeleitet.

Authentikationsmodul

Das Authentikationsmodul sorgt für die Identifikation und Authentikation der Instanzen (Prozesse in den Rechnersystemen, Benutzer etc.), die über das aktive Firewall-Element kommunizieren möchten. Hier können unterschiedliche Authentikationsverfahren verwendet werden (siehe auch Kapitel 8 *Authentikationsverfahren*).

Firewallschutzmodul

Das aktive Firewall-Element muss nicht nur Sicherheitsdienste erbringen, sondern auch selbst gegen Angriffe resistent sein.

Im Firewallschutzmodul verbergen sich aktive Sicherheitsfunktionen, die für den sicheren Betrieb des aktiven Firewall-Elements selbst sorgen. Dazu gehören z.B. die folgenden Sicherheitsmechanismen:

- Integritätstest: Dieser Sicherheitsmechanismus gewährleistet, dass Veränderungen der Software (Betriebssystem, Firewall, Sicherheitsmechanismen etc.), des Regelwerks und des Logbuches erkannt werden. Dies wird z.B. durch eine

neuKap05.fm Seite 118 Freitag, 18. Oktober 2002 3:51 15

regelmäßige und/oder spontane Checksummen-Überprüfung der Software und der Daten realisiert.

- Authentikationsmechanismus: Dieser Sicherheitsmechanismus sorgt dafür, dass nur vom (dazu berechtigten) Security Management das Regelwerk beeinflusst und die Protokolldaten aus dem Logbuch ausgelesen werden können (siehe auch Kapitel 8 *Authentikationsverfahren*).
- Betriebssicherungsmechanismen: Hier werden Sicherheitsmechanismen zusammengefasst, die für den sicheren Betrieb der aktiven Firewall-Elemente sorgen. Zu diesen Sicherheitsmechanismen gehören z. B. die Überprüfung des Überlaufs von Logbüchern und Speichermedien (z. B. Festplatte) und die Überprüfung, ob sich die Software in einem definierten Zustand (Automatenzustand) befindet, usw.

Regelwerk

Das Regelwerk ist die technische Umsetzung der Sicherheitspolitik und wird mithilfe eines Security Management erstellt.

Im Regelwerk stehen alle Informationen (Schlüssel, Access-Listen, Attribute usw.) über Benutzer, Authentikationsverfahren, Kommunikationsverbindungen etc., die notwendig sind, um eine Entscheidung für oder gegen eine Übertragung der Kommunikationsdaten über das aktive Firewall-Element fällen zu können, und bei welchen sicherheitsrelevanten Ereignissen geloggt und Alarm gemeldet werden soll.

Logbuch

Das Logbuch enthält alle Protokolldaten der sicherheitsrelevanten Ereignisse, die während des Betriebs eines aktiven Firewall-Elements aufgetreten sind und im Regelwerk entsprechend registriert werden sollen.

Security Management

Mithilfe des Security Management können die Regeln für die aktiven Firewall-Elemente festgelegt und die Protokolldaten der sicherheitsrelevanten Ereignisse aus den Logbüchern analysiert werden.

5.1.2 Designkonzept aktiver Firewall-Elemente

Im Folgenden wird ein sicheres Designkonzept für aktive Firewall-Elemente beschrieben. Die Wirksamkeit der Sicherheitsdienste eines aktiven Firewall-Elementes ist um so höher, je mehr die im Folgenden vorgestellten Sicherheitskriterien berücksichtigt werden.

Minimale Software

Zusätzlich zu den Sicherheitsdienstleistungen, die ein aktives Firewall-Element erbringen soll, muss das Firewall-Element selbst gegen Angriffe resistent sein. Daher ist es besonders wichtig, nur fehlerfreie Software einzusetzen. Das Firewall-

neuKap05.fm Seite 119 Freitag, 18. Oktober 2002 3:51 15

Element muss klar strukturiert und nachvollziehbar aufgebaut und realisiert werden. Da jedes Programm aber potenziell Sicherheitslücken enthalten kann, sollten nur die für die Erbringung der Firewall-Funktionalität unbedingt notwendigen Programme auf dem aktiven Firewall-Element eingesetzt werden (keine Routerfunktionalität, keine weiteren Anwendungen, ...).

Unnötige oder überflüssige Prozesse im Hintergrund sind häufig die Ursache von Sicherheitslücken /CERT95/.

Sichere Einbindung in das Kommunikationssystem (Netzwerk-Software, Betriebssystem usw.)

Die Sicherheit eines aktiven Firewall-Elementes hängt in entscheidendem Maße davon ab, wie gut die Sicherheitsmechanismen in das Kommunikationssystem eingebunden werden. Es muss sichergestellt werden, dass es nicht möglich ist, die Firewall-Sicherheitsfunktionen über das Betriebssystem oder über die verwendete Kommunikations-Software (TCP/IP-Software, Netzzugangs-Treiber etc.) zu umgehen (siehe dazu auch Kapitel 9.2.1 *Was bietet eine Software-Lösung?*).

Beispiele: Bei Verwendung von IP-Forwarding (Kernel-Funktionalität) kann die Kommunikation am Firewall-Element vorbeigeleitet werden, ohne dass die Sicherheitsmechanismen wirken können.

Getrenntes Security Management

Die Forderung, auf den aktiven Firewall-Elementen nur minimale Software zu installieren, bedingt, dass das Security Management von den eigentlichen Sicherheitsfunktionen des aktiven Firewall-Elementes getrennt realisiert werden muss, damit ein Höchstmaß an Sicherheit auf dem aktiven Firewall-Element gewährleistet werden kann.

Die getrennte Realisierung des Security Management kann z. B. auf einem separaten Rechnersystem oder mithilfe einer Wechselplatte, die nur für die Festlegung der Regeln eingeführt wird, realisiert werden.

Einfache, zuverlässige und berechtigte Bedienung des Security Managements

Für das Security Management ist eine einfache und zuverlässige Bedienung erforderlich, damit die Regeln ohne Fehler eingegeben werden können. Außerdem ist eine Überprüfung der Widerspruchsfreiheit der Regeln erforderlich, damit nicht versehentlich sicherheitskritische Eingaben gemacht werden.

Ebenso muss sichergestellt werden, dass nur vom berechtigten Administrator mithilfe des Security Management auf die aktiven Firewall-Elemente zugegriffen werden kann, damit das Security Management nicht von Angreifern genutzt werden kann, um eine Kommunikation über das aktive Firewall-Element zuzulassen.

neuKap05.fm Seite 120 Freitag, 18. Oktober 2002 3:51 15

In diesem Abschnitt wird beschrieben, mit welchen Grundelementen ein Firewall-System aufgebaut werden kann. Das Ziel dieser Darstellung ist, aufzuzeigen, wie technische Sicherheitsmechanismen für Firewall-Elemente realisiert werden können, welche konkreten Möglichkeiten bestehen, Sicherheit zu gewährleisten, wie sie wirken und wo ihre Grenzen liegen.

Ein Firewall-System kann aus den folgenden Grundelementen bestehen:

- Packet Filter
- Stateful Inspection
- Application Gateway
- Proxies
- Adaptive Proxies

Um die konzeptionellen Unterschiede zu verdeutlichen und so das Verständnis zu erleichtern, werden im Folgenden die einzelnen Firewall-Elemente mithilfe von Analogien erläutert.

Eine plastische, leicht fassbare Analogie zu einen Firewall-System ist ein Pförtner. Alle Zugänge zu einem Gebäude sollen vom Pförtner überwacht werden. Hier gilt: Je weniger Zugänge es gibt, desto besser kann der Pförtner den Zugang kontrollieren (Common Point of Trust).

5.2 Packet Filter

Das aktive Firewall-Element »Packet Filter« analysiert und kontrolliert die ein- und ausgehenden Pakete auf der Netzzugangs-, der Netzwerk- und der Transportebene. Dazu werden die Pakete (z. B. Ethernet oder TokenRing), die auf dem physikalischen Kabel übertragen werden, aufgenommen und analysiert. Durch den Packet Filter werden die Netze physikalisch entkoppelt. Ein Packet Filter verhält sich wie eine einfache Bridge. Packet Filter sind nicht nur auf TCP/IP-Protokolle beschränkt.

Ein Packet Filter interpretiert den Inhalt der Pakete und verifiziert, ob die Daten in den entsprechenden Headers der Kommunikationsebenen den definierten Regeln entsprechen. Die Regeln werden so definiert, dass nur die notwendige Kommunikation erlaubt ist und bekannte sicherheitskritische Einstellungen vermieden werden, z. B. die IP-Fragmentierung. Die Packet Filter werden transparent in die Leitung eingefügt.

Analogie zum Pförtner

Wenn der LKW eines Lieferanten am Werktor mit einer Lieferung vorfährt, schaut der »Packet-Filter-Pförtner« auf das Logo an der Seite des LKWs, um zu überprüfen, ob es ihm bekannt ist und lässt den LKW gegebenenfalls unmittelbar durch das Tor, ohne den Lieferschein zu kontrollieren.

neuKap05.fm Seite 121 Freitag, 18. Oktober 2002 3:51 15

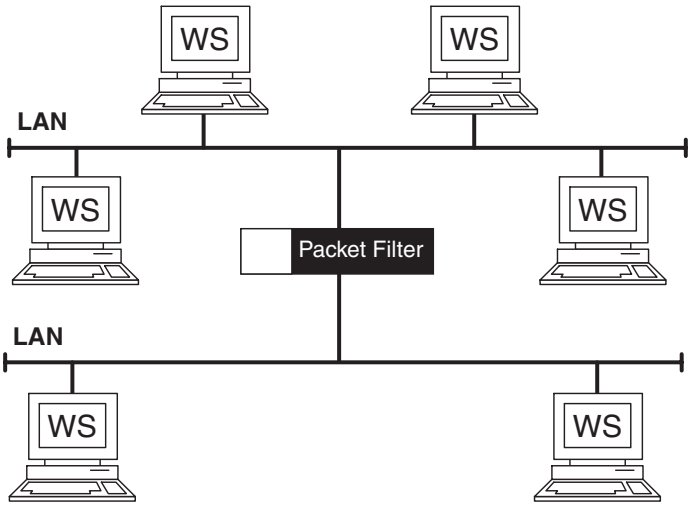


Abb. 5.2: Firewall-Element: Packet Filter

5.2.1 Allgemeine Arbeitsweise von Packet Filtern

In Abb. 5.3 ist die allgemeine Arbeitsweise von Packet Filtern dargestellt. Hier ist zu erkennen, welche Informationen aus den Paketen zur Analyse verwendet werden.

Hier können auf den verschiedenen Kommunikationsebenen unterschiedliche Überprüfungen durchgeführt werden.

- Es wird überprüft, von welcher Seite das Paket empfangen wird (Information aus dem Einbindungsmodul).
- Auf der Netzzugangsebene werden die Quell- und Ziel-Adresse und der verwendete Protokolltyp kontrolliert.
- Auf Netzwerkebene wird je nach Protokoll überprüft:
  - IP-Protokoll: z. B. die Ziel- und die Quell-Adresse und das verwendete Schicht-4-Protokoll, aber auch Optionsfeld und Flags
  - ICMP: die ICMP-Kommandos
  - IPX-Protokoll: z. B. Network/Node
  - OSI-Protokoll: die OSI-Netzwerkadresse
- Auf Transportebene findet
  - bei UDP/TCP z. B. eine Überprüfung der Portnummern (Quell- und Ziel-Port) statt (hierüber werden die Dienste wie FTP, Telnet, HTTP definiert);
  - bei TCP findet z. B. zusätzlich eine Überprüfung der Richtung des Verbindungsaufbaus statt.
- Zusätzlich kann überprüft werden, ob der Zugriff über den Packet Filter in einem definierten Zeitraum durchgeführt wird (z. B. montags bis freitags von 7 Uhr bis 19 Uhr, samstags von 7 bis 13 Uhr, sonntags nicht).

neuKap05.fm Seite 122 Freitag, 18. Oktober 2002 3:51 15

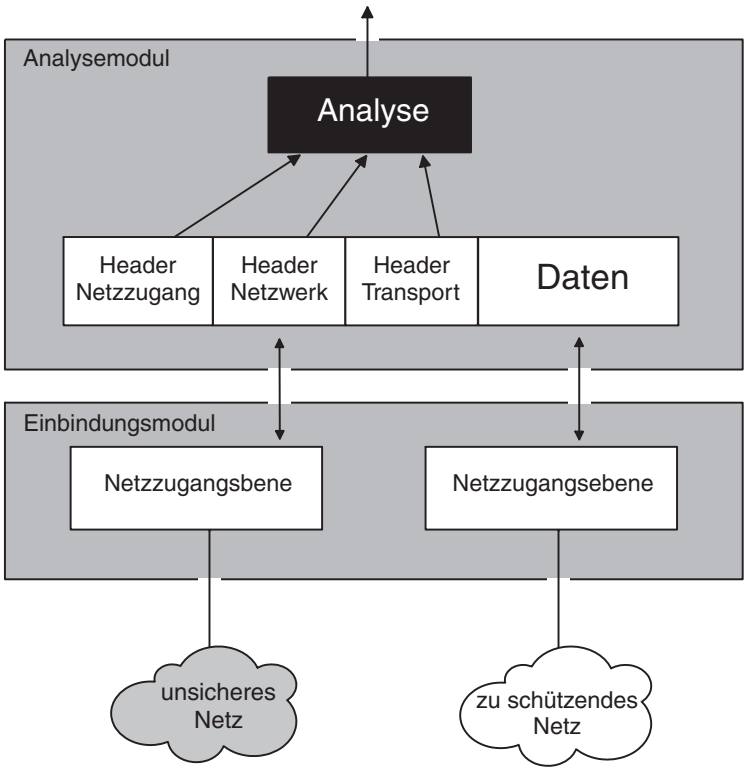


Abb. 5.3: Allgemeine Arbeitsweise eines Packet Filters

Die entsprechenden Prüfinformationen werden dem Regelwerk (Accessliste, Rechteliste) entnommen und mit den Analyse-Ergebnissen verglichen.

Bei Verstoß gegen die Regeln wird dies als sicherheitsrelevantes Ereignis entsprechend protokolliert, und falls diese Option eingerichtet ist wird eine Spontane Meldung mit den Protokolldaten des sicherheitsrelevanten Ereignisses an das Security Management gesendet, damit schnell reagiert werden kann.

Im Folgenden wird dargestellt, welche Überprüfungen auf den verschiedenen Kommunikationsebenen durchgeführt werden können. Dabei ist zu berücksichtigen, dass die Überprüfung auf der Netzzugangsebene in der Regel bei Intranets im lokalen Bereich zur Anwendung kommt und die Überprüfungen der Netzwerk- und Transportebene für die Kontrolle der Kommunikation über Internet und Intranets Anwendung finden.

5.2.2 Überprüfungen auf der Netzzugangsebene

Auf der Netzzugangsebene müssen unterschiedliche Standards unterstützt werden. Im Folgenden werden die Möglichkeiten für Ethernet aufgezeigt.

neuKap05.fm Seite 123 Freitag, 18. Oktober 2002 3:51 15

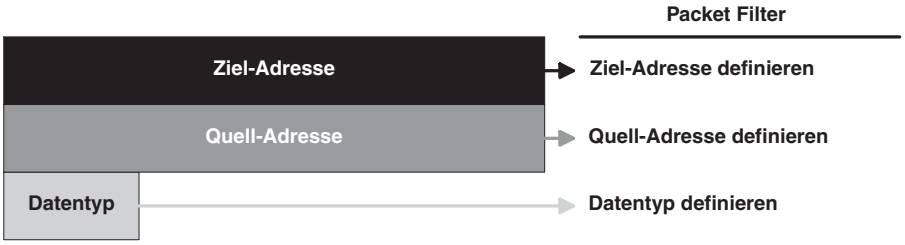


Abb. 5.4: Aufbau des Ethernet MAC-Frames (DIX2)

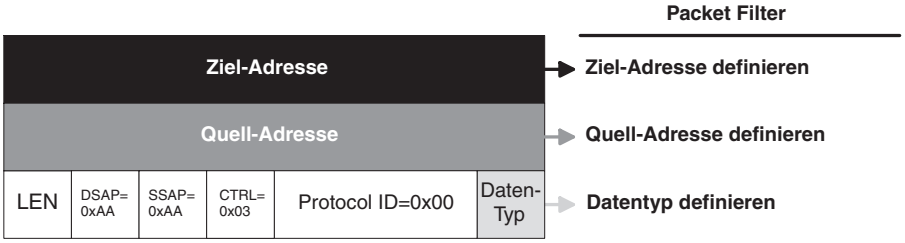


Abb. 5.5: Aufbau des Ethernet MAC Frames (802.3 + 802.2 SNAP)

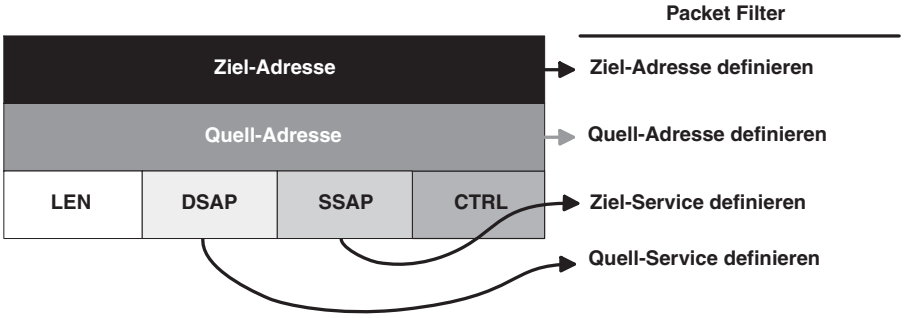


Abb. 5.6: Aufbau des Ethernet MAC Frames (802.3 + 802.2)

Bei Ethernet-Paketen kann der Packet Filter die Ziel- und Quell-Adresse analysieren und im entsprechenden Regelwerk nachsehen, ob die Rechnersysteme, Server und Router, zu denen die Adressen (MAC-Adressen) gehören, eine Kommunikation über den Packet Filter durchführen dürfen oder nicht. Bei Firewall-Systemen kann hier der unmittelbare Kommunikationspartner auf unterster Kommunikationsebene (z. B. Application Gateway, Mail- oder DNS Server) definiert werden.

Im »Datentyp«-Feld oder DSAP/SSAP-Feld kann festgestellt werden, über welches Kommunikationsprotokoll die Kommunikation auf der nächsthöheren Schicht stattfindet, z. B. IPX, IP, DECNET-Protokolle usw. Die Definitionen für das »Datentyp«-Feld sind in einem RFC (Request for Comment 1700) festgelegt.

neuKap05.fm Seite 124 Freitag, 18. Oktober 2002 3:51 15

Außerdem wird z. B. bei einer IP-Kommunikation unterbunden, dass bei einem speziellen Angriff mehrere IP-Pakete in einem MAC-Frame enthalten sind. Dabei wird eine Verbindung zwischen der Analyse der Netzzugangs- und Netzwerkebene realisiert. Hier sind in der Vergangenheit Angriffe durchgeführt worden.

5.2.3 Überprüfungen auf der Netzwerkebene

Auf der Netzwerkebene werden im Fall eines IP-Protokolls die Ziel- und die Quell-Adresse und das Transport-Protokoll überprüft, im Fall eines IPX-Protokolls werden Network und Node überprüft.

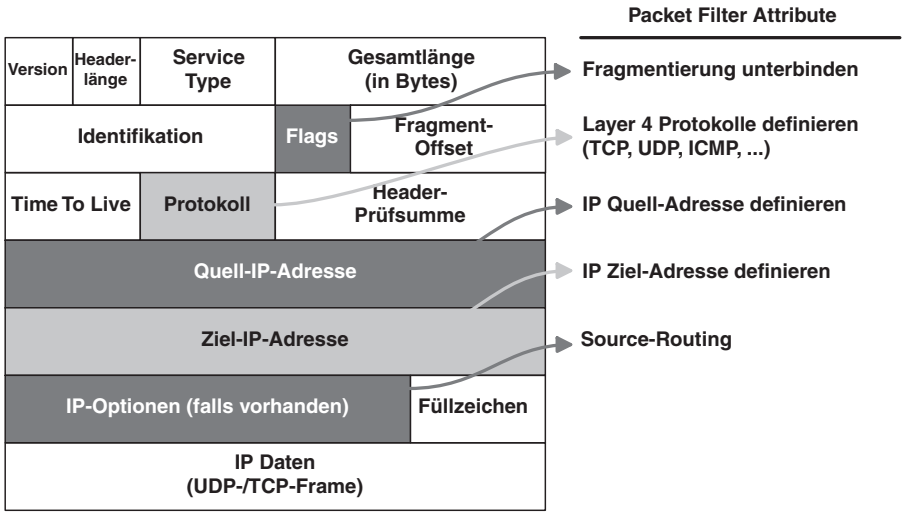


Abb. 5.7: Aufbau des IP-Frames

In Abb. 5.7 ist dargestellt, welche Möglichkeiten bei IP-Frames bestehen, eine Analyse durchzuführen, um die Kommunikation über den Packet Filter zu kontrollieren.

Bei einem IP-Frame werden Ziel- und Quell-Adresse überprüft und festgestellt, ob hier eine Kommunikationsverbindung über den Packet Filter erlaubt ist. Außerdem kann dem »Protokoll«-Feld entnommen werden, welches Transport-Kommunikationsprotokoll gefahren wird. Auch hier kann gegenüber der Rechteliste überprüft werden, ob das entsprechende Transport-Kommunikationsprotokoll (wie TCP oder UDP) verwendet werden darf oder nicht.

Dem »Flags«-Feld kann entnommen werden, ob eine Fragmentierung der IP-Pakete durchgeführt wird. Da über Fragmentierungen Angriffe gefahren werden können, kann hier die Fragmentierung über die Festlegung der Rechte unterbunden werden.

neuKap05.fm Seite 125 Freitag, 18. Oktober 2002 3:51 15

Mithilfe des »IP-Optionen«-Feldes kann festgelegt werden, welche Optionen (Source-Routing, ...) über den Packet Filter verwendet werden dürfen. Hier kann und sollte das Source-Routing unterbunden werden, da über diese Funktion Angriffe verwendet werden können (siehe Kapitel 4.5 *Angriffsmethoden und prinzipielle Gegenmaßnahmen auf der Grundlage der TCP/IP-Protokolle*).

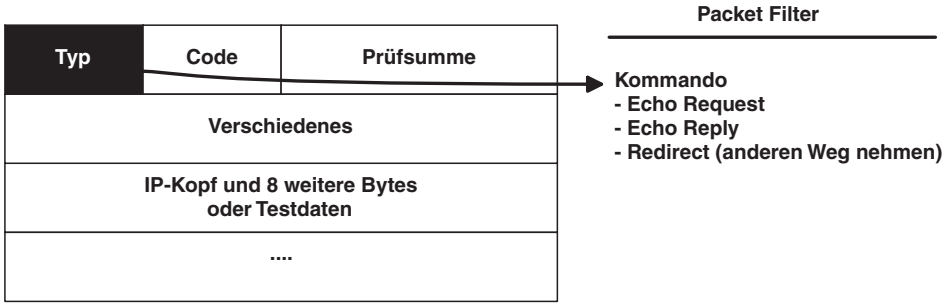


Abb. 5.8: Aufbau des ICMP-Frames

Bei ICMP kann das »Type«-Feld analysiert werden, in dem die Kommandos definiert sind. Hier können Kommandos wie EchoRequest, EchoReply, Redirect, Destination Unreachable etc. erlaubt oder verboten werden. Zum Beispiel werden EchoRequest und EchoReply, die für den »Ping«-Befehl verwendet werden, erlaubt, aber der Befehl Redirect verboten, über den Angriffe durchgeführt werden (siehe Kapitel 4.5 *Angriffsmethoden und prinzipielle Gegenmaßnahmen auf der Grundlage der TCP/IP-Protokolle*). Die Kommandos sind durch RFCs definiert.

5.2.4 Überprüfungen auf der Transportebene

Auf der Transportebene findet im Fall von UDP/TCP (und damit auch indirekt für die TCP/IP-Anwendungen HTTP, FTP, Telnet usw.) eine Überprüfung der Portnummern statt. Im Fall von TCP wird zusätzlich die Richtung des Verbindungsaufbaus überprüft.

Transportprotokoll – UDP

UDP ist ein verbindungsloses Kommunikationsprotokoll, d.h., die UDP-Pakete werden unabhängig voneinander übertragen. Bei UDP gibt es keine Garantie oder Kontrolle über die korrekte Auslieferung der Pakete. Zwischen dem Aufbau einer neuen UDP-Verbindung oder den Paketen innerhalb einer bestehenden UDP-Verbindung wird nicht unterschieden.

Beim UDP-Frame können durch den Packet Filter Quell- und Ziel-Port analysiert werden. Anhand einer Rechteliste kann bestimmt werden, welche Dienste über UDP gefahren werden können, z.B. SNMP, TFTP usw.

neuKap05.fm Seite 126 Freitag, 18. Oktober 2002 3:51 15

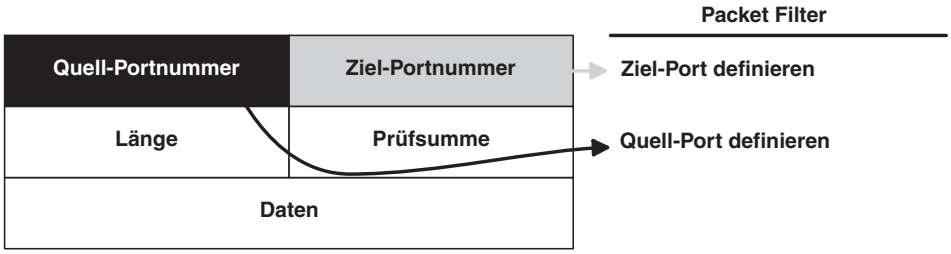


Abb. 5.9: Aufbau des UDP-Frames

In der Regel sollen UDP-Pakete möglichst nicht zugelassen werden, weil sonst mehr Angriffe realisiert werden können.

Transportprotokoll – TCP

In Abb. 5.10 ist zu sehen, welche Informationen bei einem TCP-Frame analysiert und kontrolliert werden können.

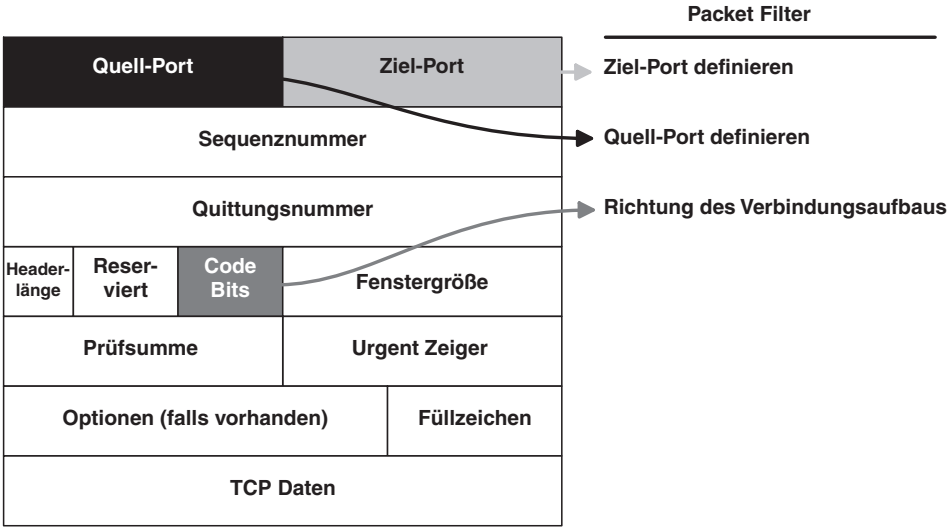


Abb. 5.10: Aufbau des TCP-Frames

Beim TCP-Frame können durch den Packet Filter wiederum Quell- und Ziel-Port analysiert werden. In einer Rechteliste wird festgelegt, welche Dienste zu welcher Zeit über den Packet Filter erlaubt sind. Außerdem kann dem »Code Bits«-Feld durch die Interpretation des ACK-Bits (acknowledge) entnommen werden, in welche Richtung der Verbindungsaufbau durchgeführt wird. So besteht die Möglichkeit, aus Sicherheitsgründen für den Verbindungsaufbau nur eine bestimmte Richtung zu erlauben (siehe unten das Beispiel für den Einsatz von Packet Filtern).

neuKap05.fm Seite 127 Freitag, 18. Oktober 2002 3:51 15

Überprüfung des Verbindungsaufbaus

TCP ist ein verbindungs-orientiertes Kommunikationsprotokoll. Beim Verbindungsaufbau arbeitet TCP immer ohne das ACK-Bit im »Code Bits«-Feld, d.h. ACK=0. Alle weiteren Pakete einer TCP-Verbindung haben dann das ACK-Bit gesetzt, d.h. ACK=1. Dadurch sind TCP-basierte Anwendungen besser durch einen Packet Filter zu kontrollieren (siehe Abb. 5.11).

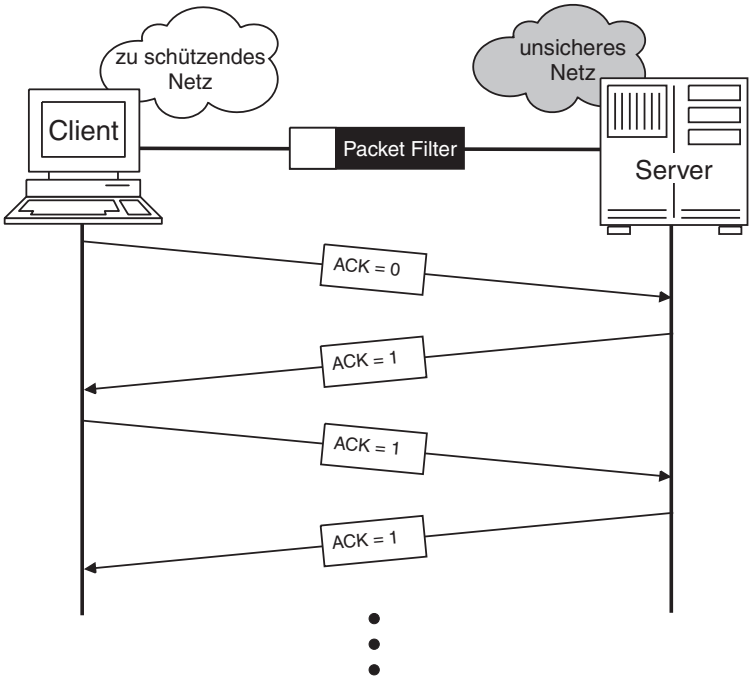


Abb. 5.11: Überprüfung des Verbindungsaufbaus

Filterung bei FTP-Verbindungen

Die FTP-Anwendungen arbeiten mit zwei logischen TCP-Verbindungen. Eine für den Austausch der Kommandos, die andere für den Austausch der Daten. Für den Aufbau dieser logischen TCP-Verbindungen gibt es zwei Methoden, die aktive und die passive Methode aus der Sicht des FTP-Clients /ChZw96/.

FTP-Verbindungsaufbau

Bei einem FTP-Verbindungsaufbau nutzt der Client zwei Portnummern oberhalb 1024 (z.B. 4320 und 4321). Über den ersten Port (z.B. 4320) baut er die TCP-Verbindung für die Kommandos auf. Der Server empfängt die Kommandos über den definierten Port 21.

neuKap05.fm Seite 128 Freitag, 18. Oktober 2002 3:51 15

Im Folgenden werden die beiden Methoden beschrieben, wie der Datenkanal bei der FTP-Anwendung von den Rechnersystemen aufgebaut werden kann.

Aktive Methode

Mit dem Kommando »PORT 4321« teilt der Client dem Server mit, über welche Portnummer der Client die Daten abwickeln will. Der Server sendet die Daten von seinem definierten Port 20 auf die Portnummmer 4321 des Clients.

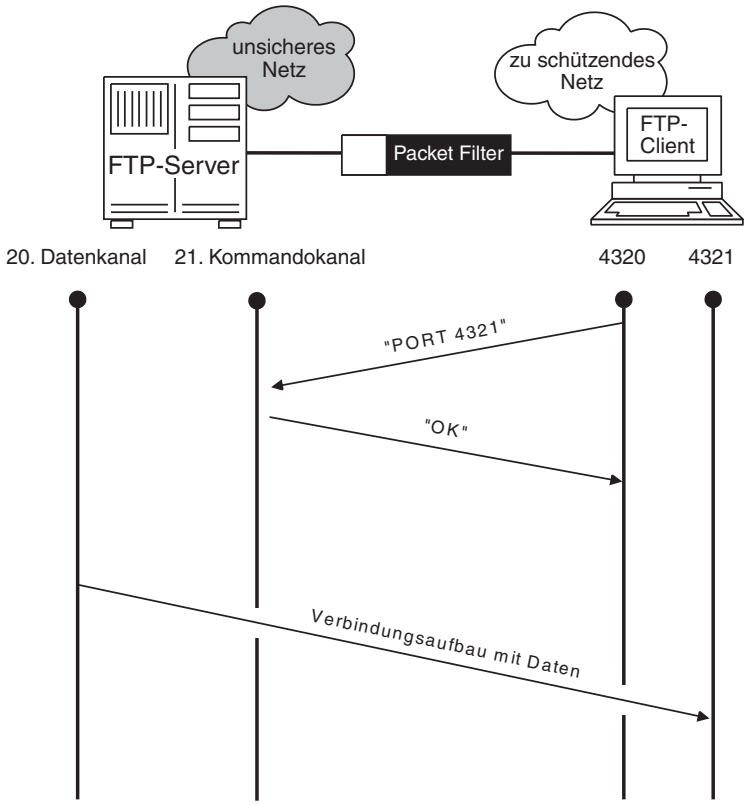


Abb. 5.12: Aktive Methode

Ein Packet Filter, der die Anforderung hat, diese Verbindungen zu kontrollieren, muss für die TCP-Verbindung einen Verbindungsaufbau aus dem unsicheren Netz in das zu schützende Netz ermöglichen. Da dies sicherheitskritisch ist, sollte diese Methode, wenn möglich, nicht verwendet werden. Aus diesem Grund ist es empfehlenswert, die Methode des passiven FTP-Verbindungsaufbaus zu verwenden, bei der der Client den Verbindungsaufbau durchführt.

neuKap05.fm Seite 129 Freitag, 18. Oktober 2002 3:51 15

Passive Methode

Bei der passiven Methode baut der Client die TCP-Verbindung auf. Hierdurch kann eine größere Sicherheit mithilfe eines Packet Filter erreicht werden. In Abb. 5.13 ist die passive Methode dargestellt.

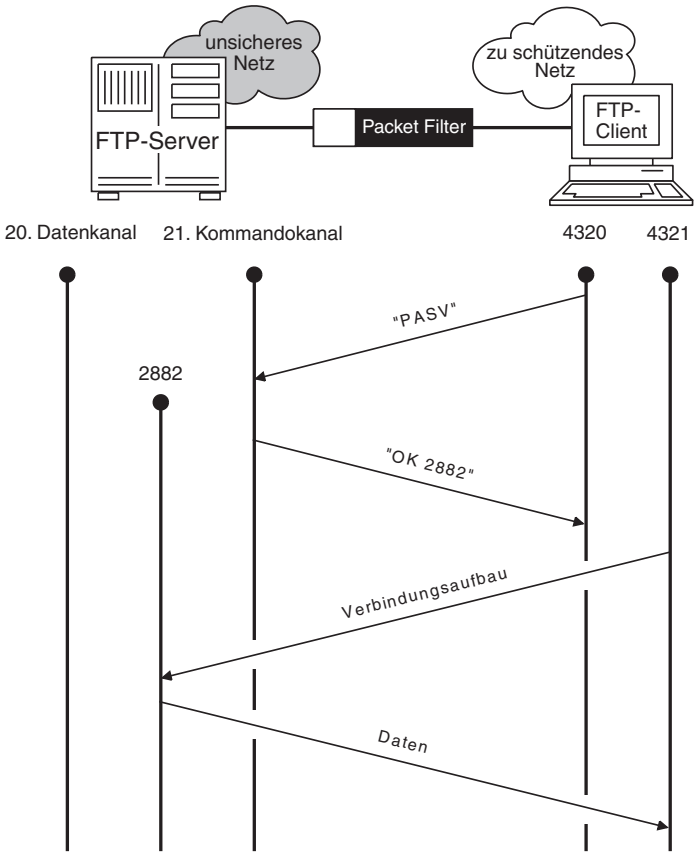


Abb. 5.13: Passive Methode

Aus Sicherheitsgründen ist eine passive Methode zu bevorzugen. Problem ist dabei, dass die passive Methode nicht von allen Client- und Server-Realisierungen angeboten wird.

Weitere mögliche Festlegungen

Zusätzlich sollte in den Packet Filtern pro Filterregel festgelegt werden, zu welchen Zeiten eine Regel (z. B. die Nutzung eines Dienstes) möglich ist, z. B. montags bis freitags von 8.00–17.00 Uhr oder samstags von 8.00–12.00 Uhr und sonntags gar nicht.

neuKap05.fm Seite 130 Freitag, 18. Oktober 2002 3:51 15

5.2.5 Strategien für den Aufbau und die Bewertung der Filterregeln

Es gibt unterschiedliche Ansätze, nach denen die Strategie für den Aufbau und die Bewertung von Filterregeln bestimmt werden kann. Im Folgenden sollen zwei Strategien vorgestellt werden.

Festlegung positiver Filterregeln

- Bei dieser Strategie muss genau festgelegt werden, was erlaubt sein soll.
- Alles, was nicht explizit erlaubt wird, ist automatisch verboten.
- Das Firewall-Element erlaubt nur das, was explizit in der Access-Liste als »erlaubt« gekennzeichnet ist.

Festlegung negativer Filterregeln

- Zunächst ist alles grundsätzlich erlaubt.
- Durch spezielle Einträge kann festgelegt werden, was verboten sein soll.
- Der Packet Filter verhindert nur das, was explizit in der Access-Liste als »nicht erlaubt« gekennzeichnet ist.

Bewertung

Positive Filter sind zu bevorzugen, weil hier nicht dadurch, dass ein Eintrag (Verbot) vergessen wurde, ein Sicherheitsproblem entstehen kann. Negative Filter sind mit Vorsicht zu behandeln, weil durch ungeschickte Festlegungen oder das Vergessen von Einträgen sicherheitskritische Einstellungen auftreten können.

5.2.6 Beispiel für den Einsatz eines Packet Filters

Im Folgenden soll anhand eines Beispiels dargestellt werden, wie mithilfe von Packet Filtern Sicherheit zwischen zwei Netzen, die einen unterschiedlichen Schutzbedarf haben, realisiert werden kann.

In der Abbildung 5.14 sind zwei Netze zu sehen: Netz X mit den IP-Adressen 192.168.3.X und Netz Y mit den IP-Adressen 192.168.5.Y. Die beiden Netze sind voneinander unabhängig, und zwischen ihnen besteht keine Verbindung.

Der Administrator des Server 1 in Netz X arbeitet an der Workstation A in Netz Y und will einen Remote-Zugang auf den Server 1 des Netzes X erreichen. Aus diesem Grund soll von Workstation A aus eine Verbindung zum Server 1 im Netz X aufgebaut werden. Die beiden Netze sollen mithilfe eines Packet Filters gekoppelt werden, wobei nur eine Telnet-Session von Workstation A im Netz Y zum Server 1 im Netz X erlaubt sein soll.

Eigenschaften des Kommunikationsdienstes Telnet

- Telnet basiert auf TCP
- die vom Telnet Server verwendete Standard-Portnummer ist 23 (TCP-Ziel-Portnummer)

neuKap05.fm Seite 131 Freitag, 18. Oktober 2002 3:51 15

- die vom Telnet-Client verwendete TCP-Quell-Portnummer ist eine beliebige Portnummer, die größer ist als 1023

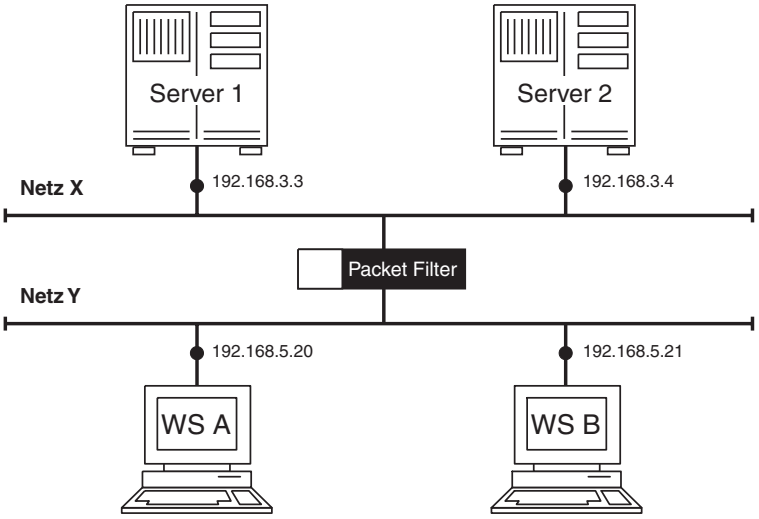


Abb. 5.14: Beispiel für den Einsatz eines Packet Filter

Der Packet Filter arbeitet mit positiven Filterregeln, d.h., es muss definiert werden, was erlaubt sein soll, und alles, was nicht explizit erlaubt wurde, ist automatisch verboten.

Festlegen der Filterregeln

Workstation A darf

- auf Server 1 an Werktagen von 7 bis 17 Uhr den Telnet-Dienst nutzen
- diese Verbindung unter folgenden Voraussetzungen aufbauen:
  - Workstation A muss die IP-Adresse 192.168.5.20 nutzen
  - Server 1 muss die IP-Adresse 192.168.3.3 nutzen
  - das verwendete Transportprotokoll ist TCP
  - der Telnet-Port auf dem Server 1 muss 23 sein
  - der Quell-Port auf Workstation A muss > 1023 liegen

Workstation A darf nicht

- auf Server 1 den Dienst Telnet zu anderen als den festgelegten Zeiten nutzen,
- andere als die festgelegten Dienste in Anspruch nehmen,
- auf andere Rechnersysteme des Netzes X, z.B. Server 2, zugreifen.

neuKap05.fm Seite 132 Freitag, 18. Oktober 2002 3:51 15

Workstation B darf nicht

- auf Server 1 und Server 2 zugreifen.

Die für die Festlegung der oben angeführten Bedingungen notwendigen Filterregeln sind in der folgenden Tabelle 5.1 dargestellt.

Rechner-system	Quell-Adresse	Ziel-Adresse	Transport-protokoll	Quell-Port	Ziel-Port	Erlaubnis zu Verbindungs-aufbau	Wochen-tage	Zeitfenster
A mit S1	192.168.5.20	192.168.3.3	TCP	> 1023	23	ja	Mo.–Fr.	7.00 Uhr–18.00 Uhr
S1 mit A	192.168.3.3	192.168.5.20	TCP	23	> 1023	nein	Mo.–Fr.	7.00 Uhr–18.00 Uhr

Tabelle 5.1: Notwendige Filterregeln

Mit diesen Filterregeln wird genau festgelegt, mit welcher Quell-Adresse die Workstation A auf welche Ziel-Adresse des Servers 1 über TCP zugreifen darf. Zusätzlich wird der Zeitrahmen (Wochentage, Uhrzeit) abgesteckt, innerhalb dessen ein Zugriff erfolgen darf. Für die Antwort wird im Packet Filter genau definiert, von welcher Quell- zu welcher Ziel-Adresse Server 1 mit Workstation A über das TCP-Kommunikationsprotokoll sowie Quell- und Ziel-Port kommunizieren darf. Der Verbindungsaufbau darf nur von der Workstation A an Server 1 erfolgen.

Ergebnis:

Mithilfe des Packet Filter kann genau festgelegt werden, dass die Workstation A zu Server 1 zu bestimmten Zeiten eine Telnet-Session durchführen kann; alle anderen Kommunikationsverbindungen werden durch den Packet Filter aktiv verhindert. Die Kommunikation bleibt für den Administrator, die Workstation A und den Server 1 transparent, d.h., der Packet Filter ist nicht »sichtbar« und benötigt keine anderen Verhaltensvorschriften.

Grenzen von Packet Filtern

Falls auf dem Server 1 am Port 23 ein anderer Dienst aktiviert wurde, kann auch dieser über den Packet Filter durchgeführt werden. Der Packet Filter ist nicht in der Lage festzustellen, ob wirklich ein Telnet-Session oder eine andere Anwendung über den Port 23 gefahren wird. Diese potenzielle Schwachstelle eines Packet Filter muss dem Bedrohungspotenzial entsprechend berücksichtigt werden. Ein solcher Angriff setzt einen internen Angreifer voraus. Daher kann diesem Angriff nur vorgebeugt werden, indem die beiden Kommunikationspartner (Benutzer der Workstation A und Server 1) zusammenarbeiten.

neuKap05.fm Seite 133 Freitag, 18. Oktober 2002 3:51 15

5.2.7 Dynamischer Packet Filter

Im folgenden Abschnitt wird die Arbeitsweise von dynamischen Packet Filtern beschrieben.

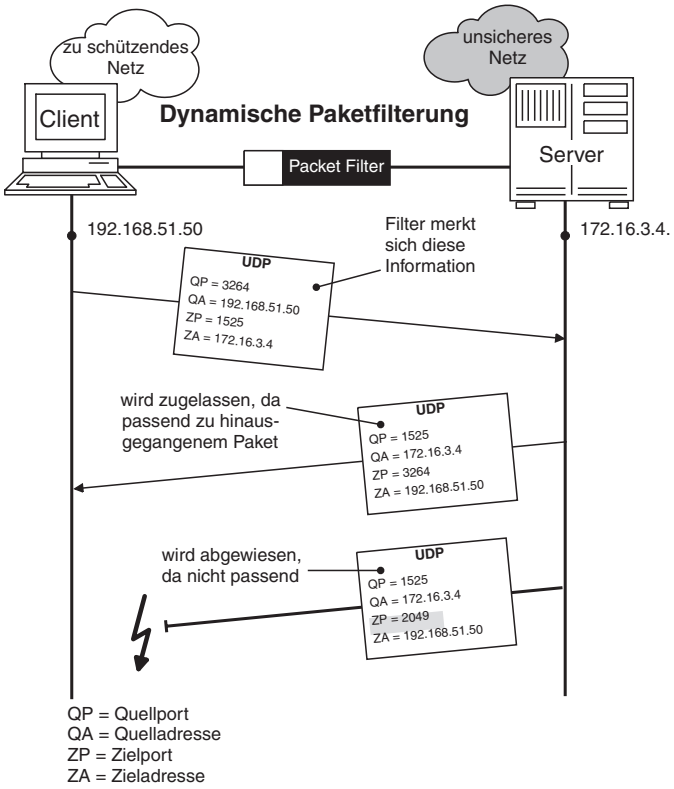


Abb. 5.15: Dynamischer Packet Filter

Bei verbindungslosen Kommunikationsverbindungen, wie z. B. UDP, kann nicht festgestellt werden, von wem ein Verbindungsaufbau durchgeführt wird. Dynamische Packet Filter besitzen im Fall der Verwendung des UDP-Protokolls ferner die Eigenschaft, sich für nach »außen« geschickte UDP-Pakete die Quelle und das Ziel der IP-Adressen und Ports zu merken, und nur die entsprechenden passenden Antworten der virtuellen Verbindung durch den Packet Filter bleiben. Das bedeutet, dass nur Antwortpakete durchgelassen werden, die vom gleichen Rechnersystem und gleichen Port kommen, an den das ursprüngliche UDP-Paket gesendet worden ist, und entsprechend zum gleichen Rechnersystem und gleichen Port zurückgesendet werden. Packet Filter, die diese Eigenschaft besitzen, werden als dynamisch bezeichnet, weil die Filterregeln intern dynamisch angepasst werden. Die angepassten Regeln für die Antwort gelten dann nur temporär und werden

neuKap05.fm Seite 134 Freitag, 18. Oktober 2002 3:51 15

nach einer zu definierenden Zeit, falls keine Antwort kommt, automatisch durch den dynamischen Packet Filter selbst gelöscht.

Der Abb. 5.15 ist zu entnehmen, welche Informationen (Quelladresse und -port, Zieladresse und -port sowie die Zeit, wann das Paket übertragen wurde) im dynamischen Packet Filter festgehalten werden, damit eine genaue Zuordnung stattfinden kann. Diese Eigenschaft kann auch für TCP-Verbindungen verwendet werden.

Dienste wie SNMP können über Packet Filter, die diese Eigenschaft besitzen, sicherer angeboten werden.

5.2.8 Benutzerorientierter Packet Filter

Die Packet Filter arbeiten in der Regel adressorientiert, d.h., sie orientieren sich an den IP-Adressen der Rechnersysteme. Es gibt aber auch Packet Filter, die eine Zuordnung der Verbindungen zu Benutzern schaffen können. Diese Packet Filter werden dann »benutzerorientierte Packet Filter« genannt. In diesem Fall werden die Zugangskontrolle und die Rechteverwaltung in einem Netzwerk mithilfe von Authentikationsverfahren benutzerorientiert definiert. Die folgende Abbildung 5.16 zeigt ein Beispiel eines benutzerorientierten Packet Filter.

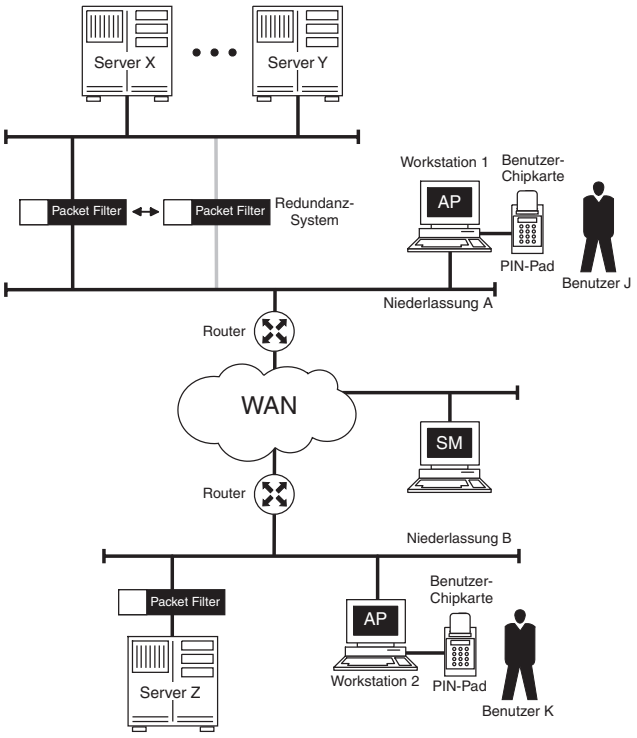


Abb. 5.16: Benutzerorientierter Packet Filter

neuKap05.fm Seite 135 Freitag, 18. Oktober 2002 3:51 15

In diesem Beispiel kontrollieren die benutzerorientierten Packet Filter den Zugriff und die Rechte auf die zu schützenden Netzkomponenten (Server-Systeme X und Y in Abb. 5.16).

Bei der benutzerorientierten Zugangskontrolle wird für jeden Benutzer, der auf eine durch ein Packet Filter geschützte Netzwerkkomponente Zugriffsrechte erhalten soll, mithilfe des Security Management ein Benutzerprofil angelegt. In diesem Benutzerprofil wird festgelegt, welche Kommunikationsprotokolle und Applikationen der einzelne Benutzer zu welchen Zeiten auf welchem Rechnersystem nutzen darf.

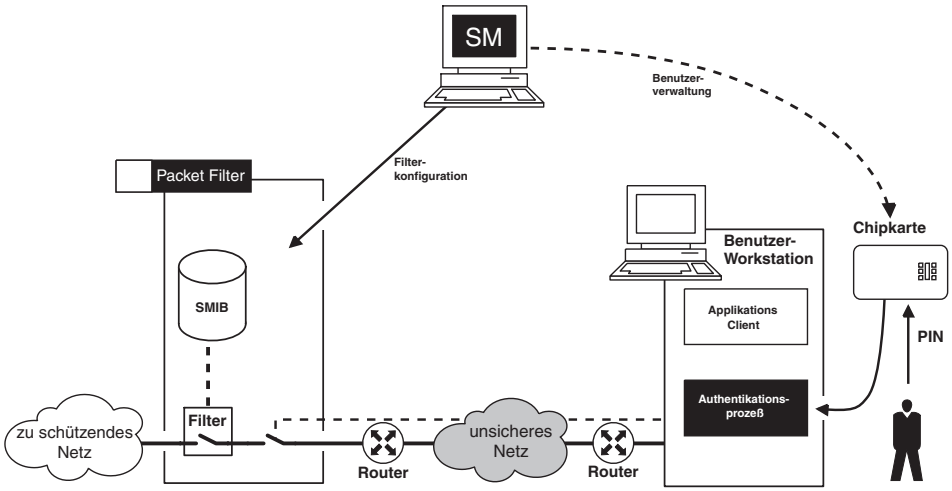


Abb. 5.17: Zugangskontrolle und Rechteverwaltung

Ein Benutzer, der auf ein geschütztes Rechnersystem (Server X oder Server Y) zugreifen will, muss zunächst seine Chipkarte aktivieren, z. B. mithilfe einer PIN (personal identification number). Danach führt ein »Authentication Process (AP)« mithilfe der Chipkarte ein Authentikationsprotokoll mit dem Packet Filter durch. Ist das Authentikationsprotokoll erfolgreich abgelaufen, hat der Packet Filter, stellvertretend für die zu schützenden Rechnersysteme (Server X und Y), den Benutzer identifiziert und authentisiert. Das Kommunikationsprofil des Benutzers wird dynamisch aus der Security-Datenbank (SMIB) in den Packet Filter geladen, d. h., der Benutzer darf dann, seinen Rechten entsprechend, mit den definierten Kommunikationsprotokollen von dem Rechnersystem, von dem er sich authentisiert hat, auf das zu schützende Rechnersystem (Server X oder Server Y) zugreifen.

neuKap05.fm Seite 136 Freitag, 18. Oktober 2002 3:51 15

Der Packet Filter verhindert aktiv, dass ein Benutzer nicht erlaubte Kommunikationsprotokolle verwendet. Falls vom Administrator definiert, würde in diesem Fall eine Spontane Meldung an das Security Management gesendet oder das Ereignis entsprechend in das Logbuch des Packet Filter protokolliert. Nach der Authentikation kann in definierten Zeitabständen die Authentikation zwischen Authentikationsprozess und Packet Filter bzw. zwischen aktivierter Chipkarte und Packet Filter wiederholt werden.

Konzeptionell ist es auch möglich, die Chipkarte für andere Anwendungen einzusetzen, z. B. für die Zugangskontrolle zum Gebäude und die lokale Sicherheit des Rechnersystems. Einige Organisationen nutzen solche Chipkarten, mit denen unterschiedliche Anwendungen realisiert werden können.

Redundanzsystem

Zur Erhöhung der Ausfallsicherheit von Packet Filtern sollte es möglich sein, Packet Filter redundant zu betreiben, damit ihre Verfügbarkeit insgesamt erhöht wird (siehe Abb. 5.16). Eine höhere Verfügbarkeit kann erreicht werden, indem ein zweiter Packet Filter parallel zum aktiven Packet Filter geschaltet wird und als Redundanzsystem im Stand-by-Mode arbeitet. Stand-by-Mode bedeutet, dass der zweite Packet Filter mit derselben Konfiguration wie der aktive Packet Filter betrieben wird, damit beim Ausfall des aktiven Packet Filter das Redundanzgerät spontan die Aufgabe übernehmen kann. Die Kommunikation zwischen den beiden Packet Filtern erfolgt über eine separate zusätzliche Verbindung. Alle Konfigurations-Änderungen, die im aktiven Packet Filter durchgeführt werden, werden dem Redundanz-Packet Filter über diese Verbindung mitgeteilt, wodurch ein zeitnaher Ausgleich der Rechtedaten in den beiden Packet Filtern erreicht wird.

Weitere Aspekte eines benutzerorientierten Packet Filters:

- Durch die Verschlüsselung der Verbindung kann eine anhaltende Authentikation zwischen dem Packet Filter und dem Client realisiert werden (siehe Kapitel 7 *Firewall-Systeme und Verschlüsselung*).
- Das beschriebene Konzept der Benutzerauthentikation ist für single-user-Systeme gedacht. Bei Multiuser-Systemen ist es möglich, dass ein anderer Benutzer die etablierte Verbindung ebenfalls nutzt. In diesem Fall muss je nach Höhe des Bedrohungs- und Schutzbedarfspotenzials entschieden werden, ob dieser Aspekt sicherheitskritisch sein kann.

Beispiele für den Einsatz benutzerorientierter Packet Filter

Im Folgenden soll anhand eines Beispiels dargestellt werden, wie mithilfe von benutzerorientierten Packet Filtern Zugangskontrolle und Rechteverwaltung in einem Netzwerk zur Verfügung gestellt werden können (siehe Abb. 5.16).

neuKap05.fm Seite 137 Freitag, 18. Oktober 2002 3:51 15

Die Server X und Y sind besonders schützenswert und werden aus diesem Grund mithilfe der benutzerorientierten Packet Filter in einem separaten Netz geschützt.

Festlegen der Filterregeln

Der Benutzer K darf

- von der Workstation 2 mithilfe von FTP Dateien auf den Server X übertragen,
- ausschließlich mittwochs von 8.00 Uhr bis 12.00 Uhr auf den Server X zugreifen.

Der Benutzer J darf

- von der Workstation 1 mit dem Kommunikationsprotokoll IPX den Novell-Server Y nutzen,
- und zwar montags bis freitags von 7.00 Uhr bis 19.00 Uhr.

Voraussetzungen:

- Benutzer Y und J besitzen persönliche Chipkarten.
- Die Workstations 1 und 2 verfügen über Chipkartenleser und eine Software, die den Authentication Process durchführt, mit dem die Authentikation mit den Packet Filtern realisiert werden kann.
- Quell- und Ziel-Rechnersystem sind über definierte Adressen adressierbar.
- Server X über eine IP-Adresse
- Server Y über eine IPX-Adresse
- Server X verwendet Standard-Portnummern für FTP.

Die für die Festlegung der oben angeführten Bedingungen notwendigen Filterregeln sind in der folgenden Tabelle 5.2 dargestellt.

Benutzer	Quell-Rechnersystem	Ziel-Rechnersystem	Protokoll	Anwendung	Wochentage	Zeitfenster
K	Workstation 2	Server X	IP	FTP	Mi.	8.00 Uhr –12.00 Uhr
J	Workstation 1	Server Y	IPX	*	Mo.–Fr.	7.00 Uhr –19.00 Uhr

Tabelle 5.2: Filterregeln

Ergebnis:

Mithilfe eines benutzerorientierten Packet Filters kann genau festgelegt werden, dass bestimmte Benutzer von bestimmten Rechnersystemen zu bestimmten Zeiten und Wochentagen über definierte Protokolle über einzustellende Anwendungen (Dienste) mit festzulegenden Servern eine Kommunikation im zu schützenden Netz durchführen können.

neuKap05.fm Seite 138 Freitag, 18. Oktober 2002 3:51 15

5.2.9 Sicherheitsrelevante Informationen in einem Packet Filter

In einem Packet Filter können Verstöße gegen die Filterregeln auf den verschiedenen Kommunikationsebenen als sicherheitsrelevante Ereignisse protokolliert werden. Die Protokolldaten der sicherheitsrelevanten Ereignisse sind für die Erkennung von Sicherheitsverletzungen wichtig und stellen somit einen wichtigen Sicherheitsmechanismus dar, mit dem Angriffe erkannt werden können (siehe Kapitel 13.1 *Logbuchdaten – Belastung oder Nutzen?*).

Bei sicherheitsrelevanten Ereignissen sollten folgende Informationen in das Logbuch des Packet Filter eingetragen werden:

- Datum und Uhrzeit, wann das Ereignis aufgetreten ist
- Laufzähler für die fortlaufende Nummerierung der Ereignisse
- Art des sicherheitsrelevanten Ereignisses, das aufgetreten ist
- IP-Adressen und Portnummer (Dienst) und evtl.
- Protokoll der Informationen des IP-Paketes

Für das Logbuch sollten, der jeweiligen Sicherheitspolitik entsprechend, folgende Modi betrieben werden können:

Free-Run-Modus

Das Logbuch arbeitet wie ein Ringpuffer, d.h., bei einem Überlauf des Logbuches wird der älteste Logbucheintrag überschrieben.

Bei diesem Modus werden immer die neuesten sicherheitsrelevanten Ereignisse festgehalten. Bei dieser Methode besteht allerdings die Gefahr, dass ein Angreifer durch das Erzeugen von anderen, neuen Ereignissen den eigentlichen Angriffsversuch im Nachhinein verschleiern könnte.

Single-Shot-Modus

Bei diesem Modus werden bei einem Überlauf des Logbuches die neuen Logbucheinträge verworfen, und die alten sicherheitsrelevanten Ereignisse bleiben erhalten.

Bei dieser Methode besteht die Gefahr, dass ein Angreifer durch das Erzeugen anderer Ereignisse im Vorfeld seines Angriffes den eigentlichen Angriff erfolgreich verschleiern könnte.

block if full

Bei diesem Modus wird bei einem Überlauf des Logbuches der Packet Filter in den Block-Mode geschaltet, d.h., es werden überhaupt keine Pakete mehr durchgelassen.

Vorteil dieser Methode ist, dass keine sicherheitsrelevanten Ereignisse verlorengehen. Bei dieser Methode besteht die Gefahr, dass ein Angreifer durch das Erzeugen von sicherheitsrelevanten Ereignissen die Kommunikation über den Packet Filter

neuKap05.fm Seite 139 Freitag, 18. Oktober 2002 3:51 15

verhindern und damit die Verfügbarkeit des zu schützenden Netzes von außen behindern könnte.

Man kann die o. a. Gefahren eliminieren indem festgelegt wird, dass eine Warnmeldung an das Security Management gesendet wird, falls das Logbuch überzulaufen droht (z. B. wenn es zu 75% gefüllt ist). Diese Meldung veranlasst das Security Management, das Logbuch sofort auszulesen, und so Platz für neue Einträge sicherheitsrelevanter Ereignisse mit den entsprechenden Protokolldaten zu schaffen. Auf diese Weise können keine Informationen verlorengehen, und der Packet Filter wird nicht blockiert.

Packet Filter sollten so konfigurierbar sein, dass definiert werden kann, welche sicherheitsrelevanten Ereignisse in das Logbuch eingetragen werden sollen und welche nicht, weil sie z. B. in einer bestimmten Organisation keine besondere Aussagekraft haben.

5.2.10 Realisierungsformen für Packet Filter

Es gibt unterschiedliche Möglichkeiten, eine Packet-Filter-Funktionalität zur Verfügung zu stellen. Die gängigsten Möglichkeiten sind, die Packet-Filter-Funktionalität in einem Router zu integrieren oder als separate Sicherheitskomponente anzubieten.

Packet Filter Realisierung im Router

Viele Router, die für die Sicherung der Netze verwendet werden sollen, bieten heute Packet Filter-Funktionalität an. Die in solchen Routern integrierten Sicherheitsfunktionalitäten sind hinreichend für interne Anwendungen, die nicht besonders sicherheitsrelevant sind, und bieten für diese Fälle eine preiswertere Lösung als separate Sicherheitskomponenten.

Router mit Packet Filter-Funktionalitäten haben jedoch einige Schwächen:

- Der Tiefengrad der Analyse ist in der Regel flacher als bei einem speziellen Packet Filter.
- Die meisten Router bieten, weil sie keine Sicherheitsprodukte sind, nur eine unzureichende Administration der Sicherheitsfunktionen: Weil das Security Management fehlt, werden Fehleinstellungen gemacht, die immer wieder für Sicherheitslöcher sorgen.
- Router haben in der Regel nur unvollständige Protokollierungsmöglichkeiten und keinen Alarmierungsmechanismus für sicherheitsrelevante Ereignisse.
- Router sind schlecht gegen Angriffe gerüstet, die auf die Sicherheitsmechanismen selbst gerichtet sind. Es fehlen Sicherheitsmechanismen, die solchen Angriffen entgegenwirken, sodass oft die Möglichkeit besteht, von außen über

neuKap05.fm Seite 140 Freitag, 18. Oktober 2002 3:51 15

Management-Funktionen die Packet-Filter-Funktionalitäten auszuschalten oder die Regeln zu ändern.

- Router sollen die Vermittlung von Paketen optimal und schnell durchführen. Die dazu benötigte Software ist sehr komplex und ist damit anfällig für Implementierungsfehler (siehe Kapitel 5.1.2 *Designkonzept aktiver Firewall-Elemente*).
- In der Praxis nimmt die Performance bei einigen Routern so stark ab, dass die eigentlichen Aufgaben des Routers nicht in der erforderlichen Geschwindigkeit durchgeführt werden können.
- Ein neuer Router, der für diese Aufgabe erst angeschafft werden muss, ist teurer als eine separate Sicherheitskomponente.
- Oft liegt die Verantwortung für den Betrieb der Router in einem anderen Bereich (andere Abteilung oder andere Firma, z. B. Netzdienstanbieter usw.), was die Einhaltung der Sicherheitspolitik schwierig bis unmöglich machen kann.

Packet Filter als separate Sicherheitskomponenten

Packet Filter als separate Sicherheitskomponenten haben die Hauptaufgabe, die Sicherheit zwischen einem unsicheren und einem zu schützenden Netz zu realisieren.

Vorteile:

- Packet Filter können die sicheren Designkriterien von aktiven Firewall-Elementen leichter erfüllen als Router, weil sie keine zusätzliche Software für andere Aufgabenstellungen benötigen.
- Mit Packet Filtern wird eine klare Abgrenzung zwischen Kommunikations- und Sicherheitsanforderungen geschaffen.
- Packet Filter bieten in der Regel ein separates Security Management, das auch zentral für die Verwaltung mehrerer Packet Filter verwendet werden kann, wodurch eine einheitliche und kontrollierbare Sicherheitspolitik einfach umgesetzt werden kann.
- Separate Sicherheitskomponenten sind flexibler als Router mit Packet Filter-Funktionalität, weil sie unabhängig von anderen Funktionalitäten sind.

Nachteile:

- Packet Filter sind oft teurer als Software-Erweiterungen im Router.
- Ein Packet Filter bedeutet zusätzliche Hardware, was prinzipiell die Verfügbarkeit der Netzdienste reduziert.

Packet Filter im Microchip:

Einige Hersteller bieten Packet Filter-Funktionalitäten in Form von Mikrochips an, die eine sehr hohe Performance erreichen und einfach in Kommunikationseinrichtungen integriert werden können.

neuKap05.fm Seite 141 Freitag, 18. Oktober 2002 3:51 15

5.2.11 Anwendungsgebiete von Packet Filtern

Ein Firewall-System, das nur auf Packet Filtern aufbaut, wird sicherlich nicht für die Kopplung eines zu schützenden Netzes an das Internet eingesetzt werden können, da der Schutzbedarf der meisten zu schützenden Netze für die Kontrollmöglichkeiten eines Packet Filter zu hoch ist.

Packet Filter werden zum Aufbau von High-level-Security-Firewall-Systemen und für die kontrollierte Kommunikation im Intranet verwendet (siehe Kapitel 10 *Praktischer Einsatz von Firewall-Systemen*). Für diese Anwendungen sind besonders Packet Filter, die gleichzeitig verschlüsseln, eine wirkungsvolle Sicherheitskomponente, mit der Internet- und Intranet-Anwendungen sicher und beherrschbar realisiert werden können (siehe Kapitel 7 *Firewall-Systeme und Verschlüsselung*).

Möglichkeiten, Vorteile und besondere Aspekte von Packet Filtern

- transparent, d.h. unsichtbar für den Benutzer und die Rechnersysteme und ohne ihre aktive Einwirkung tätig (Ausnahme: wenn eine Authentikation notwendig ist)
- einfach erweiterungsfähig für neue Protokolle
- flexibel für neue Dienste
- für andere Protokollfamilien verwendbar (IPX, OSI, DECNET, SNA...)
- hohe Performance durch optimale Mechanismen (Betriebssystem, Treiber usw.)
- leicht realisierbar, da geringere Komplexität

Nachteile und Grenzen von Packet Filtern

- Daten, die oberhalb der Transportebene liegen, werden in der Regel nicht analysiert.
- Für die Anwendungen (FTP, HTTP, ...) besteht keine Sicherheit, z.B. können bei der Freischaltung von SMTP (Port 25) Angriffe über Sendmail auf den Rechnersystemen des zu schützenden Netzes durchgeführt werden.
- Falsch konfigurierte Programme auf Rechnersystemen im zu schützenden Netz können bei erlaubten Kommunikationsverbindungen von außen genutzt werden, da ein direkter Zugriff auf das Rechnersystem besteht.
- Typische Packet Filter können die Struktur des zu schützenden Netzes nicht verbergen.
- Protokolldaten werden nur bis zur Transportebene zur Verfügung gestellt.

neuKap05.fm Seite 142 Freitag, 18. Oktober 2002 3:51 15

5.3 Zustandsorientierte Packet Filter (stateful inspection)

Der Leistungsumfang von Packet Filtern kann erweitert werden, indem die Interpretation der Pakete auch auf höheren Kommunikationsebenen durchgeführt wird. In diesem Fall werden die Pakete z. B. auch auf der Anwendungsebene interpretiert und Statusinformationen für jede aktuelle Verbindung auf den unterschiedlichen Kommunikationsebenen bewertet und festgehalten.

Analogie zum Pförtner

Wenn die Lieferung ankommt, dann schaut der Pförtner nicht nur auf die Adressen, sondern er prüft auch den Lieferschein, um zu überprüfen, ob sich in dem Paket etwas Verbotenes befindet. Das ist eine gute Überprüfung, jedoch nicht so sicher, wie das tatsächliche Öffnen des Pakets und die Überprüfung des Inhaltes. Wenn das Paket akzeptabel aussieht, dann öffnet der Pförtner das Tor und gestattet dem Fahrer des Lkws den Zutritt auf das Werksgelände.

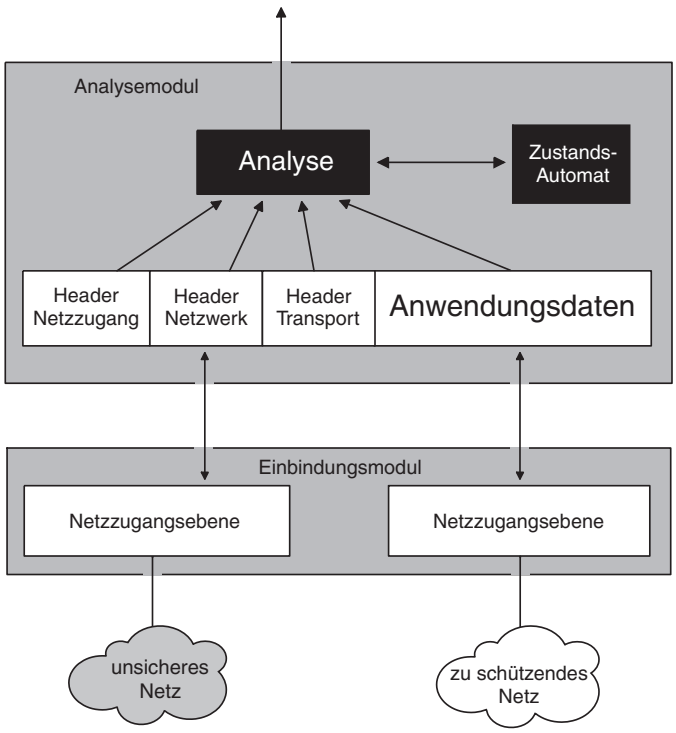


Abb. 5.18: Zustandsorientierte Packet Filter

neuKap05.fm Seite 143 Freitag, 18. Oktober 2002 3:51 15

Die Statusinformationen können in Form von »Zuständen« mit den entsprechenden Informationen festgehalten werden. Zustände sind z. B. Verbindungsaufbau, Transferzustand oder Verbindungsabbau für die jeweilige Kommunikationsebene. In jedem Zustand kann dann eine andere Interpretation der Kommunikationsdaten erfolgen. In der Literatur werden solche erweiterten zustandsorientierten Packet Filter »stateful inspection«, »smart filtering« oder »adaptive screening« genannt. Mit dieser erweiterten Funktionalität werden sie oft als benutzerorientierte Packet Filter angeboten.

Diese zustandsorientierten Packet Filter haben die Vorteile von Packet Filtern, können aber zusätzlich die Anwendungen kontrollieren. Einige Risiken bleiben, weil keine direkte Entkopplung der Dienste realisiert ist (siehe Beschreibung und Vorteile der Proxies auf Application Gateways).

Das gleichzeitige Festhalten und Interpretieren der Kommunikationsdaten auf den verschiedenen Kommunikationsebenen ist sehr komplex. Aus diesem Grund haben zustandsorientierte Packet Filter in der Regel eine geringere Tiefe der Analyse oder sind besonders fehleranfällig, da sie eine sehr mächtige Software haben. Prinzipiell ist es auch nicht möglich, die komplexe Software von zustandsorientierten Packet Filtern soweit auszutesten, dass in nachweislich keinem Betriebszustand Fehler auftreten können. Aus diesem Grund muss auch in Zukunft immer wieder damit gerechnet werden, dass die komplexen Programme potenzielle Sicherheitsrisiken aufweisen, die für Angriffe verwendet werden können.

Möglichkeiten, Vorteile und besondere Aspekte von zustandsorientierten Packet Filtern:

- wenn keine Authentikation notwendig ist: transparent, d. h. unsichtbar für den Benutzer und die Rechnersysteme und ohne ihre aktive Einwirkung tätig
- einfach erweiterungsfähig für neue Protokolle
- flexibel für neue Dienste
- eventuell für andere Protokollfamilien verwendbar (IPX, OSI, DECNET, SNA...)

Nachteile und Grenzen von zustandsorientierten Packet Filtern:

- Komplexität der Lösung
- falsch konfigurierte und fehlerbehaftete Programme auf Rechnersystemen im zu schützenden Netz können bei erlaubten Kommunikationsverbindungen von außen genutzt werden, da ein direkter Zugriff auf das Rechnersystem besteht
- typische zustandsorientierte Packet Filter können die Struktur des zu schützenden Netzes nicht verbergen

Ein besseres und sicheres Konzept der Analyse der Anwendungsdaten ist das Konzept von Application Gateways mit Proxies, welches im folgenden Abschnitt beschrieben wird.

neuKap05.fm Seite 144 Freitag, 18. Oktober 2002 3:51 15

5.4 Application Gateway/Proxy-Technik

Im folgenden Abschnitt wird die Arbeitsweise des aktiven Firewall-Elements »Application Gateway« beschrieben.

Das Application Gateway zeichnet sich dadurch aus, dass es die Netze sowohl logisch als auch physikalisch entkoppeln kann.

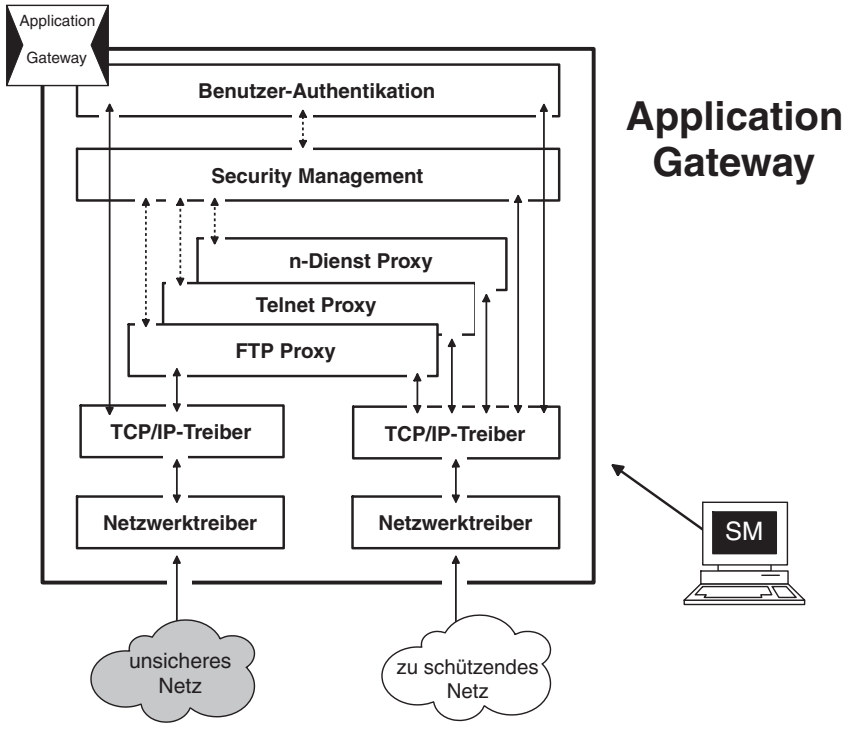


Abb. 5.19: Application Gateway

Da in einigen Firewall-Konzepten das Application Gateway das einzige vom unsicheren Netz (z.B. Internet) aus erreichbare Rechnersystem ist, muss das Application Gateway besonders geschützt werden. Aus diesem Grund wird das Rechnersystem, auf dem das Application Gateway realisiert ist, auch als Bastion bezeichnet.

Das Application Gateway – als Dual-homed Gateway realisiert – arbeitet mit zwei Netzwerk-Anschlüssen. »Dual-homed« bedeutet, dass das Application Gateway die vollständige Kontrolle über die Pakete hat, die zwischen dem unsicheren und dem zu schützenden Netzwerk übertragen werden sollen.

neuKap05.fm Seite 145 Freitag, 18. Oktober 2002 3:51 15

Das Application Gateway kann auch als Single-homed mit nur einem Netzwerkanschluss betrieben werden. Dann besteht jedoch die Möglichkeit, dass ein Angreifer das Application Gateway übergeht (siehe Kapitel 6 *Konzepte für Firewall-Systeme*).

Analogie zum Pförtner

Der Application-Gateway-Pförtner schaut nicht nur die Adressen der eingehenden Lieferungen an, er öffnet auch jedes Paket und prüft den kompletten Inhalt und checkt die Arbeitspapiere des Absenders gegen eine klar festgelegte Reihe von Beurteilungskriterien. Nach der erfolgten detaillierten Sicherheitsüberprüfung unterzeichnet der Pförtner den Lieferschein und schickt den LKW wieder auf seinen Weg. Stattdessen bestellt er einen vertrauenswürdigen Fahrer der eigenen Firma, der nun die Pakete zum eigentlichen Empfänger bringt. Die Sicherheitskontrolle ist an dieser Stelle wesentlich zuverlässiger und der Fahrer der Fremdfirma erhält keinen weiteren Einblick in das Firmengelände. Die Überprüfungen nehmen zwar mehr Zeit in Anspruch, dafür können jedoch sicherheitsgefährdende Aktivitäten ausgeschlossen werden.

5.4.1 Allgemeine Arbeitsweise des Application Gateway

Ein Benutzer, der über das Application Gateway kommunizieren möchte, muss sich zuerst identifizieren und authentisieren. Application Gateways bieten in der Regel unterschiedliche Authentikationsverfahren an (siehe Kapitel 8 *Authentikationsverfahren*).

Aus diesem Grund baut der Benutzer zuerst eine Verbindung mit dem Application Gateway auf. Der direkte Kommunikationspartner ist nicht sein Ziel-Rechnersystem, sondern das Application Gateway. Nach der Identifikation und Authentikation arbeitet das Application Gateway aber transparent, sodass der Benutzer den Eindruck hat, direkt auf dem Ziel-Rechnersystem zu arbeiten.

Grundsätzlicher Ansatz

Über die Netzzugangs- und TCP/IP-Treiber empfängt das Application Gateway die Pakete an den entsprechenden Ports. Soll nur ein Dienst über einen entsprechenden Port möglich sein, muss auf dem Application Gateway eine Software zur Verfügung gestellt werden, die das entsprechende Paket von der einen Netzwerkseite zur anderen Netzwerkseite des Application Gateway überträgt und umgekehrt. Eine solche Software, die die Paketübertragung nur für einen speziellen Dienst (FTP, HTTP, Telnet, usw.) im Application Gateway durchführt, wird als Proxy bezeichnet (siehe Abb. 5.19).

Der Name Proxy – Stellvertreter – wird verwendet, weil es aus Sicht des zugreifenden Benutzers so aussieht, als würde er mit dem eigentlichen Server-Prozess des Dienstes auf dem Ziel-Rechnersystem kommunizieren.

neuKap05.fm Seite 146 Freitag, 18. Oktober 2002 3:51 15

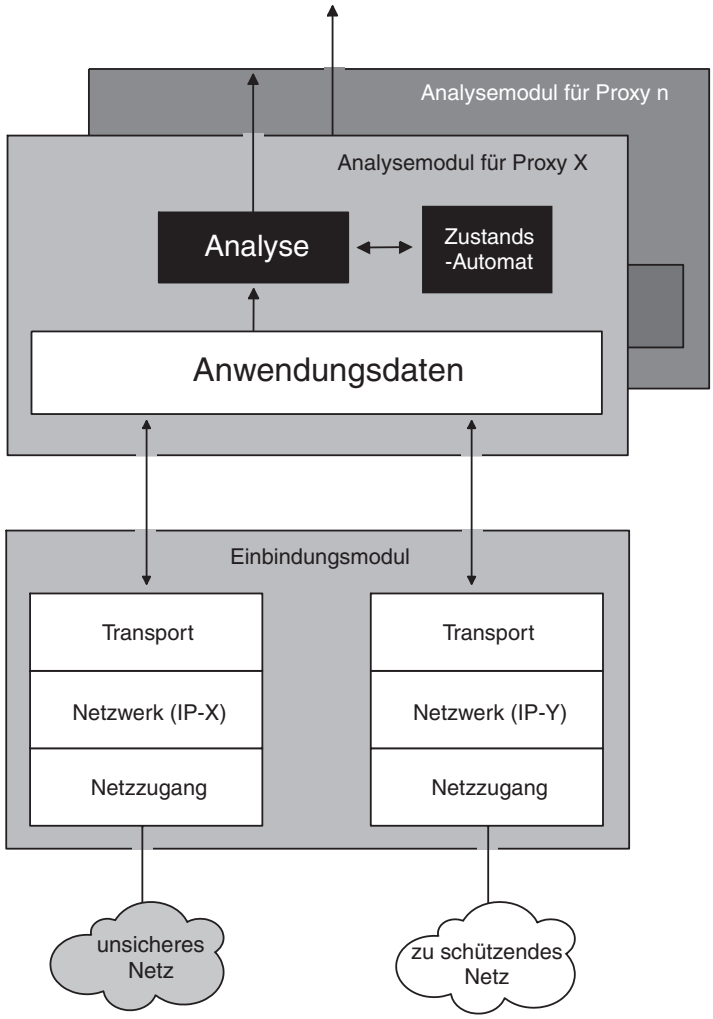


Abb. 5.20: Analysemodule für Proxies auf dem Application Gateway

Jeder Proxy auf dem Application Gateway kann speziell für den Dienst, für den er zuständig ist, weitere Sicherheitsdienste anbieten. Bedingt durch den jeweiligen speziellen Proxy und das Wissen um den Kontext eines speziellen Dienstes ergeben sich umfangreichere Sicherungs- und Protokollierungsmöglichkeiten im Application Gateway (siehe dazu die Beschreibung der speziellen Proxies).

Die Analyse ist auf dieser Kommunikationsebene besonders intensiv möglich, da der Kontext der Anwendungsdaten für den jeweiligen Dienst klar definiert ist. Die Proxies konzentrieren sich auf das Wesentliche. Der Vorteil ist, dass kleine überschaubare Module verwendet werden, wodurch die Fehleranfälligkeit durch Implementationsfehler reduziert wird (siehe Abb. 5.20).

neuKap05.fm Seite 147 Freitag, 18. Oktober 2002 3:51 15

Sicherheitskonzept eines Application Gateway

Für jeden Dienst, der über das Application Gateway möglich sein soll, muss ein spezieller Proxy zur Verfügung gestellt werden.

Sollen bestimmte Dienste generell nicht möglich sein, dann darf für diese Dienste kein Proxy auf dem Application Gateway vorhanden sein, aber auch keine weitere Software, die den Dienst ermöglichen könnte!

Aus diesem Grund ist so wenig Software wie möglich auf dem Application Gateway zu installieren, damit nicht zufällig – oder absichtlich durch einen Angreifer von außen provoziert – eine andere Software die Aufgabe eines Proxys (Paketübertragung im Application Gateway) für einen Dienst übernimmt, der nicht erlaubt sein soll.

Das Security Management, das dem Benutzer die Arbeit so leicht wie möglich gestalten soll und deshalb mit einer mächtigen Software (X-Terminal, Datenbank, ...) ausgestattet ist, darf aus Sicherheitsgründen nicht auf demselben Rechnersystem laufen oder zumindest nicht zur gleichen Zeit wie das Application Gateway.

Application Gateways sollen aus Sicherheitsgründen keine Routing-Funktionalität haben, damit nicht an den Proxies vorbeigeroutet werden kann.

Da das Application Gateway bei der Kommunikation jeweils zum Rechnersystem des unsicheren Netzes und zu dem des zu schützenden Netzes eine Kommunikationsverbindung hat, bietet das Application Gateway eine »Network Address Translation«. Dazu hat das Application Gateway eine IP-Adresse im unsicheren Netz (z. B. eine offizielle Internet IP-Adresse 194.173.3.1) und eine IP-Adresse im zu schützenden Netz (z. B. eine für diesen Zweck reservierte IP-Adresse 192.168.1.60). Bei der Kommunikation mit den Rechnersystemen des unsicheren Netzes verwendet das Application Gateway die IP-Adressen des unsicheren Netzes, und bei der Kommunikation mit den Rechnersystemen des zu schützenden Netzes verwendet das Application Gateway die IP-Adressen des zu schützenden Netzes (siehe auch Kapitel 12.1 *Network Address Translation*).

5.4.2 Die Proxies

Bei der Realisierung von Proxies wird zwischen Application Level und Circuit Level Proxies unterschieden.

5.4.2.1 Application Level Proxies

Application Level Proxies sind für bestimmte Dienste/Anwendungen implementiert. Das heißt, sie kennen die Kommandos der Anwendungsprotokolle und können diese analysieren und kontrollieren. Application-Level Proxies arbeiten mit der gängigen, unveränderten Client-Software für FTP, Telnet oder auch Browser zusammen. Bei Application Level Proxies ist aber für die benutzerorientierten

neuKap05.fm Seite 148 Freitag, 18. Oktober 2002 3:51 15

Dienste oft eine veränderte Vorgehensweise notwendig, z. B. ist zuerst eine Identifikation und Authentikation mit dem Application Level Proxy notwendig, und anschließend wird eine transparente Kommunikation für den Benutzer zur Verfügung gestellt (siehe hierzu auch die Kommunikation über Application Level Proxies).

Im folgenden Kapitel werden einige Application Level Proxies am Beispiel bestimmter Realisierungsarten näher beschrieben, um das Grundprinzip der Proxy-Technik darzustellen. Einige Proxies funktionieren nach dem Store-and-Forward-Prinzip (SMTP), andere interaktiv und benutzerorientiert (Telnet, FTP, HTTP, ...).

5.4.2.2 SMTP Proxy

Abb. 5.21 zeigt, wie ein SMTP Proxy, der nach dem Store-and-Forward-Prinzip arbeitet, aufgebaut werden kann. Store-and-Forward-Prinzip bedeutet, der SMTP Proxy nimmt die Mail vollständig an, speichert diese zwischen und sendet die Mail dann weiter. Hierfür ist keine End-to-End-Beziehung zwischen dem eigentlichen Sender und Empfänger notwendig.

Analogie zum Sammelbriefkasten (Mail Proxy)

Ein Mail Proxy kann mit einem Sammelbriefkasten einer Organisation verglichen werden. Möchte jemand einer Organisation einen Brief senden, so wirft er diesen direkt oder indirekt in den Sammelbriefkasten der Organisation. Die Briefe werden dort von der internen Poststelle entgegengenommen und mit einem Boten der eigenen Organisation verteilt. Die externen Briefboten brauchen die Organisation also nicht zu betreten und stellen somit auch kein Risiko dar. Der Schlitz nach außen definiert die potenzielle Angriffsfläche.

Bei SMTP Proxies gibt es Lösungen, die ohne oder mit einem auf dem gleichen System vorhandenen MTA (Message Transfer Agent) arbeiten. Im Beispiel wird ein SMTP Proxy mit vorhandenem MTA beschrieben.

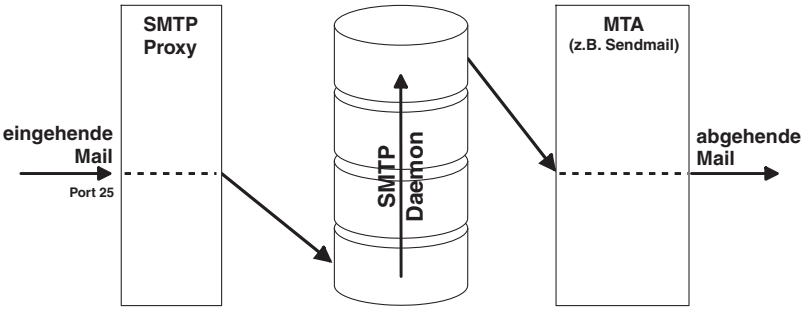


Abb. 5.21: SMTP Proxy

neuKap05.fm Seite 149 Freitag, 18. Oktober 2002 3:51 15

Beschreibung

Der SMTP Proxy arbeitet nicht benutzerorientiert. Aus diesem Grund ist hier auch keine Benutzerauthentikation erforderlich.

Eine einkommende Mail wird von einem SMTP Proxy auf Port 25 entgegengenommen und nach Überprüfung des Absenders (IP-Adresse und Rechnername des Mail Servers) auf dem Application Gateway in einem speziellen Verzeichnis abgelegt. Der SMTP Daemon prüft periodisch, ob Mails eingegangen sind. Das Mail Transfer Agent (MTA) stellt dem Adressaten die Mail direkt oder über einen oder mehrere MTAs zu. Der SMTP Proxy verhindert damit, dass der MTA direkt vom unsicheren Netz angesprochen werden kann.

Ein solches MTA ist z. B. Sendmail, das häufig eingesetzt wird, und das bekanntlich eine Vielzahl von Sicherheitslücken und Implementierungsfehlern aufweist (siehe auch Kapitel 4.5 *Angriffsmethoden und prinzipielle Gegenmaßnahmen auf der Grundlage der TCP/IP-Protokolle*).

Ein SMTP Proxy verarbeitet nur die folgenden Befehle, weil sie nicht sicherheitskritisch sind:

- HELO
- MAIL
- RCPT
- DATA
- QUIT
- RSET
- NOOP

Einige weitere Befehle werden mit Standardantworten bedient, damit eine Kommunikation ermöglicht werden kann:

- HELP
- VRFY
- EXPN

Bei sicherheitsrelevanten Befehlen wie

- DEBUG

wird eventuell direkt eine Warnmeldung an das Security Management gesendet.

Falls der Befehl debug in einem SMTP-Proxy erkannt wird, kann dadurch kein Fehler auftreten, weil der SMTP-Proxy darauf nicht reagiert. Da aber ein Fremder versucht, einen debug-Befehl durchzuführen, kann die Tatsache dahingehend interpretiert werden, dass sich dahinter ein Angriffsversuch verbirgt. Diese Information über einen Angriffsversuch kann wichtig sein.

neuKap05.fm Seite 150 Freitag, 18. Oktober 2002 3:51 15

Durch die Verwendung des Store-and-Forward-Prinzips wird z. B. eine Entkopplung des komplexen und fehlerbehafteten Programms Sendmail (MTA) erreicht. So werden bekannte Angriffe über Sendmail verhindert, denn mithilfe der Befehle kann Sendmail nicht direkt angesprochen werden, sondern nur die Stellvertreter-Software der SMTP Proxies. Der SMTP Proxy ist überschaubar und damit eine gut testbare Software.

Logbuch

In das Logbuch des Application Gateway können durch den SMTP Proxy die folgenden Protokolldaten festgehalten werden:

- IP-Adresse und Rechnername des Quell-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Absender der Mail (wie im Kopf der Mail angegeben)
- Adressat der Mail (wie im Kopf der Mail angegeben)
- Anzahl der übertragenen Bytes
- Uhrzeit und Datum des Verbindungsabbaus

In das Logbuch des Application Gateway werden durch den Message Transfer Agent (MTA) die folgenden Protokolldaten festgehalten:

- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Absender der Mail (wie im Kopf der Mail angegeben)
- Adressat der Mail (wie im Kopf der Mail angegeben)
- Anzahl der übertragenen Bytes
- Uhrzeit und Datum des Verbindungsabbaus

Wenn ein Problem auftritt, können die umfangreichen Protokolldaten der Ereignisse im SMTP Proxy verwendet werden, um es zu lösen (siehe Kapitel 13.1 *Logbuchdaten – Belastung oder Nutzen?*).

5.4.2.3 Benutzerorientierte Application Level Proxies

Die folgenden Proxies für Telnet, FTP und HTTP sind benutzerorientierte Proxies, die selbst eine Authentikation mit dem entsprechenden Benutzer durchführen, wie ein Pförtner. Im Falle einer erfolgreichen Identifikation und Authentikation eines Benutzers mit dem Proxy gilt diese Authentikation auch nur für diesen speziellen Proxy. Falls der Benutzer einen anderen Dienst, d.h. einen anderen Proxy nutzen möchte, muss eine erneute Identifikation und Authentikation stattfinden. Benutzeroriente Proxies haben den Vorteil, dass die Zuordnung zwischen Benutzer und IP-Adresse und dem gewünschten Dienst eindeutig und lückenlos ist.

Im Folgenden wird der Verbindungsaufbau über das Application Gateway mithilfe eines einfachen Passwortverfahrens für benutzerorientierte Dienste exemplarisch dargestellt.

neuKap05.fm Seite 151 Freitag, 18. Oktober 2002 3:51 15

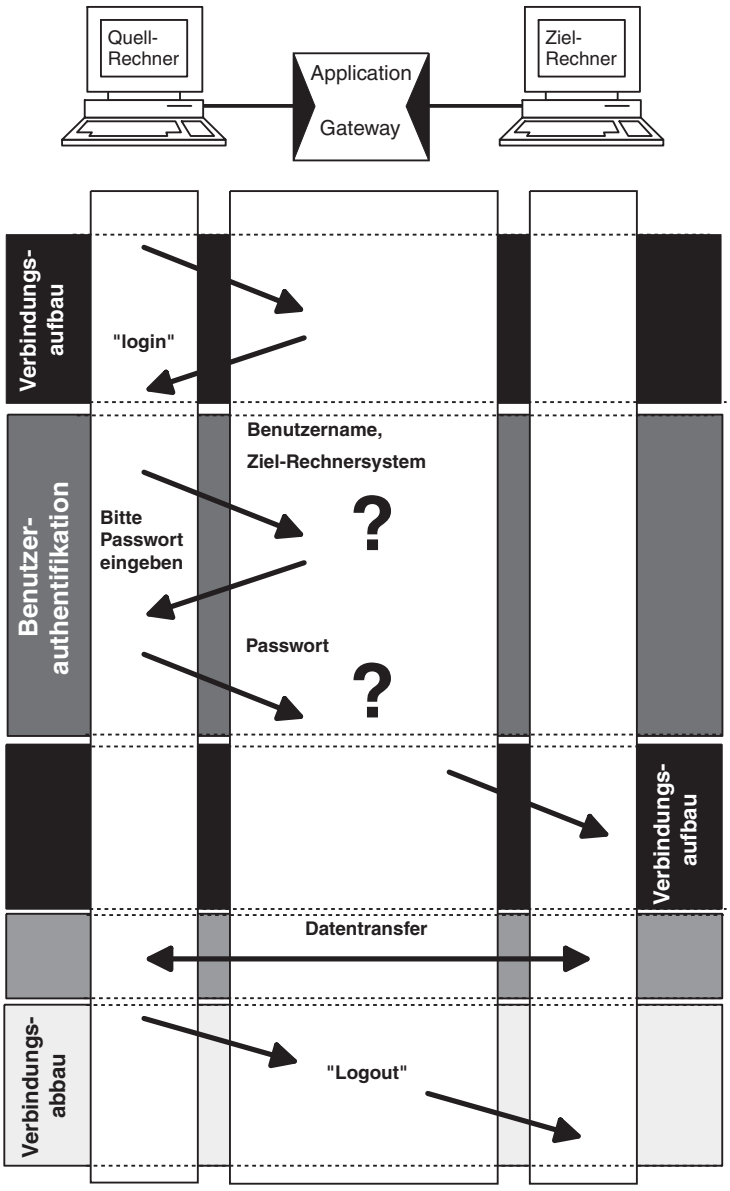


Abb. 5.22: Kommunikation über einen Application Level Proxy

1. Phase: Verbindungsaufbau zum Application Gateway

Der Benutzer versucht, über das Application Gateway eine Verbindung von seinem Quell-Rechnersystem zu einem gewünschten Ziel-Rechnersystem aufzubauen. Das Application Gateway nimmt den Verbindungsaufbau an und fordert den Zugreifenden auf, eine Identifikation und Authentikation durchzuführen.

neuKap05.fm Seite 152 Freitag, 18. Oktober 2002 3:51 15

2. Phase: Benutzerauthentikation

Der Zugreifende gibt seine Benutzer-Identifikation und sein Ziel-Rechnersystem an. Auf dem Application Gateway wird überprüft, ob der Benutzer von seinem Quell-Rechnersystem auf das angestrebte Ziel-Rechnersystem zugreifen darf und welche Restriktionen für den Zugriff bestehen. Anschließend wird der Benutzer in diesem Beispiel aufgefordert, sein Passwort einzugeben. Auf dem Application Gateway wird dann überprüft, ob der Benutzer das richtige Passwort eingegeben hat (wie beim Pförtner).

Die Authentikation bei Firewall-Systemen kann in der Regel unterschiedlich realisiert werden, z. B. Passwortverfahren, Einmal-Passwortverfahren, Challenge-Response-Verfahren. Die Authentikationsverfahren, die mithilfe von kryptographischen Algorithmen arbeiten, nutzen für den Benutzer Security Token, Chipkarte usw. Welches Authentikationsverfahren verwendet wird, hängt in der Regel von dem Schutzbedarf und der Richtung der Kommunikation über das Firewall-System ab. Von einem zu schützenden Netz in ein unsicheres Netz kann mit einem einfachen oder sogar ohne ein Authentikationsverfahren die Kommunikation über das Firewall-System realisiert werden. Bei der Kommunikation von einem unsicheren Netz in ein zu schützendes Netz sollte immer ein kryptographisches Verfahren (z. B. mit Security Token oder Chipkarte) verwendet werden (siehe auch Kapitel 8 *Authentikationsverfahren*).

3. Phase: Verbindungsaufbau zum Ziel-Rechnersystem

Wenn sich der zugreifende Benutzer identifizieren und authentisieren konnte, wird durch den Proxy auf dem Application Gateway eine zweite Verbindung vom Application Gateway zum gewünschten und erlaubten Ziel-Rechnersystem aufgebaut.

4. Phase: Datentransfer

Dann findet der Datentransfer statt. Abhängig vom jeweiligen Proxy wird der Datentransfer über den Proxy auf dem Application Gateway überwacht, kontrolliert und protokolliert. Diese Phase ist für den Benutzer transparent.

5. Phase: Verbindungsabbau

In der letzten Phase wird die Verbindung über das Application Gateway abgebaut.

5.4.2.4 Telnet Proxy

Der Telnet Proxy ist für die kontrollierte Kommunikation über Telnet verantwortlich und stellt entsprechende spezielle Sicherheitsfunktionen für diesen Dienst zur Verfügung.

neuKap05.fm Seite 153 Freitag, 18. Oktober 2002 3:51 15

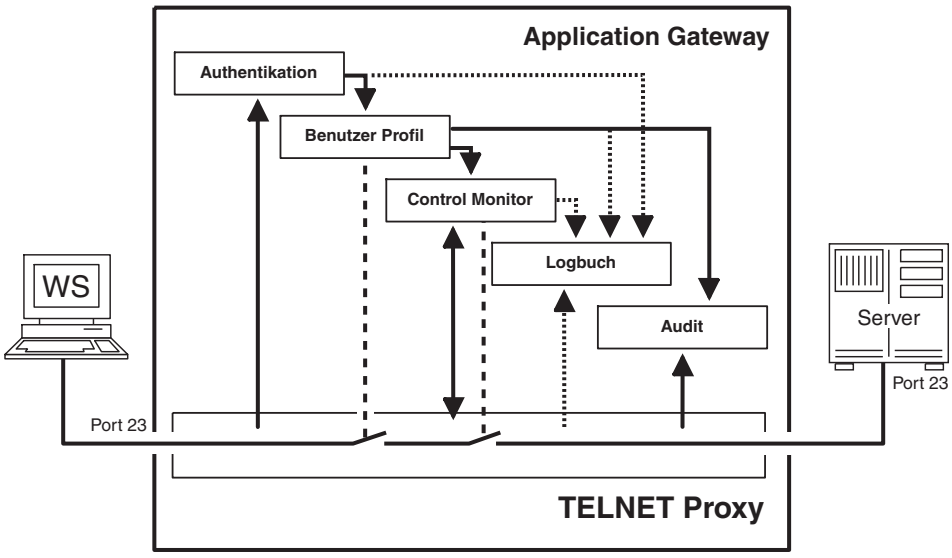


Abb. 5.23: Telnet Proxy

Der Verbindungsaufbau erfolgt vom Quell-Rechnersystem (Client) auf Port 23 (Port für den Telnet-Dienst) des Application Gateway. An Port 23 übernimmt der Telnet Proxy die Verbindung. Der Benutzer auf dem Quell-Rechnersystem identifiziert und authentisiert sich unter Angabe des Verbindungszieles gegenüber dem Telnet Proxy. Nach erfolgreicher Identifikation und Authentikation wird ein den folgenden Bedingungen entsprechendes Benutzer-Profil aktiviert:

- IP-Adresse des Quell-Rechnersystems, das die Verbindung aufbauen möchte
- Benutzername, mit dem die Identifikation und Authentikation erfolgte
- IP-Adresse des Ziel-Rechnersystems

Nun baut der Telnet Proxy eine zweite Verbindung vom Application Gateway auf Port 23 des Ziel-Rechnersystems auf. Jetzt kann der Benutzer vom Quell-Rechnersystem über den Telnet Proxy den Telnet-Dienst des Ziel-Rechnersystems nutzen (siehe Abb. 5.23).

Control Monitor

Bei der Telnet-Session ist es z. B. möglich, mithilfe eines »Control Monitors« zu überprüfen, ob der Benutzer unerlaubterweise vom Quell-Rechnersystem auf ein anderes Rechnersystem als das erlaubte Ziel-Rechnersystem zugreift (Hopping-Angriff – siehe Kapitel 4.5 *Angriffsmethoden und prinzipielle Gegenmaßnahmen auf der Grundlage der TCP/IP-Protokolle*). Dabei überprüft der Monitor den Datenstrom auf Bytefolgen, die unter Umständen für ein Hopping genutzt werden können. Es ist auch möglich, nach anderen Informationen zu suchen, wie Steuerzeichen, die nicht verwendet werden sollen (z. B. Ctrl-C).

neuKap05.fm Seite 154 Freitag, 18. Oktober 2002 3:51 15

Logbuch:

In das Logbuch des Application Gateway können durch den Telnet Proxy die folgenden Protokolleinträge vorgenommen werden:

- IP-Adresse und Rechnername des Quell-Rechnersystems
- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Name des Benutzers
- Anzahl der übertragenen Bytes
- Uhrzeit und Datum des Verbindungsabbaus

Bei der Telnet-Verbindung ist es oft sinnvoll, einen Mitschnitt der kompletten Kommunikation aufzuzeichnen (Audit). Neben der Möglichkeit, diesen Mitschnitt später auszuwerten, hat diese Sicherheitsfunktion einen nicht zu unterschätzenden Warneffekt.

Anwendungsbeispiel für Audit:

Der Sicherheitsmechanismus Audit kann z. B. bei Remote-Service mit einer Firma im Servicevertrag vereinbart werden. Dadurch ist dem Mitarbeiter der Firma, die den Service durchführt, bewusst, dass alles, was er tut, protokolliert wird. Allein das Wissen um diesen Mitschnitt wird den Serviceleistenden motivieren, nur das zu tun, was er für seine Aufgabenstellung wirklich benötigt. Im Falle eines Schadens kann dann der Mitschnitt aufklären, ob über den Remote-Zugriff unerlaubte oder nicht notwendige Aktionen durchgeführt worden sind. Der Mitarbeiter der Service-Firma kann für seine Handlungen im Nachhinein verantwortlich gemacht werden.

Beispiele für den Einsatz eines Application Gateway mit Telnet Proxy

Im Folgenden soll anhand eines Beispieles dargestellt werden, wie mithilfe eines Application Gateway mit einem Telnet Proxy Sicherheit zwischen zwei Netzen, die einen unterschiedlichen Schutzbedarf haben, realisiert werden kann.

In der Abbildung 5.24 sind zwei Netze zu sehen (Netz X mit den IP-Adressen 192.168.3.X und Netz Y mit den IP-Adressen 192.168.5.Y), die unabhängig voneinander sind und zwischen denen keine Verbindung besteht. Der Administrator des Server 1 im Netz X arbeitet an der Workstation A in Netz Y und will einen Remote-Zugang auf den Server 1 des Netzes X erreichen. Aus diesem Grund soll von Workstation A aus eine Verbindung zum Server 1 im Netz X aufgebaut werden. Die beiden Netze sollen mithilfe eines Application Gateway mit Telnet Proxy gekoppelt werden, wobei nur eine Telnet-Session von Workstation A im Netz Y zum Server 1 im Netz X erlaubt sein soll.

neuKap05.fm Seite 155 Freitag, 18. Oktober 2002 3:51 15

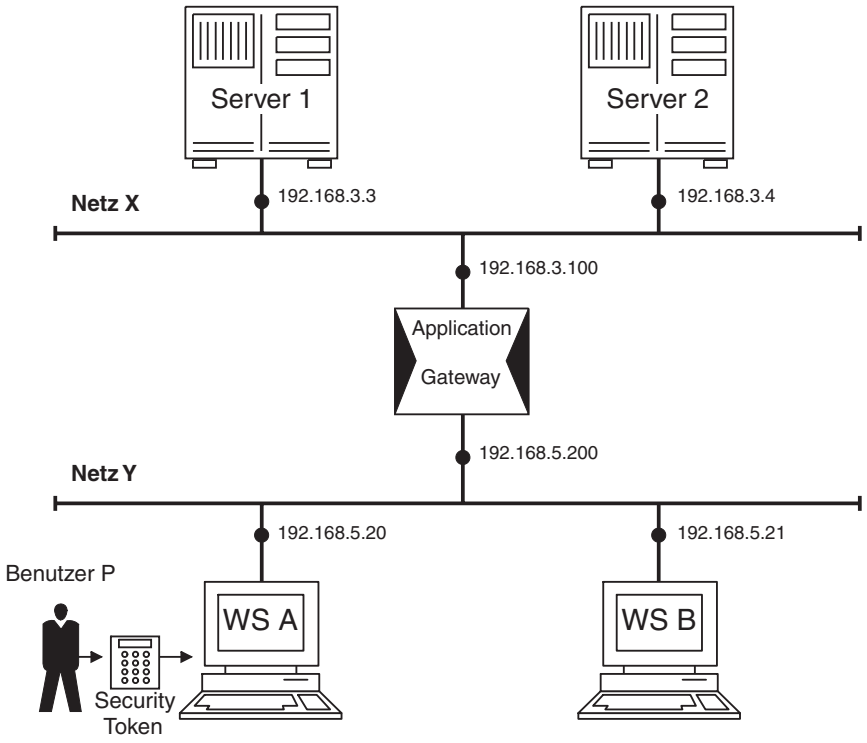


Abb. 5.24: Einsatz eines Application Gateway mit Telnet Proxy

Eigenschaften des Kommunikationsdienstes Telnet:

- Telnet basiert auf TCP
- die von Telnet Servern verwendete Standard-Portnummer ist 23 (TCP-Zielportnummer)
- die von Telnet-Clients verwendete TCP-Quell-Portnummer ist eine beliebige Portnummer, die größer ist als 1023

Festlegung der Filterregeln für Benutzer P

- P darf auf Server 1 an Werktagen von 7 bis 18 Uhr den Telnet-Dienst nutzen
- P darf diese Verbindung unter folgenden Voraussetzungen aufbauen:
  - Workstation A muss die IP-Adresse 192.168.5.20 nutzen
  - der Server 1 muss die IP-Adresse 192.168.3.3 nutzen
  - das verwendete Transportprotokoll ist TCP
  - der Telnet-Port auf dem Server 1 muss 23 sein
  - der Quell-Port auf Workstation A muss > 1023 liegen
- P muss sich mithilfe eines Security Token authentisieren
- die Verbindung soll vollständig protokolliert werden
- die Aktionen der Verbindung sollen überwacht werden (Monitor)

neuKap05.fm Seite 156 Freitag, 18. Oktober 2002 3:51 15

- Benutzer P darf den Dienst Telnet nicht zu allen Zeiten nutzen und auch keine anderen Dienste in Anspruch nehmen sowie auf andere Rechnersysteme des Netzes X, z. B. Server 2, nicht zugreifen

andere Benutzer dürfen nicht

- auf Server 1 und Server 2 zugreifen
- erfahren, welche Rechnersysteme im jeweils anderen Netz vorhanden sind

Tabelle 5.3 zeigt die dazu notwendigen Filterregeln für den Telnet Proxy:

Benutzer	Quelladresse	Zieladresse	Authentikations-verfahren	Audit	Monitor	Wochen-tage	Zeitfenster
P	192.168.5.20	192.168.3.3	Security Token	ja	ja	Mo.–Fr.	7.00 Uhr –18.00 Uhr

Tabelle 5.3: Filterregeln

Mit diesen Filterregeln wird genau festgelegt, von welcher Quell-Adresse die Workstation A auf welche Ziel-Adresse des Servers 1 zugreifen darf. Zusätzlich wird der Zeitrahmen abgesteckt, innerhalb dessen ein Zugriff erfolgen darf. Außerdem werden das Authentikationsverfahren, die vollständige Protokollierung (Audit) sowie das Überwachen der Aktionen (Monitor) festgelegt.

Ergebnis:

Mithilfe eines Application Gateway kann genau festgelegt werden, dass die Workstation A zu Server 1 zu bestimmten Zeiten eine Telnet-Session durchführen kann; alle anderen Kommunikationsverbindungen sind über das Application Gateway nicht möglich.

Im Telnet Proxy wird erkannt, ob auf dem Server 1 am Port 23 ein anderer Dienst aktiviert wurde, sodass dieser über das Application Gateway mit dem Telnet Proxy nicht durchgeführt werden kann. Die IP-Adressen der Netze X und Y bleiben verborgen.

Außerdem kann der Benutzer P eine Kommunikation per Telnet über das Application Gateway nur nach einer erfolgreichen Authentikation durchführen. Da auf dem Application Gateway die Aktionen protokolliert werden, können die Handlungen des Benutzers P mithilfe der Logbücher verfolgt werden. Die Verfahrensweise ist für den Benutzer P eine andere als bei der Kommunikation ohne Application Gateway, weil er eine Authentikation mit dem Proxy durchführen muss, bevor er Zugriff auf Server 1 bekommt. Nach der Authentikationsphase arbeitet der Telnet Proxy transparent.

neuKap05.fm Seite 157 Freitag, 18. Oktober 2002 3:51 15

5.4.2.5 FTP Proxy

Der FTP Proxy ist für die kontrollierte Kommunikation über FTP verantwortlich und stellt entsprechende spezielle Sicherheitsfunktionen für diesen Dienst zur Verfügung.

Der Verbindungsaufbau für den Kommandokanal erfolgt vom Quell-Rechnersystem (Client) auf Port 21 (FTP-Kommando-Port) des Application Gateway. Der Benutzer auf dem Quell-Rechnersystem identifiziert und authentisiert sich, unter Angabe des Verbindungszieles, nun gegenüber dem FTP-Dienst. Nach erfolgreicher Identifikation und Authentikation wird ein den folgenden Bedingungen entsprechendes Benutzerprofil aktiviert:

- IP-Adresse des Quell-Rechnersystems, das die Verbindung aufbauen möchte
- Benutzername, mit dem die Authentikation erfolgte
- IP-Adresse des Ziel-Rechnersystems

Nun baut der FTP Proxy einen zweiten Kommandokanal vom Application Gateway auf Port 21 des Ziel-Rechnersystems auf (siehe Abb. 5.25).

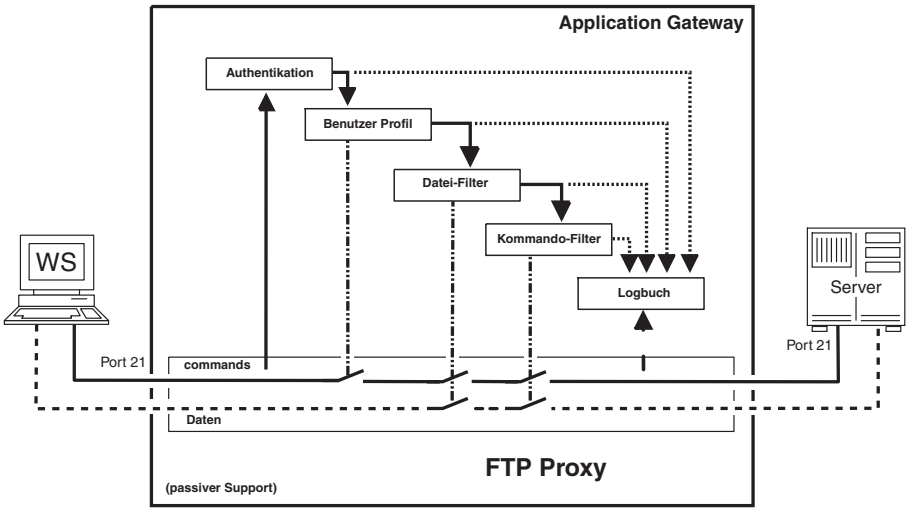


Abb. 5.25: FTP Proxy

Kommando-Filter

Der Kommando-Filter analysiert und überprüft alle vom Benutzer eingegebenen FTP-Kommandos hinsichtlich ihres Eintrags in der Rechtedatei (Benutzerprofil). Für den FTP Proxy kann z. B. definiert werden, welche Befehle (cd, put, get, del usw.) verwendet werden dürfen und welche nicht.

neuKap05.fm Seite 158 Freitag, 18. Oktober 2002 3:51 15

Gibt der Benutzer ein Kommando ein, zu dem er berechtigt und bei dem ein Datentransfer erforderlich ist, erfolgt der Verbindungsaufbau des Datenkanals abhängig davon, ob auf dem Quell-Rechnersystem (Client-Seite) eine aktive oder eine passive FTP-Verbindung gewünscht wurde.

Wird ein Kommando von einem nicht dazu berechtigten Benutzer verwendet, wird dieses dem Benutzer angezeigt, und der unberechtigte Versuch wird in das Logbuch des Application Gateway eingetragen und, falls definiert, als Spontane Meldung an das Security Management gesendet.

Datei-Filter

Außerdem kann bei FTP Proxies durch einen Datei-Filter in der Regel eine Namensrestriktion für die Dateien vorgenommen werden, die übertragen werden dürfen.

- Zum Beispiel dürfen nur Dateien mit dem Namen »Input.neu« und »Output.neu« transferiert werden.
- Es dürfen keine Dateien mit der Endung »*.exe« übertragen werden.

Logbuch

In das Logbuch des Application Gateway können durch den FTP Proxy die folgenden Protokolleinträge standardmäßig vorgenommen werden:

- IP-Adresse und Rechnername des Quell-Rechnersystems
- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Name des Benutzers
- Anzahl der übertragenen Bytes
- Name der übertragenen Dateien
- verwendete Befehle
- Uhrzeit und Datum des Verbindungsabbaus

Anwendungsbeispiel für den FTP Proxy

Mithilfe des FTP Proxy kann genau festgelegt werden, welche Befehle verwendet werden dürfen. Falls z. B. ein Software-Haus auf einem bestimmten Server ein Update senden möchte, wird einem Mitarbeiter des Software-Hauses erlaubt, die Befehle »cd« und »put« zu verwenden. Diese Befehle reichen aus, um die Arbeit durchführen zu können.

Die Reduzierung der erlaubten Befehle verhindert, dass bei dieser Aktion versehentlich oder absichtlich Schaden angerichtet wird. Falls z. B. versucht wird den Befehl »del« (Löschen) auszuführen, wird dies im FTP Proxy des Application Gateway erkannt und dem Benutzer angezeigt. Das Ereignis wird in das Logbuch eingetragen und, falls im Regelwerk definiert, eine Spontane Meldung mit den entsprechenden Protokolldaten an das Security Management gesendet.

neuKap05.fm Seite 159 Freitag, 18. Oktober 2002 3:51 15

5.4.2.6 HTTP Proxy

Der HTTP Proxy ist für die kontrollierte Kommunikation über HTTP verantwortlich und stellt entsprechende spezielle Sicherheitsfunktionen für diesen Dienst zur Verfügung.

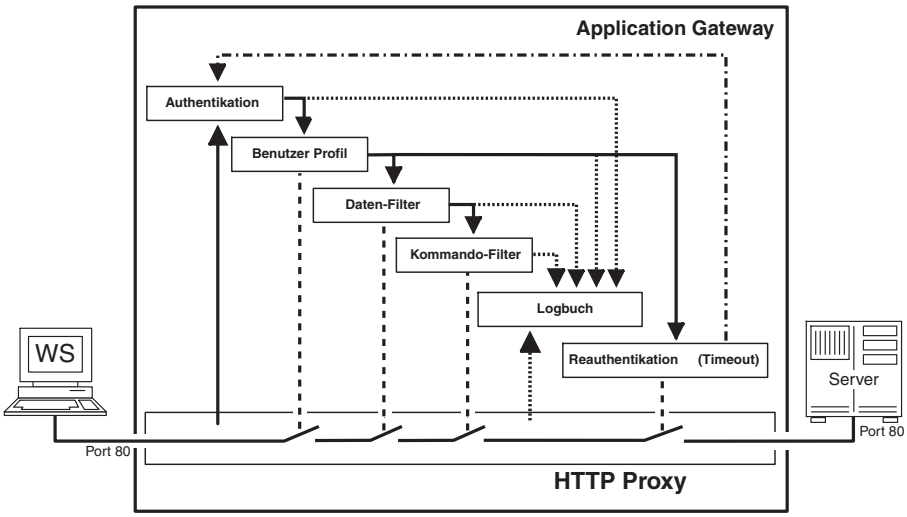


Abb. 5.26: HTTP Proxy

Der Verbindungsaufbau erfolgt vom Quell-Rechnersystem (Client) auf Port 80 (Port für den HTTP-Dienst) des Application Gateway. Der Benutzer auf dem Quell-Rechnersystem (Client-Seite) identifiziert und authentisiert sich, unter Angabe des Verbindungszieles, nun gegenüber dem HTTP-Dienst. Nach erfolgreicher Identifikation und Authentikation wird ein den folgenden Bedingungen entsprechendes Benutzer-Profil aktiviert:

- IP-Adresse des Quell-Rechnersystems, das die Verbindung aufbauen möchte
- Benutzername, mit dem die Authentikation erfolgte
- IP-Adresse des Ziel-Rechnersystems

Nun baut der HTTP Proxy vom Application Gateway eine zweite Verbindung auf Port 80 des Ziel-Rechnersystems auf. Jetzt kann der Benutzer vom Quell-Rechnersystem über das Application Gateway (HTTP Proxy) den HTTP-Dienst des Ziel-Rechnersystems nutzen (siehe Abb. 5.26).

Reauthentikation

Das HTTP-Protokoll arbeitet nicht Session-orientiert, d.h., der HTTP Proxy ist nicht in der Lage, von sich aus das Ende einer Session zu erkennen. Jedes Mal, wenn eine WWW-Seite angefordert wird, wird eine Verbindung über das Firewall-

neuKap05.fm Seite 160 Freitag, 18. Oktober 2002 3:51 15

System aufgebaut, die WWW-Seite übertragen und wieder abgebaut. Beim ersten Mal wird vor der Übertragung die Authentikation durchgeführt. Aus diesem Grund wird ein Timer gesetzt, der den Beginn der Session festhält. Nach Ablauf des Timers wird der HTTP Proxy automatisch abgeschaltet. Sobald eine Benutzeraktivität in dieser Session stattfindet, wird der Timer erneut gesetzt. War der Timer abgeschaltet, muss bei einer erneuten Kommunikation wieder eine Identifikation und Authentikation stattfinden (falls eingestellt).

Kommando-Filter

Der Kommando-Filter analysiert und überprüft die verwendeten Methoden (FTP, HTTP, NNTP, SMTP) und die verwendeten Befehle (z. B. put, get, post).

Jeder Versuch, eine nicht-gültige Methode oder einen nicht-erlaubten Befehl zu verwenden, wird dem Benutzer angezeigt, und es erfolgt ein entsprechender Eintrag in das Logbuch des Application Gateway. Falls im Regelwerk definiert, wird in diesem Fall auch eine Spontane Meldung mit den Protokolldaten an das Security Management gesendet.

Daten-Filter

Mithilfe eines Daten-Filters im HTTP Proxy ist es auch möglich, nur definierte URLs zuzulassen (URL-Blocker). Zum Beispiel kann festgelegt werden, dass die Benutzer nur HTTP-Server mit der Domäne »*.de« nutzen dürfen. Durch den Daten-Filter können aber auch bekannte, nicht gewünschte Dateien oder HTTP-Seiten durch den Proxy ausgefiltert werden. Dies kann z. B. bei bekannten Dateien, in denen Viren sind, oder HTTP-Seiten, auf denen pornographische Bilder zu sehen sind, genutzt werden.

Content Security

Unter den Begriff Content Security werden hier die Sicherheitsmechanismen verstanden, die gegen die Gefährdungen durch aktive Inhalte innerhalb von HTML-Seiten wirken.

a) Applet-Filter

Mithilfe eines Applet-Filters kann die Nutzung von Java, Java Scripts und ActiveX verhindert und kontrolliert werden. Dies ermöglicht die Sicherheitspolitik einer Organisation, bezogen auf die Nutzung von dynamischen Programmteilen durchzusetzen. Ein mögliches Beispiel ist, Java im zu schützenden Netz für die Intranet-Anwendungen zuzulassen, aber die Kommunikation mit Rechnersystemen im unsicheren Netz über das Firewall-System zu verhindern.

neuKap05.fm Seite 161 Freitag, 18. Oktober 2002 3:51 15

b) Malware-Filter

Mithilfe eines Malware-Filters können Viren, Würmer und Trojanische Pferde aufgespürt und der mögliche Schaden verhindert werden (siehe Kap. 10.8).

Logbuch:

Durch den HTTP Proxy können z. B. die folgenden Protokolleinträge in das Logbuch des Application Gateway vorgenommen werden:

- IP-Adresse und Rechnername des Quell-Rechnersystems
- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Name des Benutzers
- Anzahl der übertragenen Bytes
- Name der übertragenen Datei oder der übertragenen HTML-Seite (Name der Seite und IP-Adresse des Servers/Ziel-Rechnersystems)
- Uhrzeit und Datum des Verbindungsabbaus

5.4.2.7 Java Proxy

Der Java Proxy ist für die vertrauenswürdige Anwendung von Java Applets verantwortlich, siehe auch /BSI98/.

Grundlagen

- Die im Unternehmen genutzte Java-Laufzeitumgebung für die Ausführung von Java Applets ist einheitlich.
- Die Technologie der genutzten Java-Laufzeitumgebung ist evaluiert worden und hat somit eine sehr hohe Vertrauenswürdigkeit.
- Mithilfe von Check-Mechanismen (spezielle Java Applets, die vom Java Proxy gesendet werden) ist überprüfbar, ob eine Veränderungen der genutzten Java-Laufzeitumgebung stattgefunden haben oder nicht.

Wenn ein Benutzer von seinem Rechner in einem zu schützenden Netz auf einen WWW-Server zugreift und ein Applet heruntergeladen wird, wird dieses im Java-Relais erkannt. Das Java Relais überprüft mithilfe des Java-Policy-Managers, welche Policy für welchen Benutzer gegeben worden ist. Gegebenenfalls wird vorher ein Java Applet mit Check-Mechanismen heruntergeschickt, um die Java-Laufzeitumgebung auf ihre Vertrauenswürdigkeit zu überprüfen. Erst wenn die Antwort kommt, dass die Java-Laufzeitumgebung noch vertrauenswürdig und nicht manipuliert worden ist, wird das eigentliche Java-Applet vom Proxy heruntergeladen und in der vertrauenswürdigen Java-Laufzeitumgebung sicher ausgeführt.

neuKap05.fm Seite 162 Freitag, 18. Oktober 2002 3:51 15

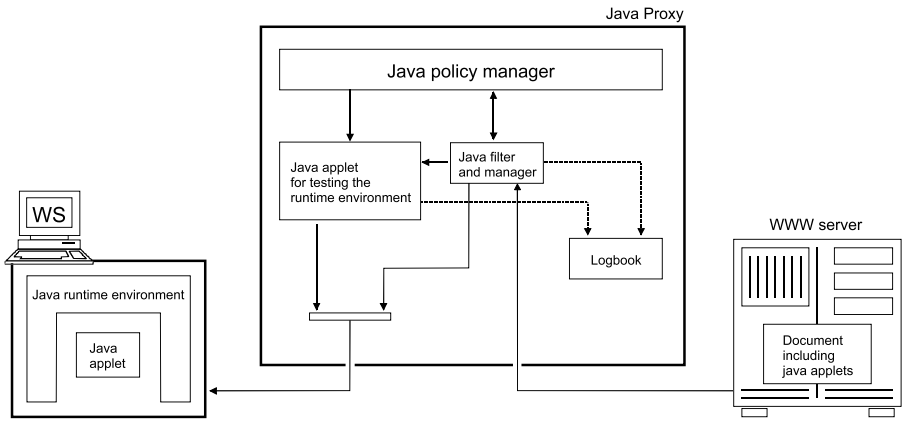


Abb. 5.27: Java Proxy

Java Proxy Manager

Der Java Proxy Manager ist für die Sicherheitspolitik der Java Anwendungen im ganzen Unternehmen zuständig. Hier wird entsprechend definiert, welche Permissions der einzelne Benutzer durchführen darf. Es wird festgelegt, welche Systemzugriffe über Klassen für den einzelnen Benutzer in der entsprechenden Java-Zeitlaufüberziehung-Klassenbibliothek überhaupt realisiert werden dürfen.

Logbuch

Durch den Java Proxy können z. B. die folgenden Protokolleinträge in das Logbuch des Application Gateway vorgenommen werden:

- IP-Adresse und Rechnername des Quell-Rechnersystems
- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Name des Benutzers
- Uhrzeit und Datum des Verbindungsabbaus

5.4.2.8 E-Commerce Proxy

Für einen Application Gateway besteht nicht nur die Möglichkeit, Proxies für Protokolle wie HTTP oder Telnet einzusetzen. Vermehrt werden solche Protokolle in Tunnel-Protokolle eingebettet. Dies geschieht zumeist, um diese Protokolle im Nachhinein mit Sicherheitsfunktionalität auszustatten, oder sie proxyfähig zu machen.

Beispiele für solche Tunnelprotokolle sind SSL und SOCKS. Der bekannteste Anwendungsfall ist HTTPS (HTTP in einem SSL-Tunnel). Solche Tunnel können als Funktionalität in einen bestehenden Tunnel integriert werden oder sie können als Wrapper realisiert werden. Ein Wrapper nimmt das getunnelte Protokoll an,

neuKap05.fm Seite 163 Freitag, 18. Oktober 2002 3:51 15

packt das Protokoll aus und leitet die Daten an den eigentlichen Protokoll-Proxy weiter. Dieses Konzept hat den Vorteil, dass mit geringem Aufwand viele Tunnel mit vielen Protokollen kombiniert werden können.

TLS-Wrapper (SSL-Gateway)

TLS (früher bekannt unter dem Namen SSL) ist ein Tunnelprotokoll, das für verschiedene Protokolle angewendet werden kann. Die häufigste Anwendung ist HTTP. Hierbei gibt es zwei Konzepte:

1) Wenn ein Firewall-System auf Clientseite steht, d.h., ein Browser soll mit HTTPS über ein Firewall-System auf viele verschiedene Server im Internet zugreifen, ist dies nur möglich, indem das Firewall-System die SSL Verbindung verschlüsselt tunnelt. Dies sichert eine End-to-End-Verschlüsselung zwischen dem Client und dem Server. Dieser Betriebsmodus kann durch den normalen HTTP Proxy realisiert werden. Aufgabe des Firewall-Systems ist es, den Client zu schützen. Das Tunneln einer verschlüsselten Verbindung ist aus Sicht des Firewall-Systems nicht ideal, da hier der Client nur begrenzt geschützt werden kann. Wenn der Client eine End-to-End verschlüsselte Verbindung bis zum Server verlangt, kann das Firewall-System dies entweder akzeptieren oder ganz ablehnen.
2) Wenn das Firewall-System auf Server-Seite steht, soll es den Server schützen. Hier kann das Firewall-System die gesamte Sicherheitsfunktionalität der Website übernehmen. Dies sind:
   - Eine sichere und protokollierte Authentikation des Clients gegenüber dem Server mittels Client-Zertifikat: Diese Funktion ist optional. Eine Bank möchte vielleicht nur bestehenden Kunden den Zugang zum Online-Banking Server erlauben. Ein Internet-Shop will allerdings auch beliebigen Neukunden den Zugang zu seinem Angebot erlauben. Dann kann die Client-Authentikation unterbleiben.
   - Eine sichere und protokollierte Authentikation des Servers gegenüber dem Client mittels eines Server-Zertifikats.
   - Eine sichere Speicherung des Server-Zertifikats: Wenn diese durch einen Hacker gestohlen wird, kann dieser im Internet die Identität der Website annehmen und großen Schaden anrichten, da die Clients darauf vertrauen, dass das Server-Zertifikat den Server sicher authentisiert. Die sichere Speicherung kann entweder auf einem separaten System hinter dem SSL Gateway geschehen. Dies wäre ein separater Authentikations-Server. Oder sie kann in einem geeigneten Hardware-Modul geschehen. Das Zertifikat kann diese ähnlich wie bei einer Chipkarte niemals verlassen.
   - Die performante Abwicklung der Verschlüsselungsoperationen und zwar Authentikation (asymmetrische Verschlüsselung) und Datenverschlüsselung (symmetrische Verschlüsselung): Dies ist vorteilhaft, da viele Websites an ihrer Leistungsgrenze operieren, und deshalb eine Realisierung von SSL auf dem Web-Server selbst nicht möglich ist oder oft an Grenzen stößt.

neuKap05.fm Seite 164 Freitag, 18. Oktober 2002 3:51 15

- Die unabhängige Protokollierung von Angriffen: Dies ist sinnvoll, da Websites ein beliebtes Angriffsziel im Internet sind. Das Firewall-System bietet hingegen einen einheitlichen und vom Administrator ständig überwachten Protokollierungs- und Alarmierungsmechanismus. Hierbei kann das Firewall-System sinnvoll durch ein Intrusion-Detection-System ergänzt werden. Das Firewall-System kann aber auch Informationen über den Authentikationsvorgang protokollieren, die dem Intrusion-Detection-System als Außenstehendem nicht zugänglich sind.

Reine SSL-Tunnel durch ein Firewall-System hindurch sind unter Sicherheitsgesichtspunkten ein Nachteil, da die Sicherheit beim Server liegt und dieser im Normalfall keine ausreichende Sicherheit gewährleisten kann.

Realisierung eines E-Commerce Proxy

Die Realisierung eines E-Commerce Proxy geschieht auf folgendem Weg: Der Client baut eine SSL-verschlüssselte Verbindung zum Application Gateway auf, das er für den Server hält. Dieser erledigt die gegenseitige Authentikation und die Verschlüsselung auf sichere Art und Weise. Nachdem die Daten entschlüsselt worden sind, kann das Application Gateway die Daten auf Protokollebene (z.B. HTTP) und auf Inhaltsebene (z.B. Viren und JavaScript) filtern. Dies kann durch den normalen Proxy geschehen. Danach leitet das Application Gateway die Daten im Klartext an den Web-Server weiter, der für die Inhalte der Webseite selbst verantwortlich ist. Diese Verbindung geschieht im internen Netz des Websitebetreibers. Wenn dieses nicht ausreichend sicher ist, kann die Strecke durch Leitungsverschlüsselung (mittels VPN-Gateways) gesichert werden.

Ein E-Commerce Proxy in einem Application Gateway garantiert eine klare Trennung von Sicherheitsfunktionalität und Webinhalt. Web-Server und der E-Commerce Proxy konzentrieren sich auf ihre jeweiligen Kernkompetenzen.

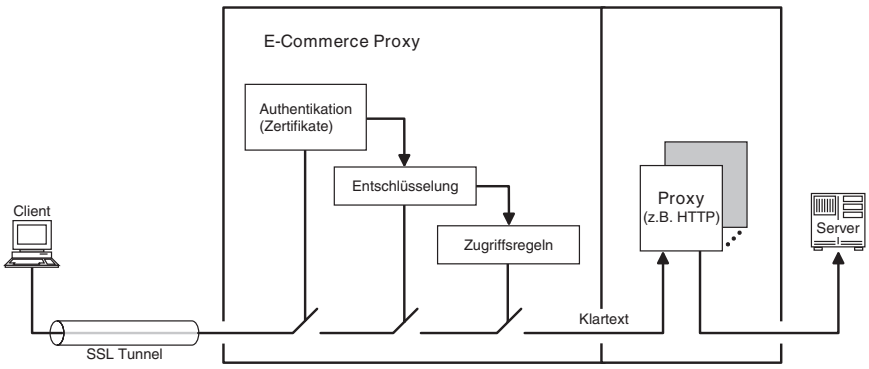


Abb. 5.28: E-Commerce Proxy

neuKap05.fm Seite 165 Freitag, 18. Oktober 2002 3:51 15

5.4.2.9 Authentication Proxy (Global Authentication)

Ein etwas anderes Konzept für ein Application Gateway ist, dass der Benutzer eine Identifikation und Authentikation mit einem so genannten Authentication Proxy durchführt. Diese Art der Authentication wird auch Global Authentication genannt. Dieser Authentication Proxy führt die Rechtverwaltung für die unterschiedlichen Dienste durch, z. B. für FTP, Telnet, HTTP. In diesem Fall muss keine erneute Authentikation durchgeführt werden, wenn der Benutzer einen Dienst wechseln möchte.

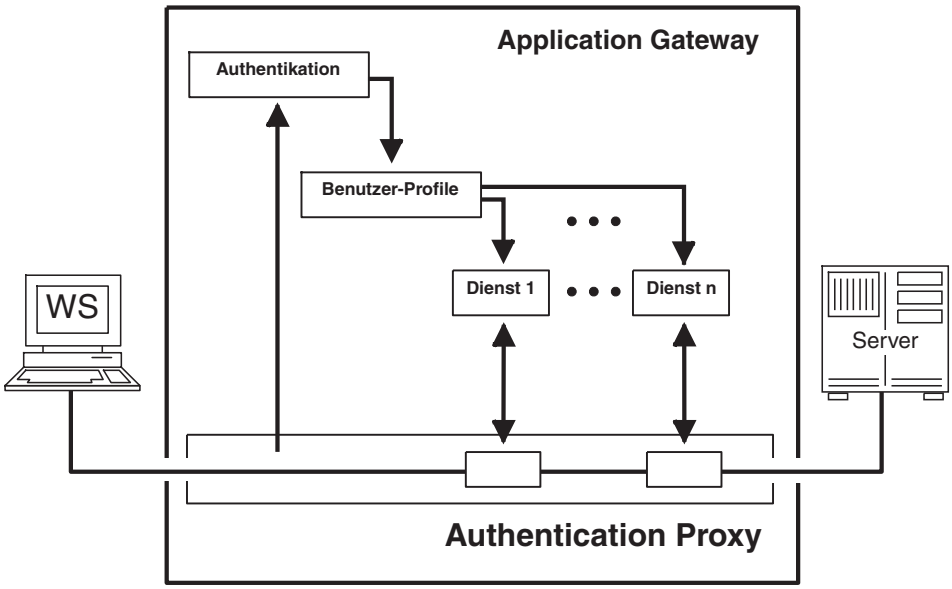


Abb. 5.29: Authentication Proxy

Ein Nachteil dieser Methode, der sich besonders bei Multiuser-Systemen zeigt, ist die nicht eindeutige Verbindung zwischen Dienst und Benutzer. Außerdem kann während der Zeit der Freischaltung der Verbindung auf dem Application Gateway und dem Connect des Clients der Dienst von Angreifern benutzt werden.

Der Authentication Proxy regelt die Identifikation und Authentikation eines Clients auf einem Server über das Application Gateway. Anschließend können die erlaubten Dienste über das Firewall-System kontrolliert genutzt werden.

neuKap05.fm Seite 166 Freitag, 18. Oktober 2002 3:51 15

5.4.2.10 Transparent Proxy

Unter den Namen »Transparent Proxy« werden Proxies verstanden, die in der Lage sind, aus der Sicht der Clients sich transparent zu verhalten. Diese Proxies sorgen z.B. dafür, dass aus dem zu schützenden Netz direkt Rechnersysteme im unsicheren Netz (z.B. Internet) adressiert werden können. Der Vorteil dieser Proxies, die sich transparent von innen nach außen verhalten, ist der, dass die Client-Software bei der Integration eines Firewall-Systems nicht verändert werden braucht. Bei bestimmten Anwendungen, wie z.B. Home-Banking Lösungen, die über Java-Applets feste IP-Adressen mitsenden, können diese Anwendungen dann auch über Firewall-Systeme realisiert werden.

5.4.2.11 Spezielle Proxies

Außerdem gibt es weitere spezielle Proxies, die für bestimmte Applikationen wiederum zusätzliche, auf diese Dienste zugeschnittene Sicherheitsdienste zur Verfügung stellen. Es können auch für nicht-standardisierte Dienste Proxies realisiert werden.

5.4.2.12 Circuit Level Proxies

Da bei Application Gateways ein Routing auf der Netzwerkebene aus Sicherheitsgründen nicht möglich sein darf, könnten für Dienste, für die kein Application Level Proxy zur Verfügung steht, so genannte Circuit Level Proxies zur Verfügung gestellt werden, wenn eine Kommunikation über das Application Gateway realisiert werden soll. Circuit Level Proxies sind eine Art generische Proxies, die für eine Mehrzahl von Diensten mit verschiedenen Protokollen verwendet werden können.

Diese Circuit Level Proxies, die auch als generische Proxies, Port-Relays oder Plug-Gateways bezeichnet werden, können in der Regel für TCP und UDP-Anwendungen verwendet werden.

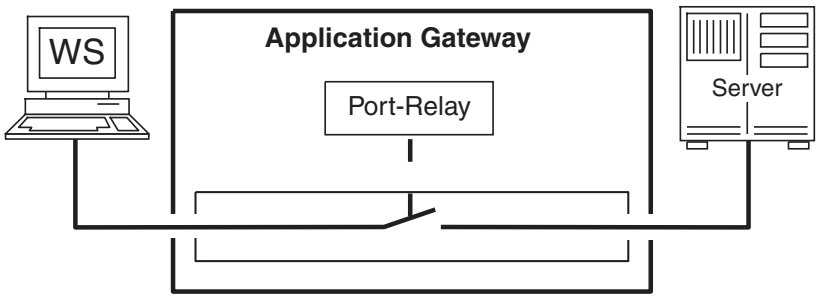


Abb. 5.30: Port-Relay

neuKap05.fm Seite 167 Freitag, 18. Oktober 2002 3:51 15

Mit einem Port-Relays kann eine Kommunikation über das Application Gateway über einen definierten Port auf *eine* definierte IP-Adresse kontrolliert erfolgen. Da die Kommunikation über die Port-Nummer des Port-Relays adressiert wird, kann die Kommunikation über das Application Gateway nur auf eine IP-Adresse aus der anderen Seite erfolgen. Aus diesem Grund sind Port-Relays immer n:1. Viele Rechnersysteme (IP-Adressen) von der einen Seite können auf ein Rechnersystem (eine IP-Adresse) auf die andere Seite. Der umgekehrte Weg ist nicht möglich.

Im Folgenden werden zwei Anwendungsbeispiele dargestellt, die aufzeigen, welche Möglichkeiten mit den Circuit Level Proxies – Port Relays – realisiert werden können.

Beispiel eines n:1 Port-Relay

In diesem Beispiel wird ein Mail Server vor dem Application Gateway im unsicheren Netz positioniert. Auf dem Mail Server ist dann z. B. ein POP3-Server installiert, mit dessen Hilfe Mails in das zu schützende Netz übertragen werden können. Auf dem Application Gateway wird dann ein Port-Relay definiert, auf den mehrere Clients (IP-Adressen) über eine bestimmte Portnummer (hier 110) auf die IP-Adresse des Mail Servers zugreifen dürfen.

Anschließend können die Clients (Quell-Rechnersysteme) über den definierten Port auf den Mail Server (Ziel-Rechnersystem) zugreifen, um ihre Mail zu holen. Das Port-Relay überprüft, ob von den zugelassenen IP-Adressen über den erlaubten Port auf die IP-Adresse des Mail Servers zugegriffen wird. Der umgekehrte Weg ist nicht möglich.

Quell-IP-Adressen (n) *zu schützendes Netz*	Ziel-IP-Adresse des Application Gateway *zu schützendes Netz*	Portnummer	Quell-IP-Adresse des Application Gateways *unsicheres Netz*	Ziel-IP-Adresse (1) *unsicheres Netz*
192.168.1.1, 192.168.1.2, 192.168.1.3, 192.168.1.4	192.168.1.60	110	194.173.3.10	194.173.3.1

Tabelle 5.4: Beispiel einer Tabelle für einen n:1 Port-Relay

Die n:1 Port-Relays sind sehr starr und können nicht für jede mögliche Anwendung verwendet werden. Es gibt aber die Möglichkeit, aus vielen n:1 Port-Relays einen n:m Port-Relay zu gestalten.

neuKap05.fm Seite 168 Freitag, 18. Oktober 2002 3:51 15

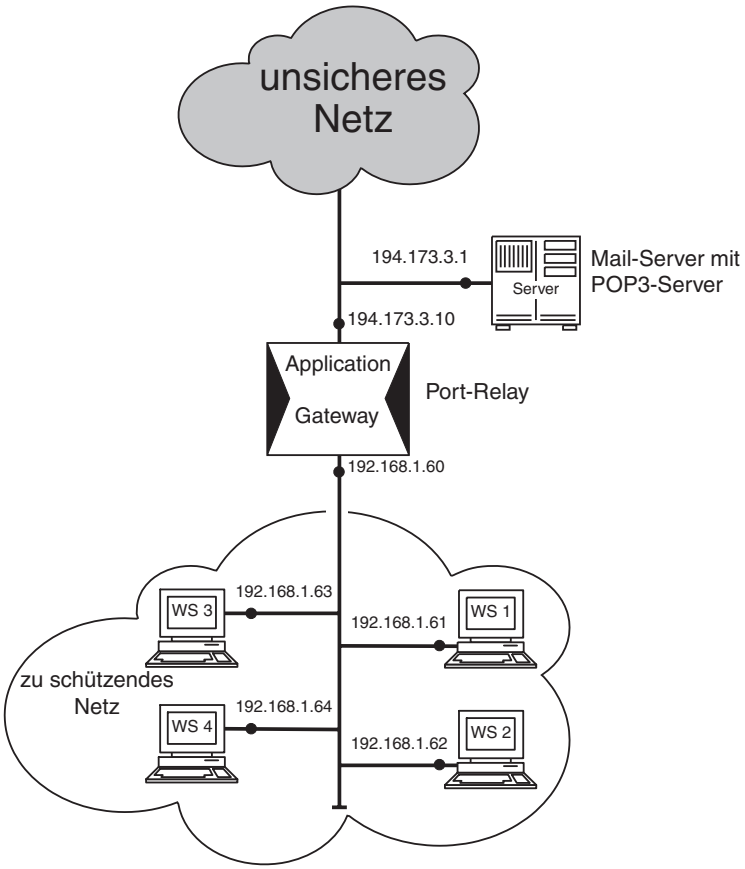


Abb. 5.31: Beispiel eines n:1 Port-Relay

Beispiel eines n:m Port-Relay

In diesem Beispiel wird beschrieben, wie die Möglichkeit geschaffen werden kann, aus dem unsicheren Netz über unterschiedliche IP-Adressen des unsicheren Netzes (z. B. Internet) auf unterschiedliche Rechnersysteme im zu schützenden Netz (z. B. Intranet) zuzugreifen. Das Application Gateway kann dann über mehrere IP-Adressen aus dem unsicheren Netz angesprochen werden. Dabei sollen die IP-Adressen der Rechnersysteme des zu schützenden Netzes verborgen bleiben.

Dazu wird m-mal ein n:1 Port-Relay für die unterschiedlichen IP-Adressen definiert, die aus dem unsicheren Netz auf das zu schützende Netz zugreifen können, und es wird festgelegt, auf welche Rechnersysteme sie im zu schützenden Netz zugreifen dürfen.

neuKap05.fm Seite 169 Freitag, 18. Oktober 2002 3:51 15

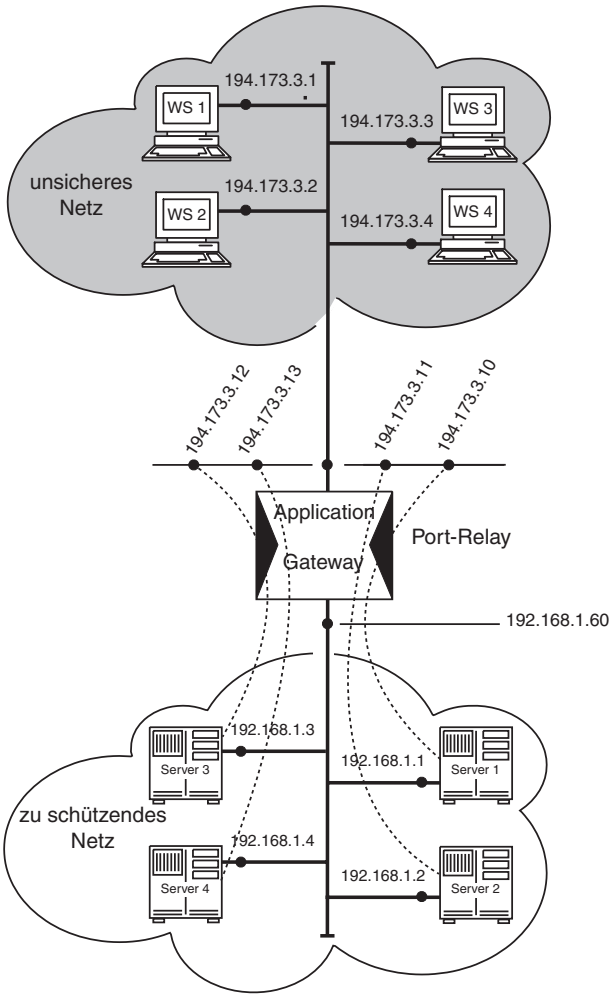


Abb. 5.32: Beispiel eines n:m Port-Relay

Aus der Sicht der Rechnersysteme im unsicheren Netz werden die IP-Adressen der Server im zu schützenden Netz wie IP-Adressen des unsicheren Netzes betrachtet.

Dabei wird auch genau definiert, über welchen Port dies ermöglicht wird (siehe Tabelle 5.5 *Port 2000*). Durch den n:m Port-Relay wird erreicht, dass die IP-Adressen des zu schützenden Netzes verborgen bleiben, weil sich nur die externen IP-Adressen darstellen, und dass die Kommunikation über den Port nur mit definierten Rechnersystemen in einer Richtung ermöglicht wird.

neuKap05.fm Seite 170 Freitag, 18. Oktober 2002 3:51 15

Quell-IP-Adressen *unsicheres Netz*	Ziel-IP-Adresse des Application Gateway *unsicheres Netz*	Portnummer	Quell-IP-Adresse des Application Gateways *zu schützendes Netz*	Ziel-IP-Adresse *zu schützendes Netz*
194.173.3.1, 194.173.3.2, 194.173.3.3, 194.173.3.4	194.173.3.10	2000	192.168.1.60	192.168.1.1
194.173.3.1, 194.173.3.2, 194.173.3.3, 194.173.3.4	194.173.3.11	2000	192.168.1.60	192.168.1.2
194.173.3.1, 194.173.3.2, 194.173.3.3, 194.173.3.4	194.173.3.12	2000	192.168.1.60	192.168.1.3
194.173.3.1, 194.173.3.2, 194.173.3.3, 194.173.3.4	194.173.3.13	2000	192.168.1.60	192.168.1.4

Tabelle 5.5: Beispiel einer Tabelle für einen n:m Port-Relay

Logbuch der Port Proxies

Durch den Port Proxy können folgende Einträge in das Logbuch des Application Gateway vorgenommen werden:

- IP-Adresse und Rechnername des Quell-Rechnersystems
- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Anzahl der Bytes, die übertragen wurden
- Uhrzeit und Datum des Verbindungsabbaus

Beispiel eines speziellen Circuit Level Proxies

Im Folgenden soll exemplarisch ein spezielles Circuit Level Proxy dargestellt werden, wie es von manchen Application Gateways angeboten wird.

Ein Permit Proxy regelt den Zugriff eines Client auf einen Server über das Application Gateway für TCP-basierte Dienste, die keinerlei Identifizierungs- und Authentisierungsmöglichkeiten bieten. Ein gutes Beispiel dafür sind NetBios Protokolle, die per IP getunnelt werden. Für solche Protokolle können keine speziellen Proxies eingesetzt werden, weil bei den Programmen auf der Client-Seite kein LogIn-Mechanismus vorgesehen ist.

neuKap05.fm Seite 171 Freitag, 18. Oktober 2002 3:51 15

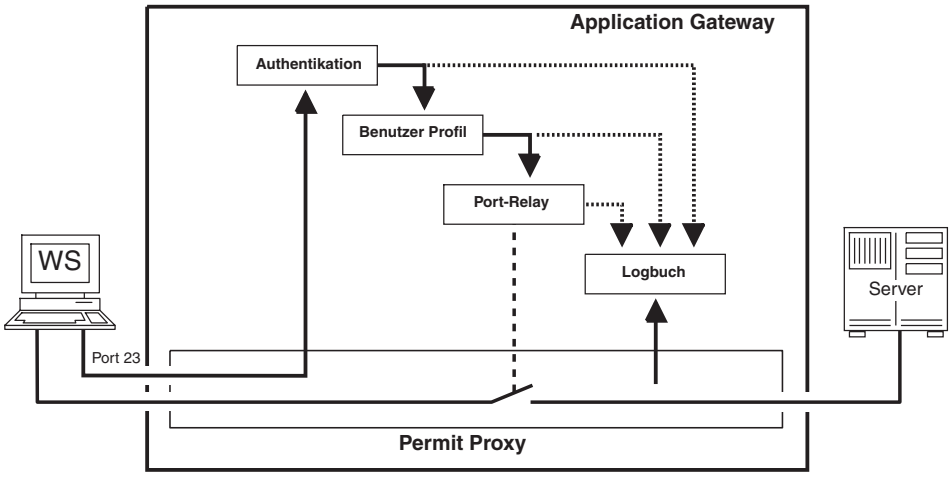


Abb. 5.33: Permit Proxy

Um dennoch den Zugriff auf bestimmte Rechnersysteme und Benutzer einzugrenzen, kann ein so genannter Permit Proxy eingesetzt werden. Dazu muss der Benutzer auf einem externen Rechnersystem zuerst eine Telnet-Verbindung (bzw. eine HTTP-Verbindung) zum Application Gateway aufbauen, bevor er seine eigentliche Applikation starten kann. Nach einer erfolgreichen Identifikation und Authentikation kann der Benutzer den eigentlichen Dienst über einen »Port-Proxy« in Anspruch nehmen.

Mithilfe des Permit Proxy kann dann festgelegt werden, über welchen Port, mit welchen Rechnersystemen (IP-Adressen) aus dem unsicheren Netz und auf welchem Rechnersystem (IP-Adresse) im zu schützenden Netz eine Kommunikation stattfinden darf. In diesem Beispiel wäre es auch möglich, über die Telnet-Verbindung weitere Verabredungen mit dem Application Gateway durchzuführen, wie z. B. die Festlegung der IP-Adresse, mit der die Kommunikation stattfinden soll (wie ein flexibler n:m Port-Relay).

Die Telnet-Sitzung wird automatisch durch das Beenden der Applikation geschlossen. Falls das Telnet-Progamm vor der Anwendung beendet wird, unterbricht der Permit Proxy die Verbindung zur Applikation.

Logbuch

Durch den Permit Proxy können folgende Einträge in das Logbuch des Application Gateway vorgenommen werden:

- IP-Adresse und Rechnername des Quell-Rechnersystems
- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus

neuKap05.fm Seite 172 Freitag, 18. Oktober 2002 3:51 15

- Name des Benutzers
- Uhrzeit und Datum des Verbindungsabbaus

Der Permit Proxy ist im Prinzip ein Circuit Level Proxy mit Authentikation.

Logbücher des Application Gateway

In den Logbüchern des Application Gateway können eine Vielzahl von Informationen festgehalten werden. Schon in der Sicherheitspolitik einer Organisation sollte festgelegt werden, welche Informationen protokolliert werden sollen und welche nicht, da die Datenmenge sonst sehr groß werden kann und einen hohen administrativen Aufwand verursacht.

5.4.2.13 SOCKS

SOCKS stellt eine standardisierte Umgebung zur transparenten und sicheren Nutzung eines Firewall-Systems zur Verfügung. Um dieses zu erreichen, integriert es sich zwischen der Anwendungs- und der Transportebene.

Abb. 5.34: SOCKS Layer

In dieser Zwischenschicht fängt SOCKS die TCP- und UDP-Verbindungsanfragen der Applikationen ab und setzt diese auf das SOCKS Protokoll um. Die Kommunikation über das SOCKS Protokoll beschränkt sich auf die Strecke zwischen dem SOCKS Client und dem SOCKS Server, sodass hierbei von einem Tunnel gesprochen werden kann.

Dieser Tunnel hat die Eigenschaft, dass sowohl für das verbindungsorientierte TCP- wie auch für das verbindungslose UDP-Protokoll ein Sicherheitskontext definiert werden kann. Das heißt, es existiert die Möglichkeit der starken Authentikation, der Integritätsüberprüfung und der Wahrung der Vertraulichkeit durch Verschlüsselung. Die Integration dieser Möglichkeiten ist in dem SOCKS Protokoll Standard »RFC1928« definiert. Hierbei handelt es sich um die Definition der Version 5 des Protokolls (SOCKS v5).

neuKap05.fm Seite 173 Freitag, 18. Oktober 2002 3:51 15

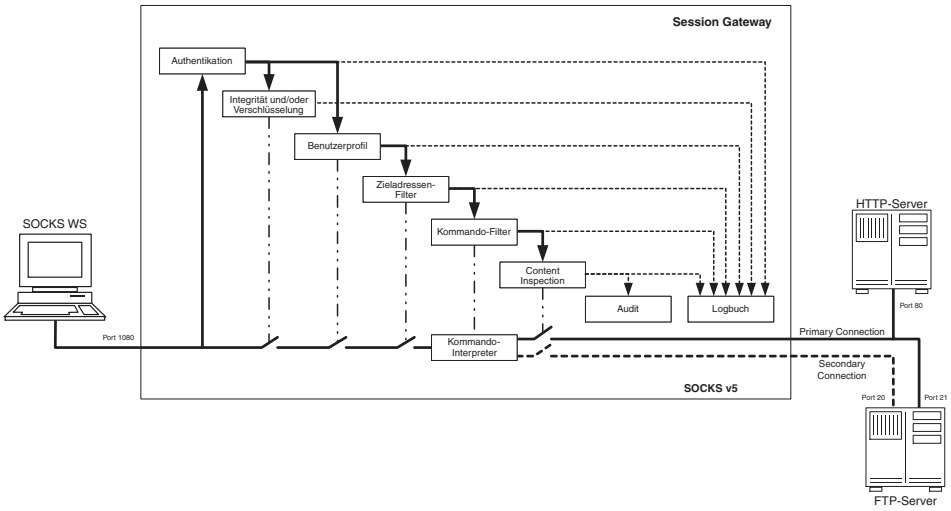


Abb. 5.35: SOCKS v5 Unterstützung für TCP

SOCKS vereint die Möglichkeiten eines Circuit Level Proxies mit den eines Application Level Proxies. Der Nachteil hierbei ist, das zur Nutzung von SOCKS Änderungen auf der Client Seite notwendig sind, da es bisher nur sehr wenige Applikationen gibt, welche SOCKS direkt unterstützen.

Der Verbindungaufbau erfolgt von der Client Applikation der Client Workstation. Dieser wird von der SOCKS v5 Client Bibliothek abgefangen und auf das SOCKS Protokoll umgesetzt. Endpunkt einer Standard SOCKS Verbindung ist TCP-Port 1080 des SOCKS v5 Server. Hierbei integriert sich die SOCKS v5 Client Implementation transparent in das Betriebssystem.

An den Verbindungsaufbau schließt sich die Aushandlung der Authentikationsmethode an. Der SOCKS v5 Client gibt eine Liste der von ihm unterstützten Methoden dem Server bekannt.

Der SOCKS v5 Server wählt eine auf die Quell-IP Adresse bezogene Methode aus und übermittelt diese dem SOCKS v5 Client. Ist keine Authentikation notwendig, bestätigt der Server den Verbindungsaufbau direkt. Hat der SOCKS v5 Client keine geeignete Methode übermittelt, bzw. ist diese Workstation nicht zur Nutzung von SOCKS berechtigt, wird die Verbindung beendet.

In allen weiteren Fällen durchlaufen SOCKS v5 Client und Server nun die notwendigen Authentikationsschritte bzw. zusätzliche methodenabhängige Unterverhandlungen.

Aus der erfolgreichen Authentikation leiten sich die Methoden zur Wahrung der Integrität und/oder der Vertraulichkeit direkt ab. Diese finden nach dem Abschluss der Authentikation Anwendung. Außerdem wird ein Benutzerprofil aktiviert, welches die möglichen Ziele wie auch Kommandos enthält.

neuKap05.fm Seite 174 Freitag, 18. Oktober 2002 3:51 15

Nach der Authentikation werden die weiteren Verbindungsdetails an den SOCKS v5 Server übermittelt. Der SOCKS v5 Server prüft die übergebenen Verbindungsdetails typischerweise auf der Basis der Quell-, Ziel-IP-Adresse und des Kommandos. Entspricht die Anfrage den aus dem Benutzerprofil stammenden Verbindungsregeln, so wird die Verbindung zum Server hergestellt. Der Verbindungsaufbau erfolgt durch den Kommandointerpreter. Der erfolgreiche Verbindungsaufbau wird dem SOCKS v5 Client mitgeteilt.

Die Client Applikation wird über den erfolgreichen Verbindungsaufbau informiert, sodass ab diesem Zeitpunkt Daten zwischen der Applikation und dem Server ausgetauscht werden können. Hierbei finden die methodenabhängigen Kriterien hinsichtlich Vertraulichkeit und Integrität Anwendung.

Zieladressenfilter

Aufgabe des Zieladressenfilters ist der Vergleich zwischen übermittelten Wunschziel und den Vorgaben aus dem aktivierten Benutzerprofil. Bei Nichtübereinstimmung erfolgt die Trennung der Verbindung und ein Eintrag in das Logbuch.

Es stehen drei Arten der Angabe von Adressen zur Verfügung:

- IP v4 Adresse
- IP v6 Adresse
- Domain Name

Diese Fähigkeiten ermöglichen den Aufbau eines IP v4 nach IP v6 Adressen Translators und vice versa mittels eines SOCKS Servers.

Kommandofilter

Der Kommandofilter vergleicht die im SOCKS Protokoll übermittelten Kommados mit den Vorgaben aus dem aktivierten Benutzerprofil. Beim Einsatz eines nicht erlaubten Kommandos wird die Verbindung getrennt und dieses im Logbuch festgehalten.

Die folgenden Kommandos sind in Protokoll Version 5 möglich:

- Connect
- Bind
- UDP Associate

Das »**Connect**« Kommando steht für den Verbindungsaufbau vom Client zum Server. Mittels des »**Bind**« Kommandos können Verbindungen vom Client akzeptiert werden, die vom Server aufgebaut werden. Als Beispiel sei der aktive FTP-Datenkanal genannt, welche von Port 20 des Servers zum Client aufgebaut wird. »**UDP Associate**« steht für den Aufbau eines UDP-Relays durch den SOCKS v5 Server.

neuKap05.fm Seite 175 Freitag, 18. Oktober 2002 3:51 15

Kommandointerpreter

Der Kommandointerpreter führt die jeweilige Aktion, welche mit dem entsprechenden Kommando verbunden ist, aus. Dieser ist auch für den Verbindungsabbau zuständig.

Content Inspection

Generell bietet SOCKS die Möglichkeit eine Inhaltsüberprüfung der Daten vorzunehmen. Diese implementationsabhängige Möglichkeit kann z. B. über eine PlugIn API verwendet werden.

Audit

Durch die inhaltliche Überprüfung eröffnet sich die Möglichkeit eines Auditings.

Logbuch

In das Logbuch können folgende Einträge vom SOCKS v5 Server standardmäßig vorgenommen werden:

- IP-Adresse und Rechnername des Quell-Rechners
- IP-Adresse und Rechnername des Ziel-Rechners
- Uhrzeit und Datum des Verbindungsaufbaus
- Name des Benutzers und das verwendete Authentikationsverfahren
- aktiviertes Benutzerprofil
- verwendete SOCKS Protokoll Kommandos
- Anzahl der übertragenen Bytes
- inhaltliche Informationen des »getunnelten« TCP- und UDP-Protokolle
- Uhrzeit und Datum des Verbindungsabbaus

Der Protokollablauf gleicht dem zuvor für eine TCP-Verbindung beschriebenen. Lediglich bei der Weiterleitung der UDP-Datagramme von der SOCKS v5 Client Bibliothek zum SOCKS v5 Server erfolgt eine Erweiterung.

Die UDP Client Applikation sendet ein UDP-Datagramm an den Server. Dieser Vorgang wird von der SOCKS v5 Client Bibliothek abgefangen und als Verbindungswunsch mit dem SOCKS Kommando »**UDP Associate**« an den SOCKS v5 Server weitergeleitet. Nach dem erfolgreichen Durchlauf der Authentikation, der Berücksichtigung aller Integritäts und/oder Verschlüsselungs Methoden, der Aktivierung eines Benutzerprofils und der Überprüfung des Verbindungswunschs erfolgt die Auswertung durch den Kommandointerpreter.

Dieser liefert als Antwort, auf die zuvor gestellt Anfrage nach einem »**UDP Associate**«, den UDP-Port den der SOCKS v5 Client zur Weiterleitung des zurückgehaltenen Datagramms verwenden soll. Außerdem wird eine UDP Relay Instanz erzeugt.

neuKap05.fm Seite 176 Freitag, 18. Oktober 2002 3:51 15

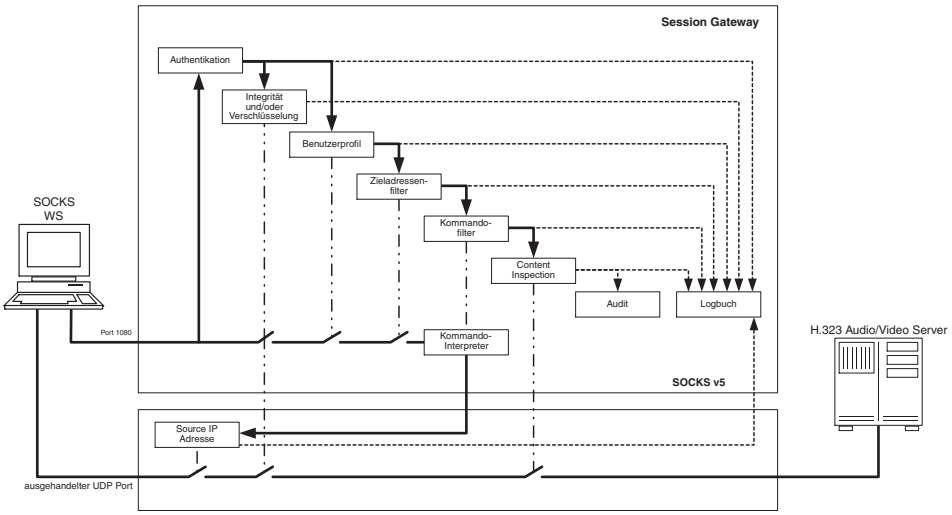


Abb. 5.36: SOCKS v5 Unterstützung für UDP

Die UDP Relay Instanz filtert alle ankommenden UDP-Datagramme und leitet nur diese weiter, welche die gleiche Quell IP-Adresse haben wie der TCP-Kontrollkanal.

Auch bei dieser zweiten Verbindung finden die methodenabhängigen Kriterien hinsichtlich Vertraulichkeit und Integrität Anwendung.

Außerdem ist auch hier die inhaltliche Überprüfung möglich, sofern dies von der Implementation unterstützt wird.

Source IP Adresse

Der Kommandointerpreter übergibt die Quell-IP-Adresse des TCP-Kontrollkanals als Filterwert an die UDP-Relay-Instanz. Alle Datagramme die nicht diese Adresse tragen werden verworfen.

Dieses kann in dem Logbuch protokolliert werden.

SOCKS-Versionübersicht

SOCKS Version 4

Die veraltete Version 4 des SOCKS Protokolls enthielt keinerlei Sicherheitsmaßnahmen zur Authentikation und Wahrung der Vertraulichkeit und/oder der Integrität. Es wurden nur die Kommandos »Bind« und »Connect« unterstützt.

SOCKS Version 5

Die aktuelle Version 5 enthält die folgenden Merkmale:

- standardisierte Schnittstellen zur Integration von starken Authentikationsmechanismen

neuKap05.fm Seite 177 Freitag, 18. Oktober 2002 3:51 15

- erweitertes Adress-Schema zur Unterstützung von IP v4, IP v6 und Domain Namen
- Unterstützung für TCP und UDP
- Verfügbare Implementationen integrieren sich transparent in das Betriebssystem.

Allerdings sollen die Nachteile von SOCKS v5 nicht verschwiegen werden:

- Der Aufbau mehrerer Verbindungen von einem Server zu einem Client ist nicht ausreichend unterstützt.
- Die UDP-Implementation bietet keine Unterstützung von Multicasts.
- großer Protokoll Overhead pro Verbindung
- Es existieren nicht standardisierte Erweiterungen.
- Die Skalierbarkeit von SOCKS v5 ist nicht ausreichend.

SOCKS Version 6

Für die nächste Protokollversion sind die folgende Erweiterungen geplant:

- Major und Minor Version Nummerierung für bessere Rückwärts-Kompatibilität
- Standard Mechanismus zur Aushandlung von Protokoll Erweiterungen
- Nutzung eines Kontrollkanals zur Reduzierung des Overheads
- TCP: Bind-Kommandoerweiterung zur Unterstützung von mehreren Verbindungen auf den offenen Port, sowie die Möglichkeit der Vorgabe eines bestimmten Ports durch den Client
- UDP: Unterstützung für Multicast in einer Multicast-Umgebung und einer Multicast freien Umgebung
- UDP: Wahlmöglichkeit zwischen Senden und Empfangen von Datagrammen
- UDP: Möglichkeit der Tunnelung von Datagrammen durch einen zuverlässigen Kanal

5.4.2.14 Anwendungsbeispiel für den SOCKS v5 Server

Mithilfe des SOCKS v5 Servers können Dienste wie H.323 (digitale Audio- und Video-Übertragung) und CORBA (IIOP) über ein Firewall-System realisiert werden. Wobei bei der Unterstützung von H.323 Protokoll Erweiterungen aus der Version 6 des SOCKS Protokolls verwendet werden müssen.

Außerdem kann die Personen und Session bezogene starke Authentikation über das Internet realisiert werden. Dies kann durch Mechanismen zur Wahrung der Vertraulichkeit und/oder der Integrität erweitert werden.

Außerdem stellt es in einigen Fällen die einzige Möglichkeit zur sicheren Nutzung mehrerer kaskadierter Firewall-Systeme dar.

neuKap05.fm Seite 178 Freitag, 18. Oktober 2002 3:51 15

5.4.3 Anwendungsgebiete von Application Gateways

Immer dann, wenn es notwendig ist, Schutzmaßnahmen für die Anwendungen zur Verfügung zu stellen, ist ein Application Gateway ein ideales aktives Firewall-Element. Die Möglichkeit der Protokollierung auf der Anwendungsebene kann ebenfalls ein besonderer Grund sein, das Application Gateway in einem Firewall-Konzept zu berücksichtigen.

Für die Ankopplung an das Internet ist auf jeden Fall ein Application Gateway in der Firewall-Konstellation zu berücksichtigen, wenn die Rechnersysteme im zu schützenden Netz einen hohen Schutzbedarf haben (siehe auch Kapitel 6 *Konzepte für Firewall-Systeme*).

Außerdem können Organisationseinheiten, die sich abschotten wollen, hiermit einen besonderen Schutz erzielen.

Vorteile und besondere Aspekte eines Application Gateway

- sicheres Design-Konzept, da kleine, gut überprüfbare Module (Proxies)
- Konzentration auf das Wesentliche
- Alle Pakete müssen über Proxies übertragen werden, das bedeutet höhere Sicherheit.
- Der Kommunikationspartner der Rechnersysteme, die über das Application Gateway kommunizieren, ist der Proxy; dadurch kann eine echte Entkopplung der Dienste erreicht werden.
- Verbindungsdaten und Applikationsdaten können protokolliert werden, wodurch die Handlungen der Benutzer, die über das Application Gateway kommunizieren, festgehalten werden können.
- Verbergen der internen Netzstruktur
- Sicherheitsfunktionen für die Anwendungen werden zur Verfügung gestellt (Kommando-, Datei- und Daten-Filter usw.)
- Eine Network Address Translation findet statt.

Nachteile und Grenzen eines Application Gateway

- geringe Flexibilität, da für jeden neuen Dienst ein neuer Proxy zur Verfügung gestellt werden muss
- Die Kosten für ein Application Gateway sind in der Regel höher.
- andere Vorgehensweise bei der Kommunikation über das Application Gateway (ist nicht transparent)
- Einige Application Gateways können kein IP-Spoofing erkennen (dies ist kein generelles Problem).

neuKap05.fm Seite 179 Freitag, 18. Oktober 2002 3:51 15

5.5 Adaptive Proxy

Einige Sicherheitshersteller versuchen, unter dem Namen »Adaptive Proxy« die Vorteile von Packet Filter und Application Gateway zu kombinieren. Die Idee bei diesem Ansatz ist, dass ein betrachtetes Firewall-System in einer ersten Phase (Verbindungsaufbauphase) der »Adaptive Proxy« wie ein Application Proxy arbeitet und in einer späteren Phase (Datentransferphase) wie ein Packet Filter agiert. Der Vorteil dieser Methode liegt auf der Hand: In der ersten Phase wird eine sehr hohe Sicherheit erreicht, danach erst werden die schnellen Tests der Packet Filter durchgeführt. Das heißt, unter der Annahme, dass alle Angriffe die ersten Phase, also den Aufbau einer Kommunikationsverbindung, betreffen, würde man bei diesem Ansatz eine hohe Sicherheit erreichen.

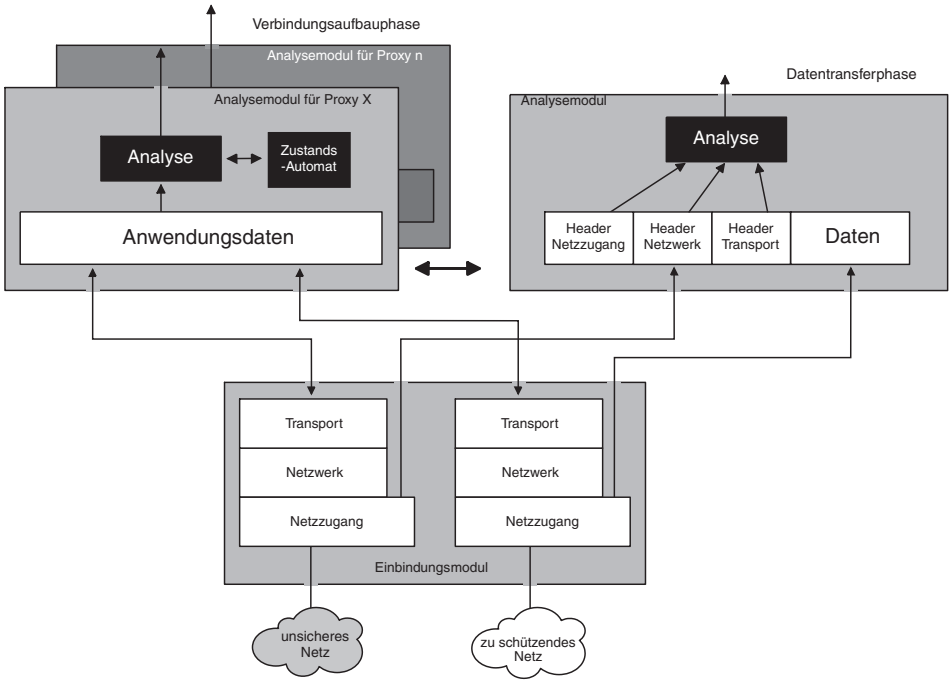


Abb. 5.37: Arbeitsweise eines Adaptive Proxy

Analogie zum Pförtner

Der Adaptive Proxy arbeitet in der ersten Phase (Verbindungsaufbauphase) wie der Application Proxy: Er schaut sich nicht nur die Adresse der eingehenden Pakete an, er öffnet auch das Paket und überprüft den gesamten Inhalt. Wenn der Adapive Proxy den Lieferanten seit langem kennt, dann sendet er den LKW des Lieferanten durch das Tor, damit dieser die Lieferung direkt zustellt. Kennt er den Lieferanten

neuKap05.fm Seite 180 Freitag, 18. Oktober 2002 3:51 15

jedoch nicht, dann schickt er den LKW-Fahrer nach Ausladung der Lieferung weg und bestellt den firmeneigenen Fahrer, der im eigenen LKW das Paket zum Empfänger bringt.

Da ein elektronischer Pförtner aber nicht auf persönliche, menschliche Bindung aufbauen kann, scheint der Adaptive Proxy mehr in der Theorie interessant zu sein als in der Praxis, da er kaum die Qualität eines Application Proxy erreichen kann. Oder das Äquivalent der persönlichen, menschlichen Bindung kann mithilfe von vertrauenswürdigen Netzen oder/und der Nutzung von Verschlüsselungssystemen realisiert werden. Hier muss aber eine genaue Analyse der Bedrohungen und der Einsatzumgebung durchgeführt werden.

5.6 Firewall-Elemente und das Verhältnis von Geschwindigkeit zu Sicherheit

Diese Darstellung stellt eine Art der Klassifizierung von Firewall-Elementen dar. Eine detailliertere und weitaus ausführlichere Darstellung wird in Kapitel 6 *Konzepte für Firewall-Systeme* diskutiert.

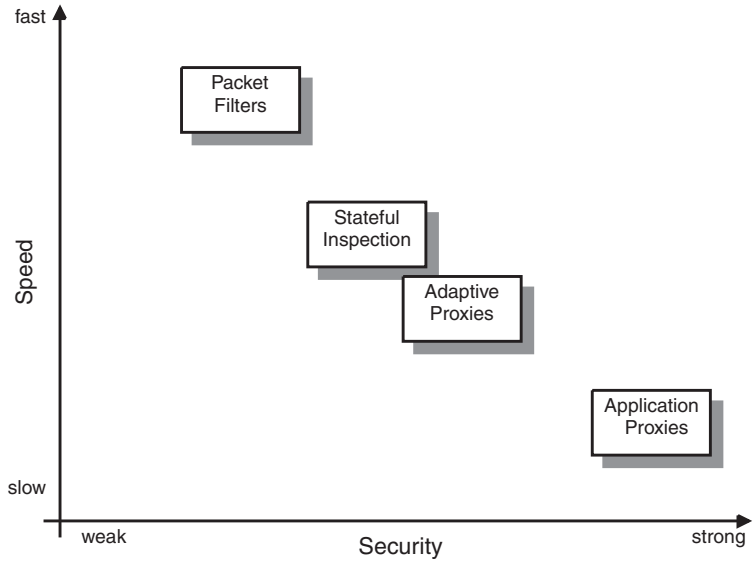


Abb. 5.38: Geschwindigkeit versus Sicherheit

Durch den Einsatz mehrerer paralleler Application Gateways ist insgesamt eine höhere Leistungsfähigkeit (Durchsatz) zu erreichen (siehe Kap. 6.4.3).

neuKap05.fm Seite 181 Freitag, 18. Oktober 2002 3:51 15

5.7 Security Management für aktive Firewall-Elemente

Mithilfe eines Security Managements sollte eine einfache, zuverlässige und nachprüfbare Verwaltung der aktiven Firewall-Elemente möglich sein.

Wegen der besonderen Designanforderung, dass aktive Firewall-Elemente mit minimaler Software realisiert werden müssen, ist ein separates Security Management unbedingt notwendig. Ein separates Security Management kann z. B. auf einem separaten Rechnersystem, oder mithilfe von Wechselplatten, die nur für die Festlegung der Regeln eingeführt werden, realisiert werden.

Anforderungen an ein Security Management

Das Security Management muss selbst gegen Angriffe resistent sein, weil sonst Angreifer über das Security Management die Sicherheitsfunktionen der aktiven Firewall-Elemente ausschalten können. Dazu sollte das Security Management selber Sicherheitsmechanismen wie Identifikation und Authentikation, Rollen-Verteilung, Protokollierung mit Audit-Möglichkeiten sowie Verschlüsselung der sicherheitsrelevanten Informationen im Security Management bieten, damit Angriffe auf das Security Management abgewehrt werden können.

Ein Security Management für aktive Firewall-Elemente soll mindestens die Sicherheitsdienste »Benutzerfreundlichkeit« und »Widerspruchsfreiheit von Regeln« erfüllen.

- Benutzerfreundlichkeit: Die Menüführung des Security Managements soll einfach und zuverlässig sein. Außerdem sollen keine redundanten Eingaben notwendig sein.
- Widerspruchsfreiheit der Filterregeln: Fehleingaben in den Eingabefeldern (MAC-Adresse, IP-Adresse, Protokollnummer, Portnummern) sollten nicht möglich sein. Hier sollte eine syntaktische Überprüfung stattfinden.
- Filterregeln sollten nur für die entsprechende Protokollschicht einstellbar sein. Benutzer sollten nicht gleichzeitig als aktiv und gesperrt für einen Dienst eingetragen werden können. Mehrfach-Einträge werden eliminiert. Des Weiteren sollte eine semantische Überprüfung der Filterregeln erfolgen.

Damit eine hohe Gesamtsicherheit des gesamten Firewall-Systems gewährleistet werden kann, müssen zusätzlich die Sicherheitsfunktionen Zugangskontrolle, Rechteverwaltung, Verschlüsselung und Protokollierung zur Verfügung gestellt werden.

- Zugangskontrolle im Security Management: Hier soll eine Identifikation und Authentikation der Nutzer durchgeführt werden, damit Unberechtigte das Security Management nicht nutzen können.

neuKap05.fm Seite 182 Freitag, 18. Oktober 2002 3:51 15

- Rechteverwaltung (Rollen) im Security Management: Um einen sicheren Betrieb des Security Management zu gewährleisten, sollten möglicherweise die folgenden Rollen auf dem Security Management angeboten werden: Security Administrator, Operator, Editor, Observer und Auditor.
  - Der Security Administrator ist z. B. für die Personalisierung des Security Management, die Vergabe der Zugriffsrechte des Security Management und das Erstellen und Wiedereinspielen von BackUps verantwortlich.
  - Der Operator hat die Aufgabe, die Rechte der Benutzer, die über die aktiven Firewall-Elemente kommunizieren dürfen, nach der Sicherheitspolitik seiner Organisation einzugeben.
  - Ein Editor ist für die Datenerfassung von nicht sicherheitskritischen Daten wie Benutzernamen, Rechnersysteme, Profile etc. verantwortlich. Er kann keine Rechte vergeben oder entziehen.
  - Der Observer hat die Aufgabe, den Betrieb des aktiven Firewall-Elementes zu beobachten und gegebenenfalls Probleme zu analysieren. Er kann keine Rechte vergeben oder entziehen.
  - Der Auditor übernimmt die Aufgabe, die Logbuchdaten des Security Managements auf sicherheitskritische Aktionen zu überprüfen. Er kann keine Rechte vergeben oder entziehen.

Für ganz besondere sicherheitskritische Aktionen auf dem Security Management kann ein Vier-Augen-Prinzip verlangt werden, bei dem zwei oder mehr Personen nur gemeinsam, z. B. durch die Eingabe ihres Passwortes, eine Aktion auslösen dürfen.

Die sicherheitsrelevanten Informationen, z. B. Passworte oder Schlüssel für die Authentikation mit den aktiven Firewall-Elementen, sollten im Security Management in verschlüsselter Form abgespeichert werden, damit kein Missbrauch mit diesen Informationen stattfinden kann.

Die verschiedenen Funktionen im Security Management sollten in separaten Logbüchern protokolliert werden. Zu diesem Zweck sollte das Security Management z. B. folgende Logbücher zur Verfügung stellen:

- In einem Funktions-Logbuch werden alle Aktionen festgehalten, die mithilfe des Security Managements durchgeführt werden, z. B. die Vergabe der Rechte für die Benutzer, das Löschen von Logbüchern usw. In diesem Logbuch können die Handlungen der Benutzer (Security Administrator, Operator usw.) des Security Managements festgehalten werden.
- Mit einem LogIn-Logbuch werden alle LogIns festgehalten, die mit dem Security Management durchgeführt werden.
- In dem Fehler-Logbuch werden alle Fehler, die im Security Management erkannt werden, festgehalten.
- Im Backup-Logbuch werden alle Backup-Aktionen geloggt, die der Security Administrator auf dem Security Management durchführt.

neuKap05.fm Seite 183 Freitag, 18. Oktober 2002 3:51 15

Weitere Anforderungen

- Kopplung an ein Netzwerkmanagement-System (NMS)
  Die besonders hohe Verfügbarkeit von Firewall-Systemen macht es in der Regel erforderlich, bestimmte Spontane Meldungen der Firewall-Elemente, die Auskunft über die Verfügbarkeit des Systems geben, an das Netzwerkmanagement zu senden, weil dieses in größeren Organisationen eine 24-Stunden-Besetzung hat und bei Ausfällen schnell reagieren kann. Dazu sollte das Security Management in der Lage sein, SNMP-Traps und einfache GET-Befehle mithilfe eines SNMP Proxy mit dem Netzwerkmanagement auszutauschen.

- Kommunikationsschutz für das Security Management
  In vielen Firewall-Systemanordnungen macht es Sinn, das Security Management selbst mit einem Packet Filter abzuschotten. Wenn ein Packet Filter mit Verschlüsselung (VPN-Box) verwendet wird, ist es auch möglich, remote auf das Security Management zuzugreifen. Dies kann dann sinnvoll sein, wenn in den unterschiedlichen Organisationseinheiten lokale Security Manager tätig sind, die dann auf ein zentrales Security Management zugreifen (siehe auch Kapitel 10 *Praktischer Einsatz von Firewall-Systemen*).

neuKap05.fm Seite 184 Freitag, 18. Oktober 2002 3:51 15

neuKap06.fm Seite 185 Freitag, 18. Oktober 2002 3:51 15

Kapitel 6

Konzepte für Firewall-Systeme

In diesem Kapitel werden verschiedene Konzepte diskutiert, nach denen Firewall-Systeme aufgebaut werden können, die zwischen einem unsicheren und einem zu schützenden Netz die Sicherheit von Daten und Kommunikation gewährleisten sollen. Die vorgestellten Firewall-Konzepte unterscheiden sich nach dem Maß an Sicherheit, das sie erbringen können, und nach den Einsatzfällen, für die sie sich eignen.

Zunächst werden nur die konzeptionellen Aspekte betrachtet. Praktische Einsatzfälle werden im Kapitel 10 *Praktischer Einsatz von Firewall-Sytemen* behandelt.

Bei den verwendeten aktiven Firewall-Elementen handelt es sich um Sicherheitskomponenten, die ausschließlich für die Erbringung von Sicherheitsdiensten verantwortlich sind und den Designkriterien entsprechen, die in Kapitel 5.1.2 *Designkonzept aktiver Firewall-Elemente* als sicher herausgestellt wurden. Routerfunktionalitäten werden, falls erforderlich, von Routern erbracht, von denen keine weitere Sicherheitsfunktionalität erwartet wird, und nicht von Packet Filtern oder Application Gateways. Alle vorgestellten Konzepte gehen davon aus, dass die aktiven Firewall-Elemente mithilfe eines Security Managements gesteuert und verwaltet werden.

6.1 Ausschließlicher Einsatz eines Packet Filters

In diesem Firewall-Konzept wird das aktive Firewall-Element »Packet Filter« ausschließlich für den Schutz zwischen unsicherem und zu schützendem Netz eingesetzt. Das Security Management steht im zu schützenden Netz.

Mit diesem Firewall-Konzept können folgende Sicherheitsziele erreicht werden:

- Die *Zugangskontrolle auf der Netzzugangs- und Netzwerkebene* bewirkt, dass nur logische Verbindungen zustande kommen, die erlaubt sind. Die Kontrolle erfolgt durch
  - Überprüfung der MAC-Ziel- und MAC-Quell-Adresse
  - Überprüfung der IP-Ziel- und die IP-Quell-Adresse

neuKap06.fm Seite 186 Freitag, 18. Oktober 2002 3:51 15

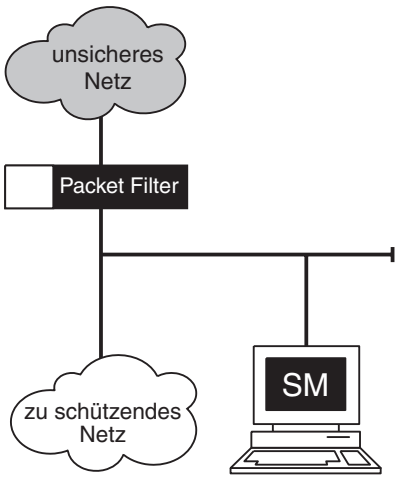


Abb. 6.1: Ausschließlicher Einsatz eines Packet Filters

- Mit der *Rechteverwaltung* wird erreicht, dass nur über Protokolle und Dienste (Portnummer) zugegriffen werden kann, die definiert und erlaubt sind, und zwar zu bestimmten Zeiten.
  Folgende Rechtebeschränkungen können z. B. mit Packet Filtern realisiert werden:
  - welche Optionen sind bei IP erlaubt (z. B. Fragmentierung, Source-Routing)
  - welche Kommunikationsprotokolle wie TCP, UDP oder ICMP dürfen verwendet werden
  - welche Quell- und Ziel-Ports sind für TCP erlaubt
  - welche Quell- und Ziel-Ports sind für UDP erlaubt
  - welche ICMP-Kommandos sind erlaubt
  - usw. (siehe Kapitel 5 *Elemente eines Firewall-Systems*)

Weitere Sicherheitsziele sind:

- *Protokollauswertung:* Sicherheitsrelevante Ereignisse werden protokolliert und können zur Erkennung von Sicherheitsverletzungen ausgewertet werden.
- *Alarmierung:* Besonders sicherheitsrelevante Ereignisse werden als Alarme spontan beim Auftreten an ein Security Management gesendet, damit bei einem Angriff schnell reagiert werden kann.

Bewertung des Firewall-Konzepts

Ein Firewall-Konzept, das aus dem ausschließlichen Einsatz eines Packet Filter besteht, kann nicht für die Kopplung eines zu schützenden Netzes an das Internet eingesetzt werden, da der Schutzbedarf für die meisten zu schützenden Netze zu hoch ist, als dass ein Packet Filter ihn alleine erfüllen könnte. Mit einem solchen Firewall-Konzept kann allerdings eine geregelte Kommunikation im Intranet rea-

neuKap06.fm Seite 187 Freitag, 18. Oktober 2002 3:51 15

lisiert werden. Kombiniert mit einer Verschlüsselung ist ein Packet Filter eine flexible und kostengünstige Möglichkeit, eine vertrauliche und kontrollierte Kommunikation im Intranet zu gewährleisten (siehe auch Kapitel 7 *Firewall-Systeme und Verschlüsselung)*.

Ein weiterer Vorteil von Packet Filtern ist, dass sie in der Regel auch andere Protokollfamilien unterstützen, z. B. IPX, OSI, DECNET, SNA.

Einsatz von Packet Filtern

Falls das unsichere Netz und das zu schützende Netz ein vergleichbares Schutzniveau innerhalb eines eigenen Verantwortungsbereiches haben, wie dies z. B. in Intranet-Anwendungen der Fall ist, kann ein einzelner Packet Filter die Kommunikationsverbindung kontrollieren. Wenn für diesen Fall Packet Filter mit Verschlüsselung verwendet werden, kann hier ein noch höheres Maß an Sicherheit im Intranet erreicht werden.

6.2 Ausschließlicher Einsatz eines Application Gateway

Das aktive Firewall-Element »Application Gateway« wird in diesem Firewall-Konzept ausschließlich für den Schutz zwischen dem unsicheren und dem zu schützenden Netz verwendet. Das Security Management steht im zu schützenden Netz.

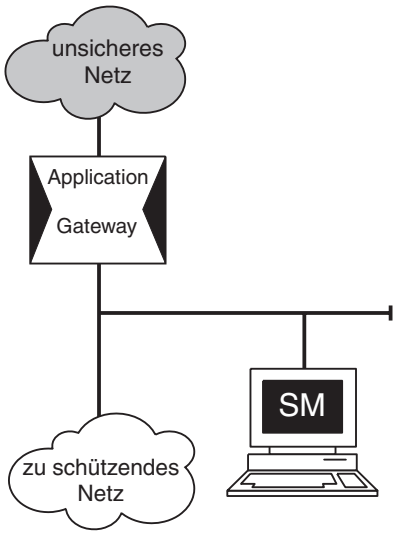


Abb. 6.2: Ausschließlicher Einsatz eines Application Gateway

Das Application Gateway wird in diesem Beispiel als dual-homed-Host eingesetzt; das bedeutet, dass das Application Gateway mit zwei Netzschnittstellen arbeitet

neuKap06.fm Seite 188 Freitag, 18. Oktober 2002 3:51 15

und somit die vollständige Kontrolle über die Pakete hat, die zwischen dem unsicheren und dem zu schützenden Netzwerk übertragen werden sollen.

Durch den Einsatz eines Application Gateway können folgende Sicherheitsziele erreicht werden:

- Die *Zugangskontrolle auf der Netzwerkebene* bewirkt, dass nur logische Verbindungen zustande kommen, die erlaubt sind.
  - IP-Ziel- und IP-Quell-Adresse werden in den jeweiligen Netzen überprüft
- Durch eine *Zugangskontrolle auf Benutzerebene* können alle Benutzer, die über das Application Gateway kommunizieren wollen, identifiziert und authentisiert werden.
- Mit der *Rechteverwaltung* wird erreicht, dass nur über Protokolle und Dienste zugegriffen werden kann, die definiert und erlaubt sind, und zwar zu bestimmten Zeiten. Nur solche Dienste sind möglich, für die ein Proxy auf dem Application Gateway installiert und freigeschaltet worden ist.
- Eine *Kontrolle auf der Anwendungsebene* erlaubt dem Benutzer nur die Dinge, die für seine Aufgabenstellung notwendig sind. Dies erfolgt für die jeweiligen Dienste durch spezielle Anwendungsfilter für Kommandos, Anwendungsdaten und Dateien.
- Durch eine *Entkopplung der Dienste* werden besonders risikobelastete Programme (wie z. B. »sendmail«) dem unsicheren Netz nur über eigene Hilfsprogramme mit eingeschränkter Funktionalität (Proxies) zur Verfügung gestellt.
- *Beweissicherung und Protokollauswertung* ermöglichen, dass Verbindungsdaten und sicherheitsrelevante Ereignisse protokolliert werden und für die Erkennung von Sicherheitsverletzungen und die Beweissicherung von Handlungen der Benutzer ausgewertet werden können.
- Eine *Alarmierung* des Security Management wird beim Erkennen von besonders sicherheitsrelevanten Ereignissen an das Security Management gesendet (Spontane Meldung). Damit kann bei einem Angriff schnell reagiert werden kann.
- Application Gateways ermöglichen das *Verbergen der internen Netzstruktur* des zu schützenden Netzes. Dies erschwert einem Angreifer aus dem unsicheren Netz den Zugriff auf interne, sicherheitskritische Systeme.
- *Weitere Ziele*, die mithilfe eines Application Gateway erreicht werden können:
  - Accounting (IP- und benutzerorientiert)
  - Network Address Translation

Einsatzfall

Falls das unsichere Netz und das zu schützende Netz ein vergleichbares Schutzniveau haben und das unsichere Netz außerhalb des eigenen Verantwortungsbereiches liegt, können die beiden Netze nur durch ein Application Gateway kontrolliert verbunden werden. Dies könnte z. B. bei der Kooperation zweier ähnlicher, gleichwertiger Organisationen zutreffen. Ein besonderer Aspekt bei der Ver-

neuKap06.fm Seite 189 Freitag, 18. Oktober 2002 3:51 15

wendung von Application Gateways ist, dass Verbindungsdaten ausführlich protokolliert werden können.

6.3 Kombination von Firewall-Elementen

Mit einer geschickten Kombination der einzelnen aktiven Firewall-Elemente lässt sich ein höheres Maß an Sicherheit erzielen als bei der Nutzung nur eines aktiven Firewall-Elementes. Im folgenden Abschnitt werden unterschiedliche Konzepte von Kombinationen dargestellt und diskutiert.

Unterschiedliche Verwendung von Application Gateways

Application Gateways werden in den verschiedenen Firewall-Konzepten unterschiedlich verwendet. Aus diesem Grund werden zwei Verwendungsvarianten von Application Gateways dargestellt.

Dual-homed Application Gateway

Ein dual-homed Application Gateway (Abb. 6.3) arbeitet mit zwei Netzschnittstellen, wobei die Pakete über die eine Netzschnittstelle (z. B. aus dem unsicheren Netz) hereinkommen und über die andere Netzschnittstelle (z. B. in das zu schützende Netz) hinausgehen. Damit hat das dual-homed Application Gateway die volle Kontrolle über die Pakete, die zwischen dem unsicheren und dem zu schützenden Netzwerk übertragen werden sollen. Es gibt keinen Weg, auf dem das dual-homed Application Gateway umgangen werden könnte. Das dual-homed Application Gateway wird als »dual-homed« bezeichnet, weil es ein Rechnersystem im unsicheren und im zu schützenden Netz ist.

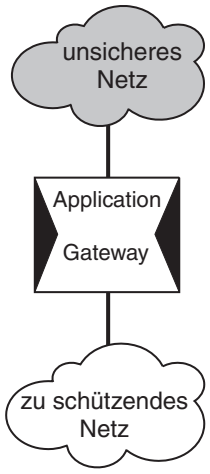


Abb. 6.3: Dual-homed Application Gateway

neuKap06.fm Seite 190 Freitag, 18. Oktober 2002 3:51 15

Single-homed Application Gateway

Bei einem single-homed Application Gateway (Abb. 6.4) kommen die Pakete über die selbe Netzschnittstelle herein, über die sie auch hinausgehen. Damit kann das Application Gateway selbst nicht garantieren, dass alle Pakete vom Application Gateway analysiert und kontrolliert werden. Aus Sicht des Application Gateway gibt es nur ein Netz, aus diesem Grund wird es als »single-homed« bezeichnet.

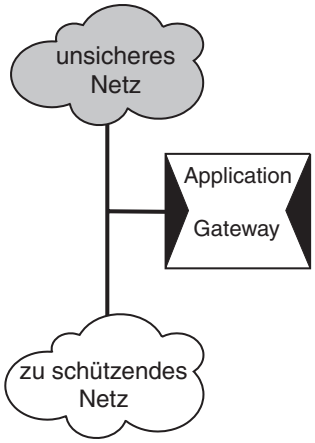


Abb. 6.4: Single-homed Application Gateway

Im Folgenden werden Kombinationsmöglichkeiten mehrerer Firewall-Elemente diskutiert. Durch eine Kombination von unterschiedlichen Firewall-Konzepten werden die Sicherheitsziele der einzelnen Konzepte Packet Filter und Application Gateway je nach Konstellation addiert, sodass ein höheres Maß an Sicherheit erreicht wird. In den jeweiligen Abschnitten wird auch eine Einschätzung und Bewertung der Firewall-Konzepte gegeben.

6.3.1 Packet Filter und single-homed Application Gateway

In der Kombination eines Packet Filter mit einem single-homed Application Gateway wird die Sicherheit in erster Linie durch das aktive Firewall-Element Packet Filter gewährleistet, während das single-homed Application Gateway optional zusätzliche Sicherheitsdienste zur Verfügung stellt.

Beschreibung der Abbildung 6.5

Der Packet Filter kann so konfiguriert werden, dass eine Kommunikation aus dem unsicheren Netz nur über das single-homed Application Gateway erlaubt ist, d.h., aus dem unsicheren Netz wird nur das single-homed Application Gateway »gesehen«. Vom single-homed Application Gateway können dann alle Sicherheitsdienste erbracht werden.

neuKap06.fm Seite 191 Freitag, 18. Oktober 2002 3:51 15

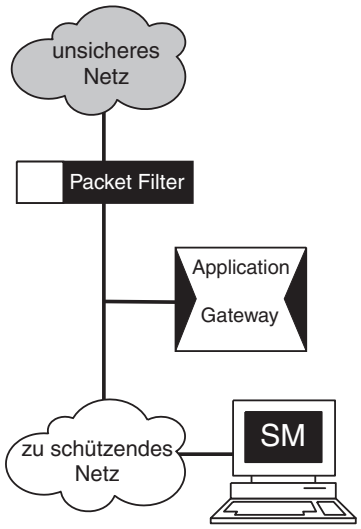


Abb. 6.5: Packet Filter und single-homed Application Gateway 1

Logisch befindet sich das single-homed Application Gateway bei diesem Firewall-Konzept im zu schützenden Netz. Die Kommunikation zwischen den Rechnersystemen im zu schützenden Netz und den Rechnersystemen aus dem unsicheren Netz wird durch den Packet Filter kontrolliert über das Application Gateway abgewickelt. Wenn ein Angreifer Zugang zum single-homed Application Gateway erlangen würde, könnte er auch auf alle Rechnersysteme im zu schützenden Netz zugreifen, weil kein weiterer Schutz vorhanden ist.

Beschreibung der Abbildung 6.6

Die Kommunikation aus dem zu schützenden Netz kann durch das Packet Filter so gesteuert werden, dass sie nur über das single-homed Application Gateway erlaubt wird, d.h., aus dem zu schützenden Netz wird nur das single-homed Application Gateway »gesehen«. Vom single-homed Application Gateway können dann alle Sicherheitsdienste erbracht werden.

Logisch befindet sich das single-homed Application Gateway bei diesem Firewall-Konzept im unsicheren Netz und muss daher Angriffen aus dem unsicheren Netz gegenüber besonders widerstandsfähig sein. Eine besondere Gefahr besteht bei diesem Konzept in einem IP-Maskerade-Angriff aus dem unsicheren Netz. Die Kommunikation zwischen den Rechnersystemen im zu schützenden Netz und den Rechnersystemen aus dem unsicheren Netz wird durch das Packet Filter kontrolliert über das single-homed Application Gateway abgewickelt.

neuKap06.fm Seite 192 Freitag, 18. Oktober 2002 3:51 15

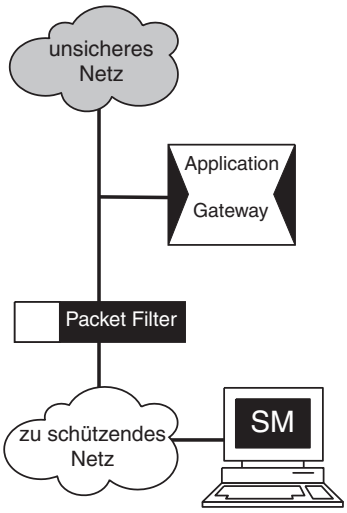


Abb. 6.6: Packet Filter und single-homed Application Gateway 2

Bewertung des Firewall-Konzepts

Die Kombination Packet Filter – single-homed Application Gateway bietet die Möglichkeit, für bestimmte Verbindungen die Kommunikation nur über das Packet Filter zu erlauben, z. B. für solche Dienste, für die es auf dem single-homed Application Gateway keine Proxies gibt. Diese Möglichkeit macht das Firewall-Konzept sehr flexibel, weil einige Dienste nur über den Packet Filter und andere nur zusätzlich über das single-homed Application Gateway zugelassen werden können.

Die Sicherheit, die dieses Firewall-Konzept bietet, hängt in erster Linie von der Sicherheit des Packet Filter ab. Aus diesem Grund muss das Packet Filter in diesem Konzept besonders sicher sein (siehe Kapitel 5.1.2 *Designkonzept aktiver Firewall-Elemente*). Da der Schutzbedarf der meisten zu schützenden Netze höher ist als der Schutz, den die Sicherheitsmechanismen Packet Filter bieten können, ist dieses Konzept für die Ankopplung eines zu schützenden Netzes an das Internet nicht ausreichend.

Die Lösung aus Abb. 6.5 bietet aus der Sicht des zu schützenden Netzes ein höheres Maß an Sicherheit, weil das single-homed Application Gateway durch das Packet Filter geschützt wird.

Einsatzfall

Falls das unsichere Netz ein geringes oder nicht einschätzbares Schutzniveau hat, aber sowohl das unsichere wie auch das zu schützende Netz innerhalb eines eigenen Verantwortungsbereiches liegen, können Kombinationen von Packet Filter und single-homed Application Gateway verwendet werden. Ein praktisches Beispiel ist die Abschottung einer besonders schutzwürdigen Organisationseinheit in einem Intranet, z. B. der Personal-Abteilung.

neuKap06.fm Seite 193 Freitag, 18. Oktober 2002 3:51 15

6.3.2 Packet Filter und dual-homed Application Gateway

In diesem Firewall-Konzept werden die aktiven Firewall-Elemente »Packet Filter« und »Application Gateway« hintereinander geschaltet.

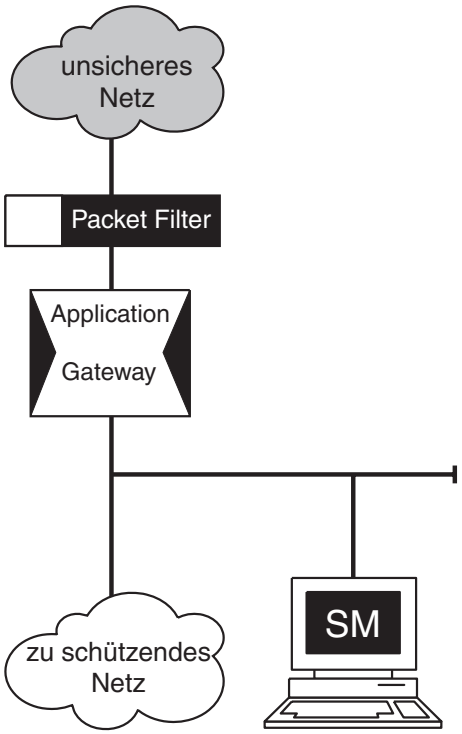


Abb. 6.7: Packet Filter und dual-homed Application Gateway 1

Beschreibung der Abbildung 6.7

Durch das Packet Filter wird das dual-homed Application Gateway aus dem unsicheren Netz geschützt. Logisch befindet sich das dual-homed Application Gateway bei diesem Firewall-Konzept im zu schützenden Netz.

neuKap06.fm Seite 194 Freitag, 18. Oktober 2002 3:51 15

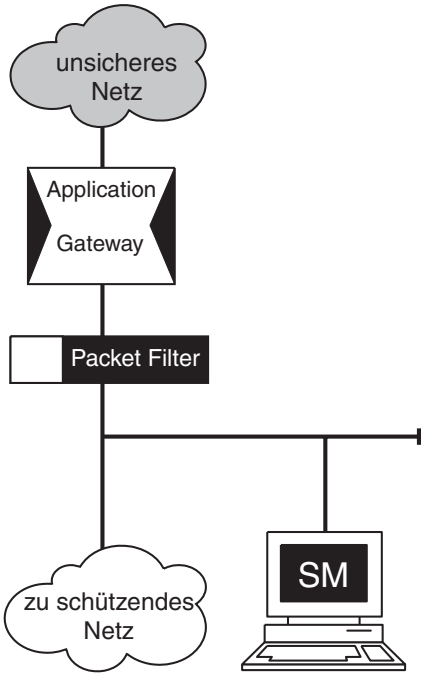


Abb. 6.8: Packet Filter und dual-homed Application Gateway 2

Beschreibung der Abbildung 6.8

Der Packet Filter schützt das dual-homed Application Gateway aus dem zu schützenden Netz. Logisch befindet sich das dual-homed Application Gateway bei diesem Firewall-Konzept im unsicheren Netz und muss daher Angriffen aus dem unsicheren Netz gegenüber besonders widerstandsfähig sein.

Bewertung des Firewall-Konzepts

Packet Filter und dual-homed Application Gateway kontrollieren die Kommunikation zwischen den Rechnern im zu schützenden Netz und den Rechnern aus dem unsicheren Netz. In diesem Konzept gibt es keine Möglichkeit, das dual-homed Application Gateway zu umgehen.

Das Maß an Sicherheit, das dieses Firewall-Konzept bietet, hängt von der Sicherheit des Packet Filter und der Sicherheit des dual-homed Application Gateway ab. Da beide aktive Firewall-Elemente mit unterschiedlichen Einbindungs- und Analysekonzepten arbeiten, werden mit dieser Kombination alle Sicherheitsziele erreicht und ein Höchstmaß an Gesamtsicherheit realisiert.

Die Kombination, die Abb. 6.7 zeigt, ist zu bevorzugen, weil hier das dual-homed Application Gateway durch das Packet Filter aus dem unsicheren Netz geschützt wird.

neuKap06.fm Seite 195 Freitag, 18. Oktober 2002 3:51 15

Einsatzfall

Falls das unsichere Netz ein geringes oder nicht einschätzbares Schutzniveau hat, das unsichere Netz außerhalb des eigenen Verantwortungsbereiches liegt und das zu schützende Netz kein besonders hohes Schutzniveau hat, kann eine Kombination von Packet Filter im unsicheren Netz und dual-homed Application Gateways im zu schützenden Netz verwendet werden.

Das Screened Subnet

Das Screened Subnet oder Grenznetz ist ein entkoppeltes, isoliertes Teilnetzwerk, das zwischen das zu schützende Netz und das unsichere Netz geschaltet wird. Im Screened Subnet wird mithilfe von zwei Packet Filtern für die Kontrolle der Verbindungen und Pakete gesorgt. Das Screened Subnet wird oft auch als DMZ (De-Militarised Zone) bezeichnet.

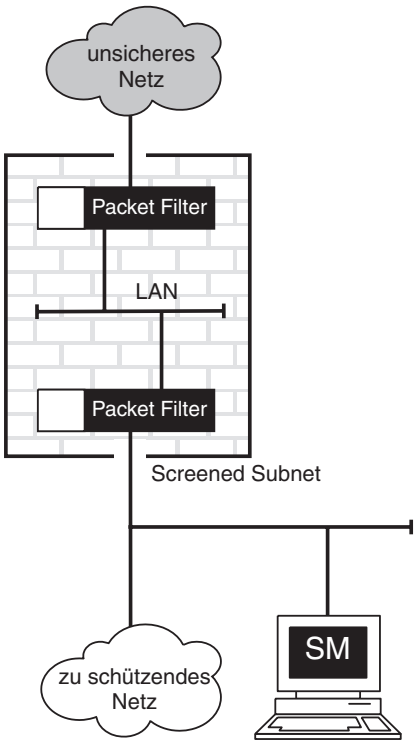


Abb. 6.9: Screened Subnet

Das äußere Packet Filter schützt das Screened Subnet und das dahinter liegende zu schützende Netz vor Angreifern aus dem unsicheren Netz und ist somit die erste Hürde, die aus dem unsicheren Netz überwunden werden muss. Das äußere

neuKap06.fm Seite 196 Freitag, 18. Oktober 2002 3:51 15

Packet Filter bestimmt außerdem, wer aus dem unsicheren Netz auf Rechnersysteme zugreifen darf, die im Screened Subnet positioniert sind.

Das innere Packet Filter ist die letzte Hürde zum zu schützenden Netz. Das innere Packet Filter bestimmt, wer aus dem zu schützenden Netz auf Rechnersysteme, die im Screened Subnet positioniert sind, zugreifen darf.

Durch die Einrichtung eines Screened Subnet werden alle Rechnersysteme, die im Screened Subnet positioniert werden, von beiden Seiten geschützt. Außerdem bietet es den Vorteil, dass die Filterregeln einfacher definiert werden können, weil sie aus der Sicht zum unsicheren und aus der Sicht zum zu schützenden Netz formuliert werden können.

6.3.3 Zwei Packet Filter als Screened Subnet und ein single-homed Application Gateway

In diesem Firewall-Konzept gewährleisten in erster Linie die beiden Packet Filter, die ein Screened Subnet bilden, die Sicherheit. Das single-homed Application Gateway stellt optional zusätzliche Sicherheitsleistungen zur Verfügung.

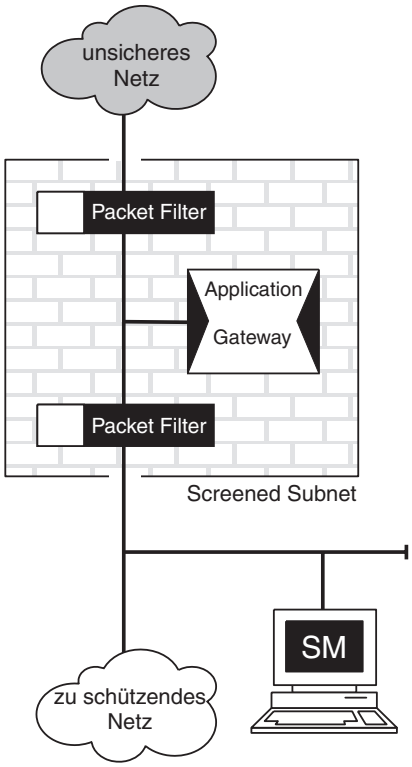


Abb. 6.10: Screened Subnet und ein single-homed Application Gateway

neuKap06.fm Seite 197 Freitag, 18. Oktober 2002 3:51 15

Die beiden Packet Filter können so eingerichtet werden, dass eine Kommunikation nur über das single-homed Application Gateway erlaubt ist, das in diesem Fall alle Sicherheitsdienste erbringt. Die Kommunikation zwischen den Rechnern im zu schützenden Netz und den Rechnern aus dem unsicheren Netz wird durch den Packet Filter kontrolliert über das Application Gateway abgewickelt. Das single-homed Application Gateway befindet sich bei diesem Firewall-Konzept im Screened Subnet und wird durch die beiden Packet Filter geschützt.

Bewertung des Firewall-Konzepts

Bei dieser Konstellation ist es für bestimmte Verbindungen möglich, die Kommunikation nur über die Packet Filter abzuwickeln, z. B. für solche Dienste, für die es auf dem single-homed Application Gateway keine Proxies gibt. Dadurch wird das Firewall-Konzept sehr flexibel. Einige Dienste sind dann nur über die Packet Filter und andere nur zusätzlich über den single-homed Application Gateway zugelassen.

Die Sicherheit, die dieses Firewall-Konzept bietet, hängt in erster Linie von der Sicherheit der Packet Filter ab. Aus diesem Grund müssen die Packet Filter in diesem Konzept besonders sicher sein (siehe Kapitel 5 *Elemente eines Firewall-Systems*). Da der Schutzbedarf der meisten zu schützenden Netze höher ist als der Schutz, den die Sicherheitsmechanismen eines Packet Filter bieten können, ist dieses Konzept für die Ankopplung eines zu schützenden Netzes an das Internet nicht ausreichend.

Einsatzfall

Eine Kombination von Packet Filtern als Screened Subnet und single-homed Application Gateway ist dann sinnvoll, wenn unsicheres und zu schützendes Netz eigene Verantwortungsbereiche bilden, aber das Schutzniveau des unsicheren Netzes gering oder schwer einschätzbar ist und das zu schützende Netz einen sehr hohen Schutzbedarf hat. In der Praxis ist ein solcher Fall gegeben, wenn eine besonders schutzwürdige Organisationseinheit im Intranet, z. B. der Vorstand einer Organisation, abgeschottet werden soll.

6.3.4 Zwei Packet Filter als Screened Subnet und ein dual-homed Application Gateway (High-level-Security-Firewall-System)

Ein High-level-Security-Firewall-System fasst mehrere aktive Firewall-Elemente zusammen, sodass ein *Höchstmaß an Sicherheit* garantiert werden kann.

Das High-level-Security-Firewall-System besteht aus einem Screened Subnet mit einem dual-homed Application Gateway und einem separaten Security Management. In diesem Firewall-System werden die aktiven Firewall-Elemente »Packet Filter« und »Application Gateway« hintereinander geschaltet.

neuKap06.fm Seite 198 Freitag, 18. Oktober 2002 3:51 15

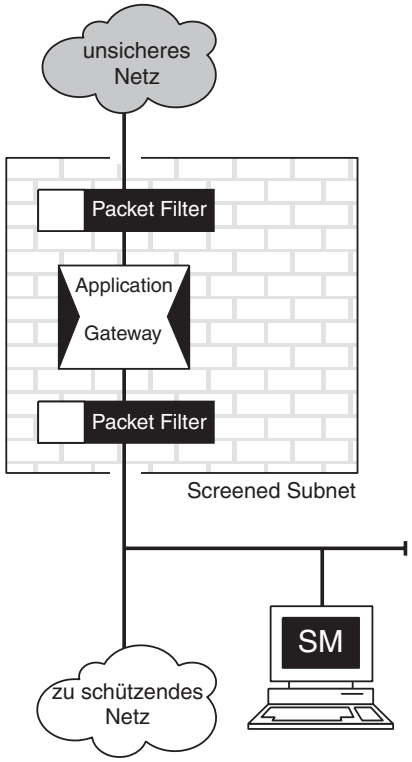


Abb. 6.11: High-level-Security-Firewall-System

Das dual-homed Application Gateway befindet sich bei diesem Firewall-Konzept im Screened Subnet. Durch die Packet Filter wird das dual-homed Application Gateway vor Angriffen aus dem unsicheren und dem zu schützenden Netz geschützt.

Bewertung des Firewall-Konzepts

Die Kommunikation zwischen Rechnersystemen im zu schützenden Netz und Rechnersystemen aus dem unsicheren Netz wird durch die Packet Filter und das dual-homed Application Gateway kontrolliert. Dieses Konzept lässt keine Möglichkeit zu, das dual-homed Application Gateway zu umgehen.

Das Maß an Sicherheit, das dieses Firewall-Konzept bietet, addiert sich aus der Sicherheitsleistung des Packet Filter und der Sicherheit des dual-homed Application Gateway, sodass eine besonders hohe Gesamtsicherheit erreicht wird.

Der Grundgedanke und die Zielsetzung eines High-leve-Security-Firewall-Systems lassen sich durch folgende Punkte beschreiben:

neuKap06.fm Seite 199 Freitag, 18. Oktober 2002 3:51 15

- *Einfache Regeln:* Die Anordnung der Elemente ermöglicht eine einfache Definition der Regeln für die einzelnen aktiven Firewall-Elemente. Aus der Sicht des Packet Filter kommuniziert immer nur der Application Gateway mit den Rechnersystemen des entsprechenden Netzes.
- *Gegenseitiger Schutz:* Die Packet Filter sorgen dafür, dass nicht jeder auf das dual-homed Application Gateway zugreifen darf, und schützen damit das dual-homed Application Gateway selbst.
- *Geschachtelte Sicherheit:* Wer auf ein zu schützendes Netz zugreifen will, das durch ein High-level-Security-Firewall-System abgeschottet wird, muss verschiedene Barrieren überwinden: zuerst ein Packet Filter, dann ein dual-homed Application Gateway und zum Schluss wieder ein Packet Filter.
- *Verschiedene Betriebssysteme:* Aus Sicherheitsgründen verwenden High-level-Security-Firewall-Lösungen für die verschiedenen aktiven Firewall-Elemente verschiedene Betriebssysteme: z. B. ein UNIX-Betriebssystem für das dual-homed Application Gateway und ein Real-Time-Betriebssystem für die Packet Filter (siehe *Sicherheitsanforderungen an Internet-Firewalls* im Anhang F). Eventuell auftretende Betriebssystemfehler oder Lücken wirken sich dadurch nur jeweils auf ein aktives Firewall-Element aus.
- *Unterschiedliche Einbindungs- und Analysemöglichkeiten*: Außerdem arbeiten die verschiedenen aktiven Firewall-Elemente mit unterschiedlichen Strategien (Sicherheitsansätzen). Die Packet Filter interpretieren die übertragenen Pakete von unten nach oben auf der Netzzugangs-, der Netzwerk- und der Transportebene. Das dual-homed Application Gateway interpretiert die Kommunikation auf der Anwendungsebene. Auch hier können sich mögliche Schwächen der Einbindungs- und Analysemöglichkeiten nur jeweils auf ein aktives Firewall-Element auswirken.
- *Separates Security Management:* Das separate Security Management stellt viele eigene Sicherheitsmechanismen wie Zugangskontrolle, Rechteverwaltung, Verschlüsselung und Protokollierung zur Verfügung und sorgt auf diese Weise ebenfalls für High-level Security.

Das Ganze ist mehr als die Summe der Einzelteile!

Alle diese Sicherheitsmechanismen zusammen garantieren ein höheres Maß an Sicherheit als jeder Sicherheitsmechanismus für sich alleine, so wie bei einem Auto der Sicherheitsgurt, der Airbag, der Seitenaufprallschutz und die Knautschzone zusammen ein Höchstmaß an Sicherheit bieten.

Einsatzfall

Der Einsatz eines High-level-Security-Firewall-Systems empfiehlt sich immer dann, wenn ein zu schützendes Netz an ein unsicheres Netz angekoppelt wird, das ein geringes oder nicht einschätzbares Schutzniveau hat und außerhalb des eigenen Verantwortungsbereiches liegt. Dies ist z. B. bei der Ankopplung an das Internet der Fall.

neuKap06.fm Seite 200 Freitag, 18. Oktober 2002 3:51 15

Im Folgenden wird für die Verwendung eines High-level-Security-Firewall-Systems ein vereinfachtes Symbol verwendet. Dieses Symbol steht für das Screened Subnet mit den zwei Packet Filtern und das dual-homed Application Gateway.

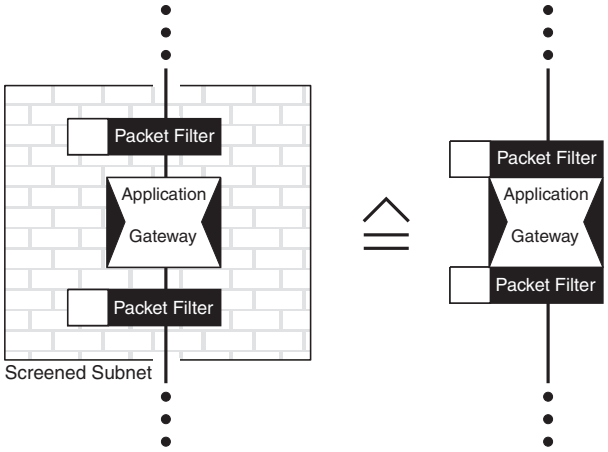


Abb. 6.12: Symbol eines High-level-Security-Firewall-Systems

6.4 Möglichkeiten eines High-level-Security-Firewall-Systems

Die Skalierbarkeit von Firewall-Systemen ist eine Anforderung an die zukünftige Entwicklung von Geschäftsprozessen über Kommunikationsnetze, deren Bedeutung nicht zu unterschätzen ist (siehe auch Kapitel 10 *Praktischer Einsatz von Firewall-Systemen*). Im Folgenden werden einige prinzipielle Möglichkeiten aufgezeigt, die mit einem High-level-Security-Firewall-System realisiert werden können.

Zur besseren Differenzierung wird der Bereich zwischen innerem Packet Filter und Application Gateway im Folgenden auch als internes Screened Subnet, der Bereich zwischen Application Gateway und äußerem Packet Filter als externes Screened Subnet bezeichnet.

6.4.1 Internet Server

Informationen, die öffentlich zugänglich sein sollen, können dem Internet auf einem (oder mehreren) Information Server(n) zur Verfügung gestellt werden. Dieser Internet Server befindet sich z. B. zwischen dem äußeren Packet Filter und dem Application Gateway im externen Screened Subnet. Diese Positionierung macht einen direkten Zugriff von außen über das ganze Firewall-System auf Rechnersysteme im zu schützenden Netz überflüssig. Dies ist eine organisatorische Sicherheitsmaßnahme.

neuKap06.fm Seite 201 Freitag, 18. Oktober 2002 3:51 15

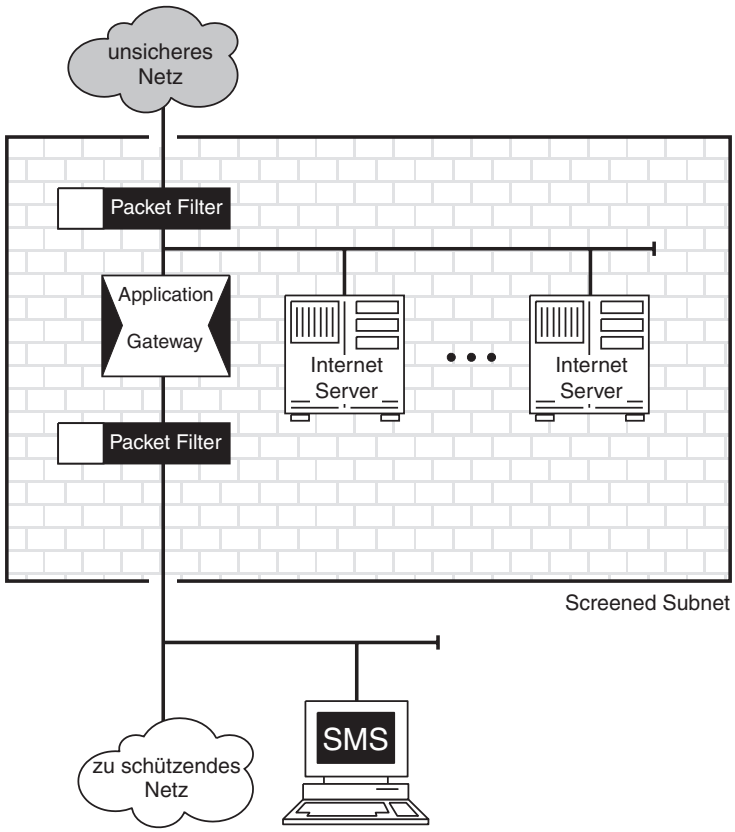


Abb. 6.13: Internet Server 1

Die Entkopplung der Netze bewirkt, dass keine direkte Verbindung mehr zwischen unsicherem Netz und zu schützendem Netz besteht. Daten aus dem unsicheren Netz werden nur bis zum Internet Server (oder zu den Internet Servern) transportiert, der sich vor dem Application Gateway befindet, gelangen jedoch nicht unkontrolliert durch ihn hindurch.

Für die Öffentlichkeit bestimmte Daten werden vom zu schützenden Netz auf den Internet Servern zur Abholung gespeichert. Alle Teilnehmer, die auf den Internet Server Zugriff haben, werden durch das äußere Packet Filter kontrolliert.

Falls es einem Angreifer gelänge, auf den Internet Server zuzugreifen und hier eigene Software aufzuspielen, mit deren Hilfe dann ein Angriff auf das Application Gateway durchgeführt werden könnte, hätte dieser Angreifer die erste Schranke schon überwunden, den ersten Packet Filter. Diese potenzielle Schwachstelle kann beseitigt werden, wenn folgende Hinweise beachtet werden:

neuKap06.fm Seite 202 Freitag, 18. Oktober 2002 3:51 15

- Der äußere Packet Filter muss so konfiguriert sein, dass nur Dienste erlaubt sind, die für seinen Betrieb notwendig sind. Für einen WWW-Server soll z. B. nur das HTTP-Protokoll (Port 80) freigeschaltet werden.
- Die Internet Server müssen so konfiguriert sein, dass es einem Angreifer von außen nicht möglich ist, auf die Betriebssystemebene des Internet Servers zuzugreifen und einen Angriff durchzuführen.

  Folgende Aspekte sind zu berücksichtigen:

  - richtige und sichere Konfigurierung der angebotenen Server-Software und des Betriebssystems
  - Restriktion der Einrichtungsrechte für Zugangskontrolle und Rechteverwaltung auf den Internet Servern nur für definierte Administratoren
  - minimale Software auf den Server-Systemen
  - auf den Server-Systemen soll nur lesender Zugriff erlaubt sein

Eigener Packet Filter für die Internet Server

Eine weitere Möglichkeiten der Integration von Internet Servern ist die, ein eigenes Packet Filter nur für die Internet Server zur Verfügung zu stellen, siehe Abbildung 6.14. Damit kann eine insgesamt höhere Sicherheit erreicht werden, weil diese unabhängig von den Rechnersystemen der Internet Server ist und eine klarere Trennung der Sicherheitsziele realisiert werden kann.

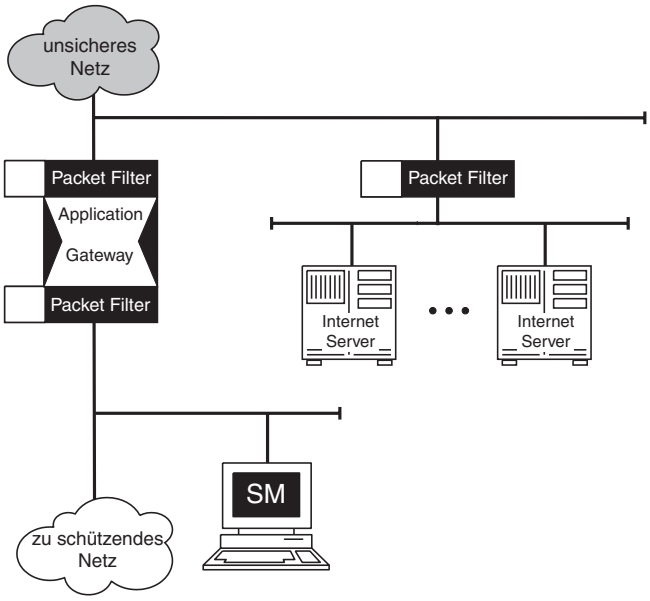


Abb. 6.14: Internet Server 2

neuKap06.fm Seite 203 Freitag, 18. Oktober 2002 3:51 15

Dritter Netzanschluss am Application-Gateway

Durch einen dritten Netzanschluss am Application Gateway ist eine weitere Möglichkeit gegeben, Internet Server einzubinden. Dieser dritte Netzanschluss wird auch für die Ankopplung von Anti-Virus-Systemen, Content-Filtering und speziellen URL-Filtern/Blockern verwendet.

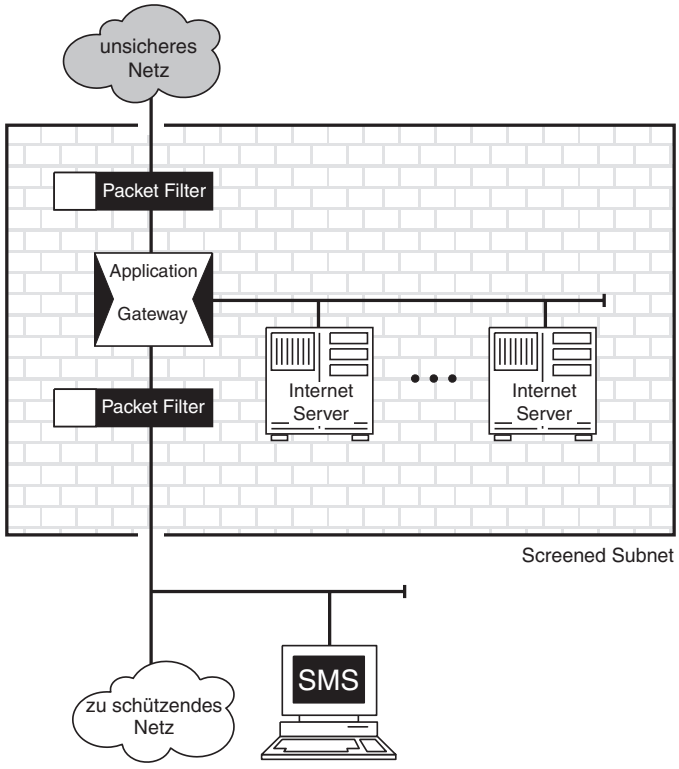


Abb. 6.15: Internet Server 3

6.4.2 Intranet Server

Informationen, die den Teilnehmern aus dem zu schützenden Netz zugänglich sein sollen, können dem Intranet auf einem (oder mehreren) Intranet Servern zur Verfügung gestellt werden. Dieser Intranet Server befindet sich zwischen dem inneren Packet Filter und dem Application Gateway im inneren Screened Subnet. Diese Positionierung macht einen Zugriff von innen auf das unsichere Netz überflüssig.

Die Entkopplung der Netze bewirkt, dass keine direkte Verbindung zwischen unsicherem Netz und zu schützendem Netz besteht. Daten aus dem zu schützenden Netz werden nur bis zum Intranet Server (oder zu den Intranet Servern) transportiert, der sich vor dem Application Gateway befindet.

neuKap06.fm Seite 204 Freitag, 18. Oktober 2002 3:51 15

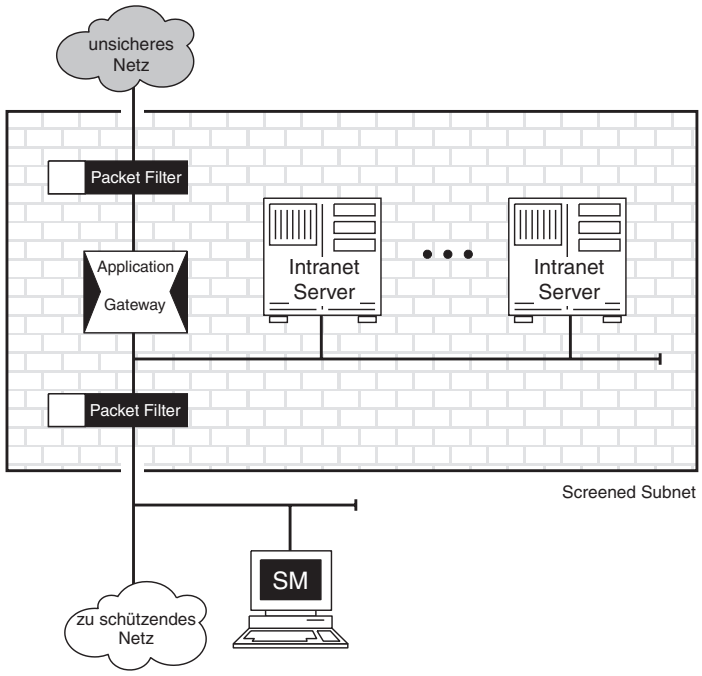


Abb. 6.16: Intranet Server

Daten, die für Teilnehmer aus dem zu schützenden Netz bestimmt sind, werden auf dem Intranet Server im inneren Screened Subnet zur Abholung gespeichert. Alle Teilnehmer, die auf den Intranet Server Zugriff haben, werden durch das innere Packet Filter kontrolliert. Es ist auch möglich, die Kommunikation der Rechnersysteme aus dem zu schützenden Netz zu den Intranet Servern zusätzlich über das Application Gateway zu realisieren. Das Application Gateway wird dann aus der Sicht des zu schützenden Netzes wie ein single-homed Application Gateway betrieben. Dadurch können Sicherheitsdienste wie Benutzerauthentikation und Protokollierung der Handlungen der Benutzer genutzt werden.

Weitere Einsatzmöglichkeiten von Intranet Servern sind im Kapitel 10 *Praktischer Einsatz von Firewall-Systemen* beschrieben.

6.4.3 Mehrere Application Gateways parallel

Es gibt Fälle, in denen es sinnvoll ist, im Screened Subnet mehrere Application Gateways parallel zu betreiben. Dies ist der Fall, wenn z. B. die Leistung gesteigert, eine Redundanz geschaffen oder eine Trennung zwischen bestimmten Diensten gehalten werden soll. Diese Möglichkeiten können verwendet werden, um zukünftig flexibel und sicher weiteren Anforderungen gerecht zu werden.

neuKap06.fm Seite 205 Freitag, 18. Oktober 2002 3:51 15

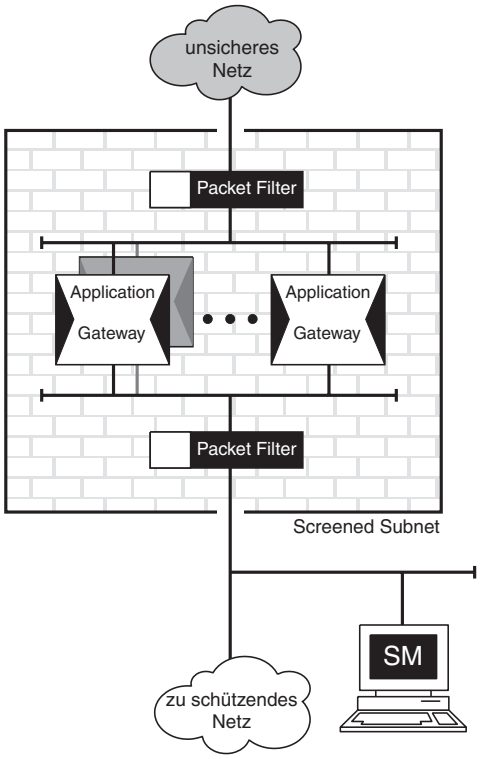


Abb. 6.17: Mehrere Application Gateways parallel

Trennung zwischen bestimmten Diensten

Ein Application Gateway kann für die Kommunikation verantwortlich sein, die zwischen unsicherem und zu schützendem Netz stattfindet, und ein weiteres Application Gateway für die umgekehrte Kommunikation zwischen zu schützendem und unsicherem Netz. Bei dieser Konstellation können unterschiedliche Betriebszeiten, verschiedene Sicherheitspolitik und unterschiedliche Verantwortliche für den Betrieb »klarer« definiert werden.

Leistung steigern

Der Einsatz mehrerer Application Gateways kann sinnvoll sein, um insgesamt eine höhere Leistungsfähigkeit (Durchsatz) zu erreichen. Dies könnte z. B. durch die Verteilung der Dienste auf verschiedene Application Gateways realisiert werden. Proxies für Dienste, die nach dem Store-and-Forward-Prinzip arbeiten und keine Benutzerauthentikation erfordern, wie SMTP- und NNTP-Proxy sowie Proxies für Dienste, die benutzerorientiert arbeiten, werden auf einem oder mehreren Application Gateways separat eingerichtet. Durch diese Methode kann die Leistungsfähigkeit eines Firewall-Systems einfach vergrößert werden.

neuKap06.fm Seite 206 Freitag, 18. Oktober 2002 3:51 15

Application Gateways können auch für verschiedene Gruppen oder Organisationseinheiten verwendet werden. Mit dieser Möglichkeit können Firewall-Systeme flexibel auf weitere Anforderungen reagieren.

Für einen größeren Durchsatz kann es auch sinnvoll sein, einen Dienst auf mehreren Application Gateways anzubieten. Hier ist es besonders wichtig, dass das Security Management auf beiden Application Gateways dieselbe Sicherheitspolitik realisiert, damit nicht auf einem Application Gateway erlaubt wird, was auf dem anderen verboten ist.

Unterschiedlichen Gruppen kann eine unterschiedliche Durchsatzgarantie geboten werden. Die eine Gruppe verwendet ein leistungsfähiges Application Gateway, das einen bestimmten Durchsatz garantieren kann, weil es nur von einer begrenzten Teilnehmerzahl genutzt wird. Alle anderen nutzen das andere Application Gateway, das seiner Gesamtbelastung gemäß keine Garantie für den Durchsatz geben kann.

Redundanz schaffen

Ein weiterer Grund, mehrere Application Gateways parallel bereitzustellen, ist die hohe Verfügbarkeit. Wenn die Application Gateways z. B. in Hot-Stand-By-Mode parallel arbeiten, können sie eine höhere Verfügbarkeit gewährleisten.

6.5 Das richtige Firewall-Konzept für jeden Einsatzfall

Es gibt sehr unterschiedliche Enscheidungskriterien, welches Firewall-Konzept wann für die Kopplung unterschiedlicher Netze eingesetzt werden soll. Die wichtigste Motivation ist immer die Tatsache, dass mithilfe eines Firewall-Konzepts die dem Schutzbedarf entsprechende notwendige Sicherheit erreicht werden soll.

Um eine einschätzbare Aussage über Firewall-Systeme treffen zu können, ist die Sicherheitseinstufung von Firewall-Konzepten sehr hilfreich. Dabei werden Einsatzfälle definiert, die nach den Kriterien Vertrauenswürdigkeit des Netzes und des Kommunikationspartners und Angriffspotenzial in Abhängigkeit des Einsatzfalles

1. das unsichere Netz ist innerhalb der eigenen Organisation oder
2. das unsichere Netz ist außerhalb der eigenen Organisation

betrachtet.

Die wichtigste Motivation für den Einsatz eines Firewall-Systems ist also die Reduzierung des Risikos der Verwundbarkeit, wenn ein Schutzbedarf der eigenen Werte besteht. Wenn das zu schützende Netz keinen Schutzbedarf hat, muss auch kein Firewall-System eingesetzt werden. Wenn aber ein Schutzbedarf vorliegt, dann muss der Einsatzfall entsprechend berücksichtigt werden und ein angemessenes Firewall-Konzept ist auszuwählen.

neuKap06.fm Seite 207 Freitag, 18. Oktober 2002 3:51 15

Im Folgenden wird eine Methode erläutert, wie dies in der Praxis mit den gewonnenen Erkenntnissen geschehen kann.

Definition des Einsatzfalls

Im Folgenden werden die beiden prinzipiellen Einsatzfälle von Firewall-Systemen definiert:

Kriterien	Einsatzfall: innerhalb der eigenen Organisation	Einsatzfall: außerhalb der eigenen Organisation
Vertrauenswürdigkeit des Netzes	**sehr hoch** – wird regelmäßig überprüft – liegt in der eigenen Verantwortung	**schwer bemessbar**, da von speziellen Faktoren abhängig – liegt nicht in der eigenen Verantwortung – es muss mit allen Risiken gerechnet werden
Vertrauenswürdigkeit des Kommunikationspartners	**sehr hoch** – die Kommunikationsteilnehmer gehören zur gleichen Organisation und arbeiten unter der gleichen Sicherheitspolitik – Vorsicht vor Innentätern ist dennoch geboten	Annahme: **sehr gering** – Kommunikationsteilnehmern von außerhalb kann prinzipiell keine Vertrauenswürdigkeit unterstellt werden.
Angriffspotenzial	**sehr gering** – die Kommunikationsteilnehmer gehören zur gleichen Organisation und arbeiten unter der gleichen Sicherheitspolitik – Vorsicht vor Innentätern ist dennoch geboten	**sehr hoch** – die Teilnehmer des Netzes haben einen sehr unterschiedlichen Schutzbedarf (Hacker und professionelle Angreifer) – z. B. aus dem Internet

Tabelle 6.1: Definition des Einsatzfalls

Bemerkung

Auch beim Einsatzfall innerhalb von Organisationen ist »blindes Vertrauen« in die Vertrauenswürdigkeit der Mitarbeiter falsch und würde trügerische Sicherheit bedeuten, wie die Fallbeispiele von Innentätern zeigen.

Die nächste Tabelle zeigt, wie in Abhängigkeit des Schutzbedarfes und des Einsatzfalls welches aktive Firewall-Element oder Kombination aktiver Firewall-Elemente verwendet werden soll. Die Definition des Schutzbedarfs ist an das Grundschutzhandbuch des BSI /BSI99/ angelehnt.

neuKap06.fm Seite 208 Freitag, 18. Oktober 2002 3:51 15

Entscheidungsmatrix für das Firewall-Konzept

Schutzbedarf	Risiken	Einsatzfall	Firewall-Konzept
niedrig	– geringfügiger Verstoß gegen Gesetze – beschränkte negative Außenwirkung – finanzieller Schaden < 12500 EUR	innerhalb der Organisation:	Packet Filter
		außerhalb der Organisation:	Dual homed Application Gateway
hoch	– erheblicher Verstoß gegen Gesetze – breite negative Außenwirkung – finanzieller Schaden < 2,5 Millionen EUR	innerhalb der Organisation:	Packet Filter + Single-homed Application Gateway *oder* Stateful Inspection *oder* Adaptive Proxy
		außerhalb der Organisation:	Packet Filter + Dual homed Application Gateway
sehr hoch	– fundamentaler Verstoß gegen Gesetze – existenzgefährdend negative Außenwirkung – finanzieller Schaden > 2,5 Millionen EUR	innerhalb der Organisation:	Screened Subnet mit Packet Filter + Single-homed Application Gateway
		außerhalb der Organisation:	Screened Subnet mit Packet Filter + Dual homed Application Gateway ⇒ High-Level-Firewall-System

Tabelle 6.2: Entscheidungsmatrix für das Firewall-Konzept

Falls überhaupt ein Schutzbedarf besteht, ist für die Kommunikation mit einem unsicheren Netz außerhalb des eigenen Verantwortungsbereiches immer ein dual-homed Application Gateway im Firewall-Konzept notwendig.

Dem Schutzbedarf entsprechend kann dann entweder ein dual-homed Application Gateway allein oder in Kombination mit einem Packet Filter bzw. einem Screened Subnet zum Einsatz kommen.

Falls das unsichere Netz innerhalb des eigenen Verantwortungsbereichs liegt, wie z. B. das Intranet, genügt es, abhängig vom Schutzbedarf, nur Packet Filter oder Kombinationen mit single-homed Application Gateways zu verwenden. Eine Alternative in diesem Anwendungsbereich sind Stateful Inspection oder Adaptive Proxy Lösungen, die auch auf der Anwendungsebene Sicherheitsfunktionen zur Verfügung stellen.

Durch die Kombination eines dual-homed Application Gateway mit Packet Filter oder Screened Subnet ist eine sehr hohe Sicherheit zu erreichen.

neuKap06.fm Seite 209 Freitag, 18. Oktober 2002 3:51 15

Stets muss der Leitsatz sein: »Das passende Firewall-Konzept für den jeweiligen speziellen Anwendungsfall«.

Neben der grundsätzlichen Stärke des Firewall-Konzepts, die den möglichen Einsatzfall bestimmt, spielen weitere sicherheitsrelevante Aspekte eine Rolle, z. B.

- die eigentlichen Sicherheitsdienste, die angeboten werden,
- die Tiefe der Analyse auf den unterschiedlichen Kommunikationsebenen,
- das Designkonzept der Firewall-Lösung,
- die Qualität der Realisierung,
- die Nachweisbarkeit der Sicherheit und
- die staatlichen Restriktionen der Firewall-Lösung.

Damit das Firewall-Konzept den Sicherheitserwartungen genügen kann, müssen alle aufgeführten Aspekte berücksichtigt werden. Außerdem sollen infrastrukturelle, organisatorische und personelle Sicherheitsmechanismen in Betracht gezogen werden, damit ein hohes Maß an Gesamtsicherheit erreicht werden kann (siehe dazu Kapitel 11 *Ein Firewall-System ist mehr als ein Produkt*).

Weiterhin muss berücksichtigt werden, dass mithilfe eines Firewall-Konzepts ein sicherer, kontrollierter Übergang zwischen zwei unterschiedlichen Netzen realisiert werden kann.

Mithilfe zusätzlicher Sicherheitsmechanismen wie z. B. Intrusion Detection können auch noch zusätzliche Informationen gewonnen werden, z. B. dass »intelligente« Angriffe auf das Firewall-System selbst realisiert werden (siehe dazu Kapitel 13.7 *Intrusion-Detection/Response-Systeme)*.

Mit der Einbindung von Anti-Viren-Konzepten können Content-Security-Probleme gelöst werden.

Es muss also in der Gesamtheit beachtet werden, ob weitere Mechanismen, die nicht direkt mit dem Firewall-System zusammenhängen, im Firewall-Gesamtkonzept berücksichtigt werden müssen.

6.6 Mail-Konzept

Bei der Integration eines High-level-Security-Firewall-Systems können verschiedene Mail-Konzepte realisiert werden. Hier soll ein Mail-Konzept diskutiert werden, bei dem sowohl im zu schützenden als auch im unsicheren Netz ein eigener Mail Server positioniert wird.

Wenn Mails zwischen Rechnersystemen im zu schützenden Netz ausgetauscht werden, können sie über den internen Mail Server weitergeleitet werden und verlassen das zu schützende Netz nicht. Mails an Rechnersysteme im unsicheren Netz werden über das Firewall-System kontrolliert an den externen Mail Server gesendet und von dort weitergeleitet.

neuKap06.fm Seite 210 Freitag, 18. Oktober 2002 3:51 15

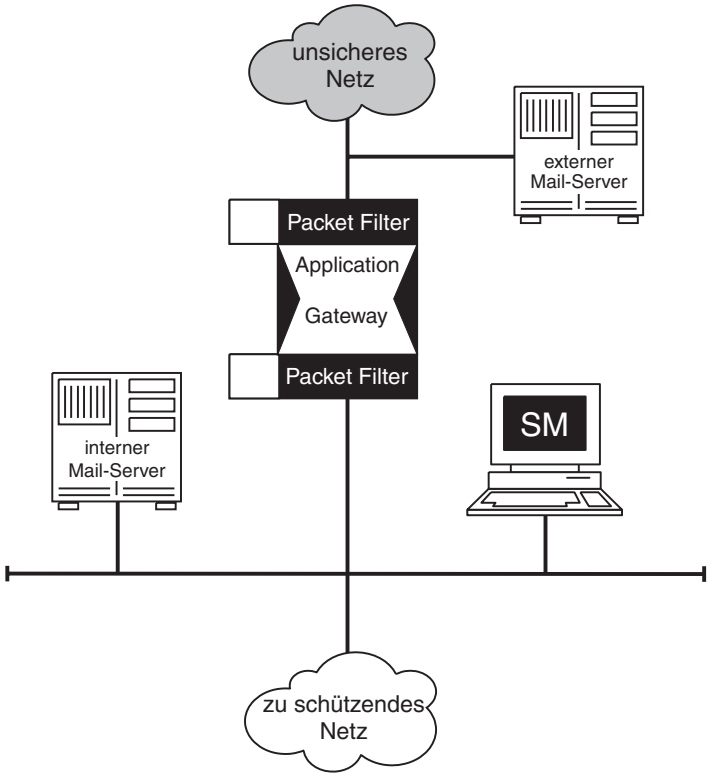


Abb. 6.18: Mail-Konzept

Mails aus dem unsicheren Netz in das zu schützende Netz werden vom Firewall-System kontrolliert empfangen und weitergeleitet (siehe Kapitel 5.3.2.2 *SMTP Proxy*).

Der Mail Server im unsicheren Netz wird von der eigenen Organisation betrieben. Vorteil hierbei ist, dass weitere Einschränkungen vorgenommen werden können:

- Im Packet Filter vor dem Application Gateway kann die MAC-Adresse des Mail Server überprüft werden, sodass sichergestellt ist, dass alle Mails diesen vorgeschalteten Mail Server passieren.
- Mails werden nur zu bestimmten Zeiten übertragen, wodurch für die Kommunikation von außen aus dem unsicheren Netz nach innen in das zu schützende Netz nur ein begrenzter Zeitraum zur Verfügung steht.

In vielen Firewall-Systemen ist die Mail-Anwendung die einzige Anwendung, bei der eine Verbindung vom unsicheren Netz in das zu schützende Netz aufgebaut wird. In allen anderen Fällen findet der Verbindungsaufbau nur umgekehrt statt.

neuKap06.fm Seite 211 Freitag, 18. Oktober 2002 3:51 15

Konfiguration im zu schützenden Netz

Ein Message Transfer Agent (MTA) hinter dem SMTP Proxy sorgt für die Verteilung der Mails im zu schützenden Netz. Dafür muss der MTA auf dem Application Gateway installiert sein. Falls die Rechnersysteme im zu schützenden Netz nicht verfügbar sind, wird die Mail als nicht vermittelbar verworfen.

Der SMTP Proxy sendet alle Mails zu einem Mail Server im zu schützenden Netz und dieser sorgt dann für die Verteilung. Da der Mail Server in der Regel immer verfügbar ist, werden alle Mails über das Firewall-System im zu schützenden Netz angenommen.

Welche der beiden Mail-Konzepte oder Kombinationen verwendet wird, hängt von der Größe des zu schützenden Netzes und den Möglichkeiten des Firewall-Systems ab.

Der Inhalt einer Mail kann durch Verschlüsselung und digitale Signatur gesichert werden (siehe dazu Kapitel 7 *Firewall-Systeme und Verschlüsselung*).

6.7 DNS-Konzepte

Der Domain Name Service (DNS) dient zur Umsetzung von Rechnernamen in IP-Adressen und umgekehrt und stellt ferner Informationen über im Netz vorhandene Rechnersysteme zur Verfügung. Bei der Integration des DNS Server in ein Firewall-System sollten einige Aspekte berücksichtigt werden. Aus dem unsicheren Netz dürfen nur minimale Informationen über das zu schützende Netz und dessen Rechnersysteme zur Verfügung gestellt werden, damit die interne Struktur verborgen bleibt.

Im unsicheren Netz und im zu schützenden Netz wird je ein DNS Server eingesetzt. Namen und IP-Adressen des zu schützenden Netzes sind nur dem DNS Server dieses Netzes bekannt.

Der DNS Server im unsicheren Netz darf die Struktur des zu schützenden Netzes nicht kennen. Für die Umsetzung eines DNS-Konzepts gibt es mehrere Möglichkeiten:

Das Application Gateway fragt immer den internen DNS Server

Alle DNS-bezüglichen Abfragen werden vom Application Gateway über einen internen DNS Server aufgelöst. Falls der interne DNS Server die Auflösung nicht durchführen kann, wird die Anfrage automatisch über das Application Gateway »transparent« an den externen DNS Server weitergeleitet. Das Ergebnis bekommt das Application Gateway vom internen DNS Server. Die Kommunikation zwischen den beiden DNS Servern läuft für die Proxies auf dem Application Gateway transparent.

neuKap06.fm Seite 212 Freitag, 18. Oktober 2002 3:51 15

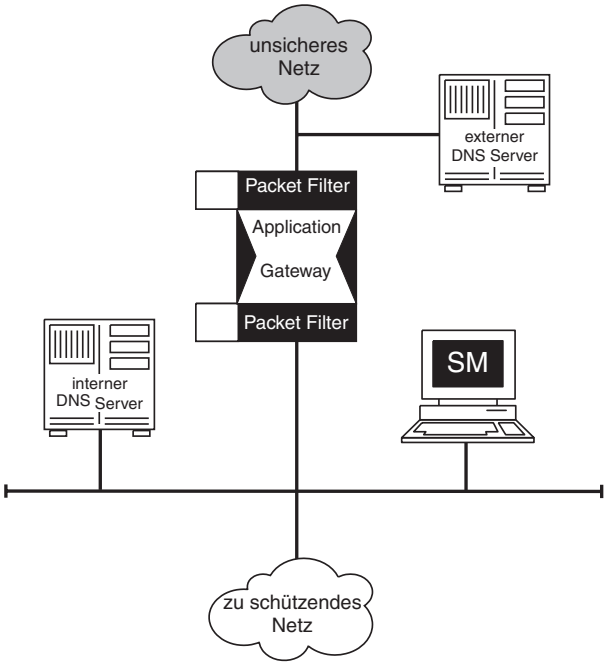


Abb. 6.19: DNS-Konzepte

Wegen des hohen Kommunikationsaufwandes, den dieses DNS-Konzept mit sich bringt, gibt es bei einigen DNS Realisierungen Probleme. Die eingesetzten Packet Filter werden so konfiguriert, dass zwischen den Servern nur der DNS-Dienst gestattet ist, d.h., DNS Port 53 ist Quell- und Zielport.

Splitted DNS

Beim splitted DNS Konzept hat das Application Gateway die Informationen darüber, welche Domänennamen und IP-Adressen im unsicheren und im zu schützenden Netz sind, und es kann entscheiden, in welche Richtung es die Auflösung vornimmt. Nachteil dieser Lösung ist, dass die externen IP-Adressen und Namen aus dem unsicheren Netz (z.B. dem Internet) aus dem zu schützenden Netz heraus nicht aufgelöst werden können.

Eigener DNS Server oder DNS Proxy

Eine dritte Lösungsmöglichkeit besteht darin, den DNS Server selbst im Application Gateway zu realisieren und die Auflösung der IP-Adressen und Namen aus dem internen Netz über das Application Gateway durchzuführen. Die Adressen aus dem unsicheren Netz (z.B. Internet) werden dann aus dem zu schützenden Netz heraus vom DNS Server auf dem Application Gateway aufgelöst. Für Transport-Proxy und Socks ist ein eigener DNS Server auf dem Application Gateway notwendig.

neuKap07.fm Seite 213 Freitag, 18. Oktober 2002 3:52 15

Kapitel 7

Firewall-Systeme und Verschlüsselung

Es gibt unterschiedliche Möglichkeiten, die Verschlüsselung von Daten bei der TCP/IP-Kommunikation durchzuführen.

Eine erste Möglichkeit ist die Integration von Sicherheitsfunktionen auf der Applikationsebene, z. B. in eine E-Mail-Anwendung.

Eine weitere Möglichkeit ist die direkte Integration von Sicherheitsfunktionen in den Kommunikationsstack, wie z. B. zwischen der Netzwerk- und Transportebene als Virtual Private Network (VPN) oder oberhalb der Transportschicht als Secure Socket Layer (SSL).

Beide Varianten der Verschlüsselung sind so konzipiert, dass die Firewall-Funktionalitäten weiterhin verwendet werden können. Die Verschlüsselung wird nicht nur für die Vertraulichkeit der Daten verwendet, sondern kann auch Restrisiken von Firewall-Systemen wie z. B. Trittbrettfahrer aktiv ausschalten. Somit kann durch das Zusammenwirken von Firewall-Systemen und Verschlüsselung eine hohe Gesamt-Sicherheit für die Kommunikation über öffentliche Netze gewährleistet werden (siehe auch *»Theoretische Grundlagen von Firewall-Systemen«* Kap. 14.5.12 und 14.6).

Ein wesentlicher Unterschied zwischen den Sicherheitskonzepten eines Firewall-Systems und Verschlüsselungskonzepten ist, dass ein Firewall-System unabhängig von anderen Sicherheitskomponenten betrachtet werden kann. Ein Firewall-System überwacht den Übergang zwischen zwei Netzen, ähnlich wie ein Pförtner.

Bei Verschlüsselungskonzepten muss immer eine Sicherheitskomponente auf der Gegenseite vorhanden sein, mit der kryptographisch kommuniziert wird. Damit bei der Verschlüsselung auf beiden Seiten der gleiche Schlüssel vorhanden ist, muss ein gemeinsames Schlüssel-Management organisiert werden. Die Organisation eines Schlüssel-Managements ist immer dann sehr einfach, wenn die Sicherheitskomponenten im selben Verantwortungsbereich liegen. Ist dies nicht der Fall, muss ein Schlüssel-Management realisiert werden, dem die unterschiedlichen Verantwortungsbereiche vertrauen. Die in diesem Kapitel beschriebenen Verfahren sind die VPN-Lösung, bei der das Security Management von einer Organisation gehandhabt werden kann, die SSL-Verschlüsselung, bei der das Security Management zentral von einem Trustcenter-Anbieter realisiert wird, und schließlich die

neuKap07.fm Seite 214 Freitag, 18. Oktober 2002 3:52 15

E-Mail-Verschlüsselung, mit deren Hilfe unterschiedliche Verantwortungsbereiche über eine Sicherheitsinfrastruktur kryptographisch kommunizieren können.

Zuerst werden Sicherheitsmechanismen beschrieben, mit denen Verschlüsselungskonzepte aufgebaut werden können.

7.1 Sicherheitsmechanismen für Verschlüsselung und Digitale Signatur

In diesem Kapitel werden Sicherheitsmechanismen beschrieben, mit denen Daten auf ihrem Weg über öffentliche Netze geschützt werden können. Sicherheitsmechanismen sind die Werkzeuge, mit denen die jeweils erforderlichen Sicherheitsdienste wie z.B. Verschlüsselung und Digitale Signatur realisiert werden können.

Die Vertraulichkeit von Daten kann nur gewährleistet sein, wenn die Daten verschlüsselt übertragen werden. Bei der Verschlüsselung unterscheiden wir verschiedene Verfahren (siehe auch /Rula94/).

7.1.1 Private-Key-Verfahren

Verschlüsselungsverfahren, die für die Verschlüsselung von Daten den gleichen Schlüssel verwenden wie für ihre Entschlüsselung, werden als symmetrische oder Private-Key-Verfahren bezeichnet.

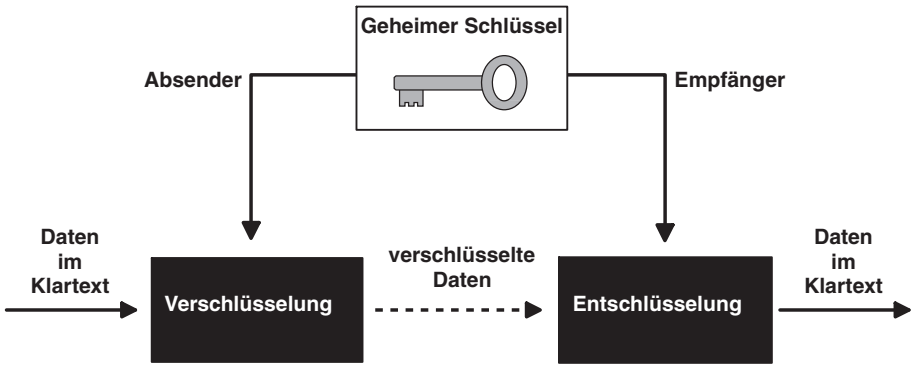


Abb. 7.1: Symmetrisches Verschlüsselungsverfahren

Eines der bekanntesten, am weitesten verbreiteten und meistuntersuchten symmetrischen Verschlüsselungsverfahren ist der DES-Algorithmus, der 1978 in den USA normiert wurde (ANSI X3.92). DES steht für »Data Encryption Standard«.

neuKap07.fm Seite 215 Freitag, 18. Oktober 2002 3:52 15

Der DES-Algorithmus wird heute meist als Triple-DES mit 128 Bit effektiver Schlüssellänge verwendet, wobei der Algorithmus dreimal durchlaufen wird, und zwar entweder mit zwei (A-B-A) oder drei (A-B-C) verschiedenen Schlüsseln.

Bei dreimaligem Durchlauf mit je 56 Bit Schlüssellänge entspricht die Sicherheit des Verfahrens jedoch nicht etwa der einer einmaligen Verschlüsselung mit der Schlüssellänge von 3 * 56 Bit = 168 Bit, sondern ist geringer. Die Kryptologen haben deshalb den Begriff »effektive Schlüssellänge« eingeführt.

Zukünftig wird der neue AES (Advanced Encryption Standard) verwendet, der mit einer Schlüssellänge von 256 Bit arbeitet. Weitere symmetrische Verschlüsselungsverfahren sind z. B. IDEA und Safer.

Der *Nachteil von symmetrischen Verschlüsselungsverfahren* wie Triple-DES ist, dass beide Kommunikationspartner über den gleichen Schlüssel verfügen müssen. Der Schlüssel, von dessen Geheimhaltung die Sicherheit abhängt, muss von einem Kommunikationspartner an den anderen übermittelt werden. Dieser Unsicherheitsfaktor muss durch eine sichere Methode zur Schlüsselverteilung minimiert werden. Im Extremfall kann dies z. B. die persönliche Übermittlung durch einen Kurier sein. Das Risiko besteht darin, dass die Schlüssel, von deren Geheimhaltung die Sicherheit des Verfahrens abhängt, durch Nachlässigkeit, Vorsatz oder Zufall in falsche Hände geraten können.

Der *Vorteil von Private-Key-Verfahren* wie dem DES ist, dass sie sehr schnell sind. Es gibt Hardware-Lösungen, die bis zu 1 GBit/s und Software-Lösungen, die bis zu mehreren MBit/s verschlüsseln.

7.1.2 Public-Key-Verfahren

Um die Schlüsselverteilung, das klassische Problem der Kryptographie, zu vereinfachen, wurden Verfahren entwickelt, die mit so genannten »öffentlichen Schlüsseln« (public-keys) arbeiten. Ein Public-Key-Verfahren oder asymmetrisches Verfahren arbeitet mit zwei verschiedenen Teilschlüsseln. Wird eine Verschlüsselung mit einem der beiden Teilschlüssel durchgeführt, kann nur mit dem entsprechenden passenden Teilschlüssel die korrekte Entschlüsselung erfolgen.

Aus der Kenntnis des einen Teilschlüssels kann der andere nicht berechnet werden. Aus diesem Grund kann ein Teilschlüssel ohne Bedenken veröffentlicht werden. Dieser heißt »öffentlicher Schlüssel«. Der andere Schlüssel muss geheimgehalten werden und heißt dementsprechend »geheimer Schlüssel« /Pohl90/.

neuKap07.fm Seite 216 Freitag, 18. Oktober 2002 3:52 15

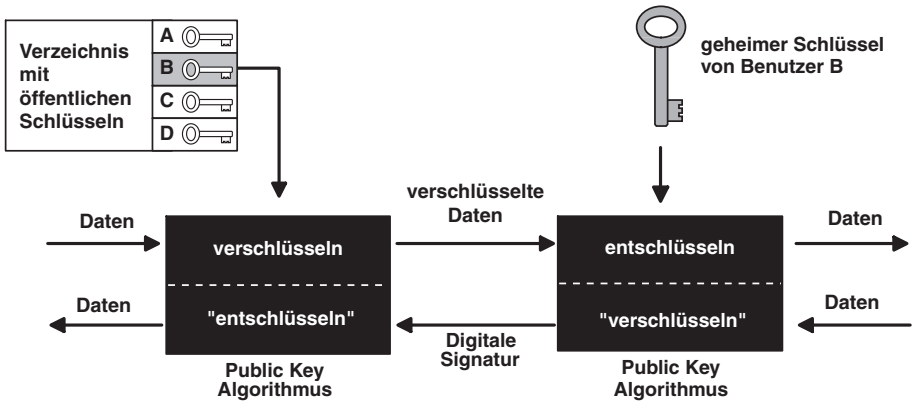


Abb. 7.2: Asymmetrisches Verschlüsselungsverfahren

Digitale Signatur

Eine wichtige Anwendung des Public-Key-Verfahrens ist die Digitale Signatur.

Daten, die mit einem bestimmten geheimen Schlüssel verschlüsselt wurden, können nur mithilfe des dazugehörigen öffentlichen Schlüssels wieder entschlüsselt werden (siehe Abb. 7.2). Hat nun eine Person die Daten mit ihrem geheimen Schlüssel digital signiert, kann mithilfe des öffentlichen Schlüssels überprüft werden, ob es wirklich diese Person war, die die Daten digital signiert hat. Die erfolgreich durchgeführte Überprüfung ist der Beweis für die Authentizität der Signatur. Mit dem Prinzip der Digitalen Signatur steht somit ein Äquivalent zur handgeschriebenen Unterschrift zur Verfügung.

Das bekannteste Public-Key-Verfahren ist das RSA-Verfahren, mit dem gleichzeitig signiert und verschlüsselt werden kann.

Vertraulichkeit von Sicherheitsinformationen

Wird eine Information zuerst mit dem öffentlichen Schlüssel einer bestimmten Person verschlüsselt, kann diese Information nur von der Person, die den dazugehörigen geheimen Schlüssel besitzt, rekonstruiert werden. Diese Anwendung erlaubt den vertraulichen Austausch von sicherheitsrelevanten Informationen – z. B. von Schlüsseln für symmetrische Verfahren wie DES.

Vorteile asymmetrischer Verfahren:

Mithilfe von Public-Key-Verfahren sind ein einfaches Key-Management (Schlüsselverteilung) und die Digitale Signatur möglich.

neuKap07.fm Seite 217 Freitag, 18. Oktober 2002 3:52 15

Nachteile asymmetrischer Verfahren:

Public-Key-Verfahren entstammen der Komplexitätstheorie. Sie sind daher sehr rechenintensiv und nicht für die Verschlüsselung von großen Datenmengen geeignet.

7.1.3 One-Way-Hashfunktion

Die Digitale Signatur entspricht einer Operation mit dem Public-Key-Verfahren und ist daher sehr rechenintensiv. Um den Aufwand zu vermindern, signiert man nicht die gesamte Information mit dem Public-Key-Verfahren, sondern erstellt eine Prüfsumme als »Konzentrat« der Nachricht, das digital signiert wird.

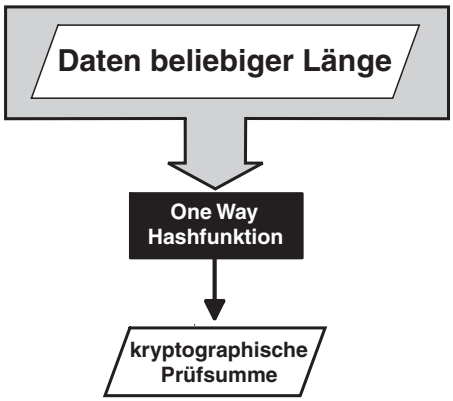


Abb. 7.3: One-Way-Hashfunktion

Auf eine Nachricht, deren Länge variabel ist, wird eine so genannte One-Way-Hashfunktion angewendet, die eine kryptographische Prüfsumme fester Länge als Ergebnis erzeugt. Zu den besonderen Eigenschaften von One-Way-Hashfunktionen gehört, dass die Berechnung des Funktionswertes einfach ist, während es aber praktisch unmöglich ist, systematisch einen Wert zu finden, der dieselbe kryptographische Prüfsumme ergibt. Eine kryptographische Prüfsumme muss eine Vielzahl von weiteren Eigenschaften aufweisen, die in ISO 10118 sowie in der Fachliteratur beschrieben sind. Verfahren in der Praxis sind u.a. die One-Way-Hashfunktionen RIPEMD, SHA-1.

7.1.4 Hybride Verschlüsselungstechnik

Da Public-Key-Verfahren wegen ihrer Komplexität zur Verschlüsselung von großen Datenmengen nicht geeignet sind und bei symmetrischen Verfahren die Schlüsselverteilung zu aufwendig ist, erweist sich eine Kombination von beiden als ideale Lösung: Die eigentliche Verschlüsselung der Daten eines Dokuments wird mit einem symmetrischen Verfahren (z.B. mit dem Triple-DES-Verfahren) durchge-

neuKap07.fm Seite 218 Freitag, 18. Oktober 2002 3:52 15

führt, und der Schlüssel wird für seine Verteilung mit dem Public-Key-Verfahren verschlüsselt. Eine Kombination des symmetrischen mit dem asymmetrischen Verschlüsselungsverfahren bietet neben der höchstmöglichen Sicherheit die Vorzüge der praktischen Handhabung.

7.1.5 Ein Wettlauf um die Sicherheit

Für die Sicherheit einer Verschlüsselung sind vier Faktoren ausschlaggebend:

- der verwendete Algorithmus
- die Schlüsselgenerierung
- die Schlüssellänge
- die Aufbewahrung des Schlüssels

Bei symmetrischen Verschlüsselungsverfahren geht man heute davon aus, dass die Praxissicherheit gegeben ist, wenn man eine Schlüssellänge von 128 Bit und mehr verwendet.

Eine vollständige Suche zur Entschlüsselung (»Brute Force Attack«) hieße, 2^{128} Schlüssel auszuprobieren. Damit stößt man auf ein praktisches Problem, denn mit den derzeitigen Ressourcen ist die Berechnung nicht in einer angemessenen Zeit möglich. Da aber die Geschwindigkeit von Computern, die man für diesen Angriff nutzen kann, immer weiter steigt, müssen in der Folge auch die Schlüssellängen von Zeit zu Zeit entsprechend vergrößert werden. Galt vor 10 Jahren noch eine praktische Sicherheit bei einer Schlüssellänge von 64 Bit als gegeben, so sind heute 128 Bit und in naher Zukunft 256 Bit erforderlich.

Gleiches gilt auch für Public-Key-Verfahren. In der Vergangenheit galt eine Schlüssellänge von 512 Bit als »sicher«, heute sind es 1024 Bit. Um langfristig Sicherheit zu gewährleisten, wird man zur Verendung von 2048-Bit-Schlüsseln übergehen müssen.

Trotz aller Bemühungen gibt es keine absolute Sicherheit, da die Sicherheit anwendbarer Algorithmus mathematisch nicht bewiesen werden kann. Ein Algorithmus gilt dann als »sicher«, wenn fünf Jahren nach seiner Veröffentlichung die Mathematiker der Welt nicht in der Lage sind, ihn erfolgreich mathematisch anzugreifen. Nicht publizierte »geheime« Algorithmen gelten – weil nicht durch Experten überprüfbar – als »unsicher«.

7.1.6 Zertifikations-Systeme

Ein offenes Problem bei Public-Key-Verfahren ist die Frage, wie der öffentliche Schlüssel zum Kommunikationspartner gelangt. Selbst im Fall der Verwendung öffentlicher Schlüssel müssen diese authentisch ausgetauscht werden. Eine elegante Möglichkeit, öffentliche Schlüssel authentisch auszutauschen, ist die Einrichtung eines Zertifikations-Systems, eines Trustcenters oder einer Public-Key-Infrastruktur.

neuKap07.fm Seite 219 Freitag, 18. Oktober 2002 3:52 15

Der öffentliche Schlüssel jedes Benutzers wird dem Zertifikationssystem in Form eines »digitalen Zertifikats« von der vertrauenswürdigen dritten Instanz – der Zertifizierungs-Instanz – zur Verfügung gestellt. Dieses Sicherheitsprinzip ist im Directory-Authentication Framework /CCITT/ beschrieben.

Betrachten wir die Authentikation von Personen mit Hilfe von Ausweisen (Personalausweis, Reisepass usw.): Hier fungieren unsere Behörden (Einwohnermeldeämter) als vertrauenswürdige dritte Instanz. Nachdem sich eine Person bei uns vorgestellt hat, können wir mithilfe eines Ausweises die Echtheit dieser Aussage verifizieren. Genau diese Funktionalität müssen wir zur Verfügung stellen, um komplexe Sicherheitssysteme elektronisch zu realisieren.

Eine PKI stellt in aller Regel zentrale Sicherheitsdienste zur Verfügung, schafft also die Voraussetzungen dafür, dass eine Anwendung vertrauenswürdig realisiert werden kann.

Das folgende Bild zeigt im oberen Teil den prinzipiellen Aufbau einer Public-Key-Infrastruktur sowie einige Kommunikationskanäle. Im unteren Bereich ist schematisch eine Anwendung abgebildet, die auf der PKI-Grundfunktionalität basiert.

Aufgaben und Komponenten einer PKI

Public-Key-Infrastrukturen bestehen aus Hardware, Software und einem abgestimmten Regelwerk, der Policy. /Pohl 2002b/

Die Policy definiert, nach welchen Sicherheitsregeln die Dienstleistungen erbracht werden. Dazu zählt das Betriebskonzept der PKI, die Benutzerrichtlinien sowie Organisations- und Arbeitsanweisungen.

Im Allgemeinen ist es üblich, die Registrierung der Teilnehmer und die Zertifizierung der Schlüssel voneinander zu trennen und zum Teil auch an unterschiedlichen Orten vorzunehmen.

Die **Registration Authority (RA)** kann als private (innerhalb einer Organisation) oder öffentliche Einrichtung betrieben werden. Ihre Hauptaufgabe besteht darin, die Anträge auf Zertifizierung zu erfassen und die Identität der Antragsteller entsprechend der Policy zu prüfen. Die Identitätsprüfung kann sehr einfach, z. B. per E-Mail, oder auch aufwendiger und sicherer, z. B. durch persönliches Erscheinen und Vorlage des Ausweises, erfolgen.

Die Registration Authority bildet die Schnittstelle zwischen den Teilnehmern bzw. Antragstellern und der **Certification Authority (CA)**, an die sie die Anträge weiterleitet.

neuKap07.fm Seite 220 Freitag, 18. Oktober 2002 3:52 15

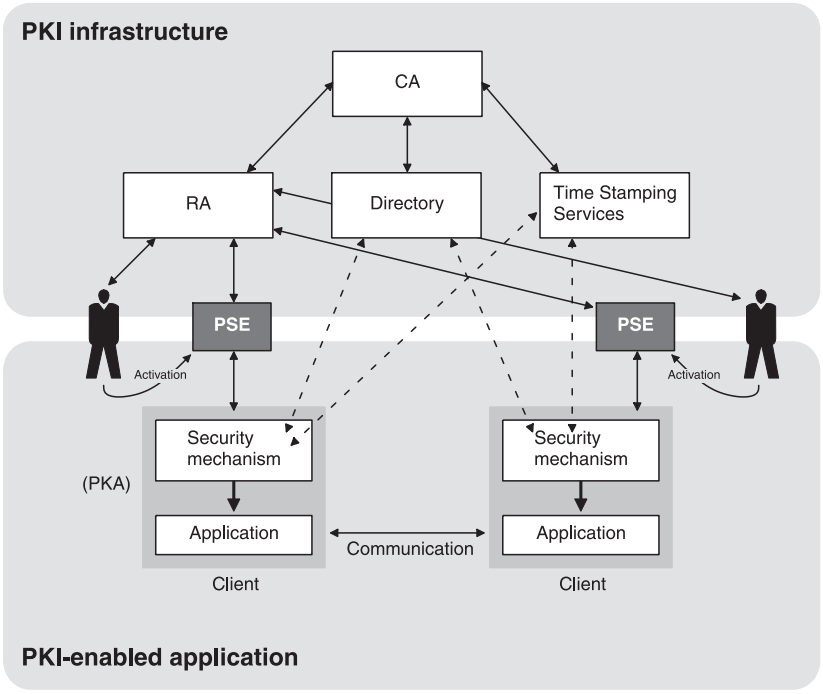


Abb. 7.4: PKI und PKA

Die **Certification Authority** vergibt eindeutige Identitäten und verwaltet für jeden Teilnehmer ein oder mehrere Schlüsselpaare mit den dazugehörigen Zertifikaten. Jedes von der CA erzeugte Zertifikat verbindet den öffentlichen Schlüssel des Teilnehmers mit dessen Namen und zusätzlichen Daten (Gültigkeitszeitraum, Seriennummer, evtl. weitere Attribute).

Die Certification Authority gibt die Zertifikate aus und verwaltet sie, damit die öffentlichen Schlüssel und Attribute (Position im Unternehmen, Rechte usw.) der Teilnehmer möglichst einfach verifiziert werden können.

Zur Verwaltung der Zertifikate unterhält jede PKI einen **Directory Service**. Hier werden die gültigen zertifizierten öffentlichen Schlüssel der Teilnehmer veröffentlicht. Zurückgezogene oder kompromittierte Schlüssel werden in einer Sperrliste (**»Certificate Revocation List«**, **CRL**) zum Abruf bereitgehalten.

Ein **Zeitstempeldienst** dient dazu, gesicherte Zeitsignaturen gemäß der Policy zu erstellen. Damit wird ein Dokument oder eine Transaktion mit der aktuellen Zeitangabe verknüpft und diese Gesamtinformation anschließend digital signiert.

Das **Personal Security Environment (PSE)** ist die Sammlung aller sicherheitsrelevanten Daten eines Teilnehmers. Dazu gehören seine geheimen Schlüssel, die Zertifikate seiner Kommunikationspartner sowie der öffentliche Schlüssel der Zertifizierungsinstanz.

neuKap07.fm Seite 221 Freitag, 18. Oktober 2002 3:52 15

PKI-enabled Application

Als »PKI-enabled Application« (PKA) wird eine Anwendung bezeichnet, die auf der Grundlage der von der PKI zur Verfügung gestellten Sicherheitsdienste (Zertifikate, Verzeichnisdienst etc.) eine vertrauenswürdige Nutzung ermöglicht. Eine PKA enthält selbst unterschiedliche Sicherheitsmechanismen oder -verfahren (Authentisierung, Verschlüsselung etc.), mit denen Vertrauenswürdigkeit (Authentizität, Integrität, Verbindlichkeit, Einmaligkeit und Vertraulichkeit) erzielt wird.

Eine PKI bildet die Sicherheitsgrundlage für die vertrauenswürdige Nutzung von Anwendungen wie

- E-Mail
- Dokumentverschlüsselung (z. B. von MS-Office-Dokumenten)
- Transaktionen im Finanzbereich (EDIFACT)
- XML-Prozessen
- SSL-Kommunikation
- VPN-Kommunikation
- Identifikations- und Authentisierungsprozessen
- Zahlungssystemen

Modelle von Public-Key-Infrastrukturen

Es gibt prinzipiell verschiedene Modelle von Public-Key-Infrastrukturen, die im Folgenden kurz dargestellt werden:

- **Geschlossene Systeme**
  Eine Organisation betreibt eine PKI für eine oder mehrere Anwendungen (PKAs), die in ihrem eigenen Verantwortungsbereich liegen. Sicherheitsdienste wie z. B. gesicherte Kommunikation oder Authentisierung stehen nur innerhalb der Infrastruktur zur Verfügung.

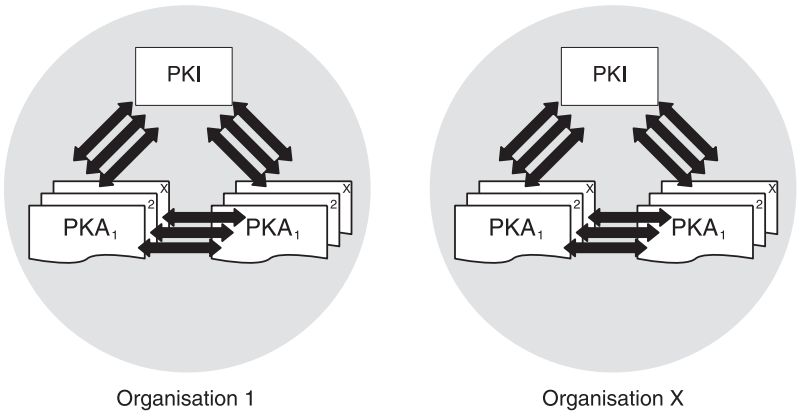


Abb. 7.5: Geschlossene PKI-Systeme

neuKap07.fm Seite 222 Freitag, 18. Oktober 2002 3:52 15

- **Offene Systeme**
  Mehrere Organisationen betreiben PKIs für eine oder mehrere Anwendungen, die in den Verantwortungsbereichen der unterschiedlichen Organisationen liegen. So ist z. B. die gesicherte Kommunikation zwischen den Organisationen möglich. Der Austausch beruht auf gegenseitigem Vertrauen sowie auf kompatiblen Technologien und Verfahren.

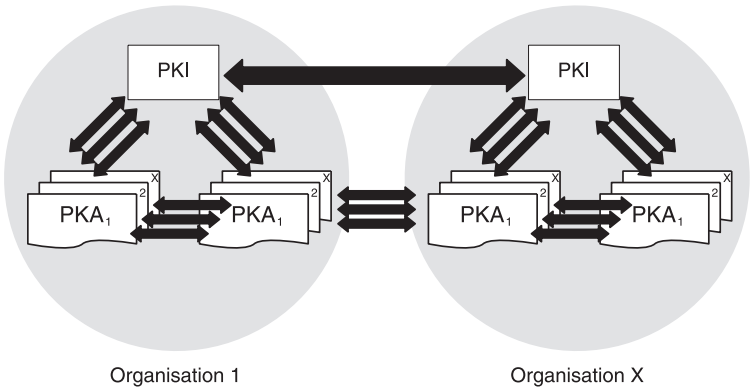


Abb. 7.6: Offene PKI-Systeme

- **Zentral administrierte Systeme**
  Ein PKI-Anbieter betreibt die PKI für eine oder mehrere Anwendungen, die in den Verantwortungsbereichen der sie nutzenden Organisationen liegen. Wenn die verschiedenen Organisationen der zentralen PKI vertrauen und kompatible Technologien und Verfahren verwendet werden, kann eine vertrauenswürdige Kommunikation realisiert werden.

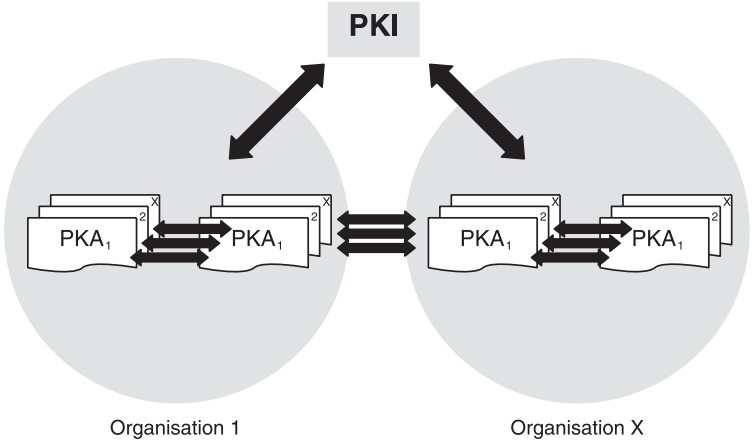


Abb. 7.7: Zentral administriertes PKI-System

neuKap07.fm Seite 223 Freitag, 18. Oktober 2002 3:52 15

Probleme mit PKIs in der Praxis

Bei der Nutzung von PKIs gab und gibt es einige Probleme, die im Folgenden diskutiert werden.

- Probleme bei geschlossenen Systemen
  »Geschlossenes System« bedeutet, dass die PKI nur innerhalb einer Organisation verwendet wird und nicht für die Kommunikation nach außen genutzt werden kann. Da jedoch in der Praxis viele organisationsübergreifende Prozesse stattfinden, ist der Nutzen einer solchen PKI sehr eingeschränkt.

- Probleme bei offenen Systemen
  Bei offenen Systemen muss zum Aufbau einer organisationsübergreifenden Kommunikation ein Abgleich der verschiedenen organisationsspezifischen Policies erfolgen. Ziel ist ein gemeinsames »Level of Trust«. Hier müssen geeignete Instrumente implementiert werden, um die organisatorischen sowie die IT-infrastrukturellen Konzeptionen zu bewerten, zu analysieren und zu gewichten.

  Gerade bei der Nutzung für personenbezogene organisationsübergreifende Prozesse stellt sich aus ökonomischer Sicht und aus den tatsächlichen Anforderungen heraus die Frage, ob das Signaturgesetz zwingend die Grundlage für die PKI und die zum Einsatz kommenden PKAs bilden muss. Hierbei muss berücksichtigt werden, dass viele organisationsübergreifende Prozesse automatisiert sind und somit nicht mehr personenbezogen arbeiten. Die Kardinalfrage in diesem Zusammenhang ist, ob innerhalb des Sicherheitskonzepts der PKI beispielsweise die Verantwortlichkeit für von Servern erstellte Signaturen geregelt ist (Haftungsausschluss).

  Hinzu kommt, dass eine Vielzahl von unterschiedlichen, teilweise sehr komplexen Standards existiert, die darüber hinaus der ständigen Weiterentwicklung unterliegen. Die Ursache hierfür liegt in der großen Vielfalt der Anwendungen (SSL, E-Mail etc.) und den daraus resultierenden besonderen Anforderungen.

- Unterschiedliche Verantwortung für PKIs und PKAs in Unternehmen
  Ein weiteres Problem, dem insbesondere große Organisationen gegenüberstehen, beruht darauf, dass die PKAs und PKIs zwar voneinander abhängig sind, aber häufig organisatorisch getrennt werden. In derartigen Fällen müssen sich beispielsweise verschiedene Abteilungen auf gemeinsame Ziele und Vorgehensweisen verständigen, um die entsprechenden technologischen Grundlagen zu erarbeiten.

- »Henne-Ei-Problem«
  Public-Key-Infrastrukturen sind nur dann ökonomisch sinnvoll, wenn der Einsatz dieser Strukturen und damit der vertrauenswürdige Ablauf von Geschäftsprozessen so umfassend wie möglich realisiert wird, d.h., wenn die gesicherte

neuKap07.fm Seite 224 Freitag, 18. Oktober 2002 3:52 15

Kommunikation mit so vielen Partnern wie möglich stattfinden kann. Voraussetzung dafür ist der konsequente Einsatz der bestehenden Technologien und die Umsetzung der Security Policies.

Die Realität ist aber, dass sich die beteiligten Organisationen nur schwer auf den Abgleich ihrer individuellen Sicherheitskonzepte einigen können. Dadurch gestaltet sich der Aufbau eines gemeinsamen »Level of Trust« langwierig und längst fällige Entscheidungen werden nicht getroffen. Zu viele Beteiligte nehmen noch eine abwartende Haltung ein und der Ausbau der bestehenden PKI-Infrastrukturen stagniert.

- Hoher personeller und organisatorischer Aufwand
  Die Einführung und der Betrieb einer Public-Key-Infrastruktur erfordert neben der technischen Umsetzung auch einen hohen personellen und organisatorischen Aufwand. Gerade in der Einführungsphase einer PKI ist die Sensibilisierung der Anwender für die IT-Sicherheit, die Schulung der Anwender auf die Produkte und die Planung und Durchführung des Roll-Outs ein nicht zu vernachlässigender Faktor.
- Key-Recovery bei der Verschlüsselung
  Falls Unternehmenswerte verschlüsselt werden, muss ein Verfahren realisiert werden, das bei technischen Defekten, bei einem PSE-Verlust oder beim Ausscheiden eines Mitarbeiters aus dem Unternehmen garantiert, dass die Unternehmenswerte sicher wieder entschlüsselt werden können.

Erstellung und Verifizierung von Zertifikaten

Der öffentliche Schlüssel eines jeden Benutzers wird dem System in Form eines Zertifikats zur Verfügung gestellt. Dieses enthält die Kennung der Zertifizierungsinstanz, die das Zertifikat erstellt hat, die Kennung des Benutzers, für den das Zertifikat erstellt wurde, den öffentlichen Schlüssel des Benutzers und eine Angabe zur Gültigkeitsdauer des Zertifikats (siehe Abb. 7.8).

Das Zertifikat ist von der Zertifizierungsinstanz, die es erstellt hat, digital signiert.

Jeder, der den öffentlichen Schlüssel der Zertifizierungsinstanz besitzt, ist damit in der Lage, zu überprüfen, ob der öffentliche Schlüssel eines Benutzers wirklich von der Zertifizierungsinstanz stammt.

neuKap07.fm Seite 225 Freitag, 18. Oktober 2002 3:52 15

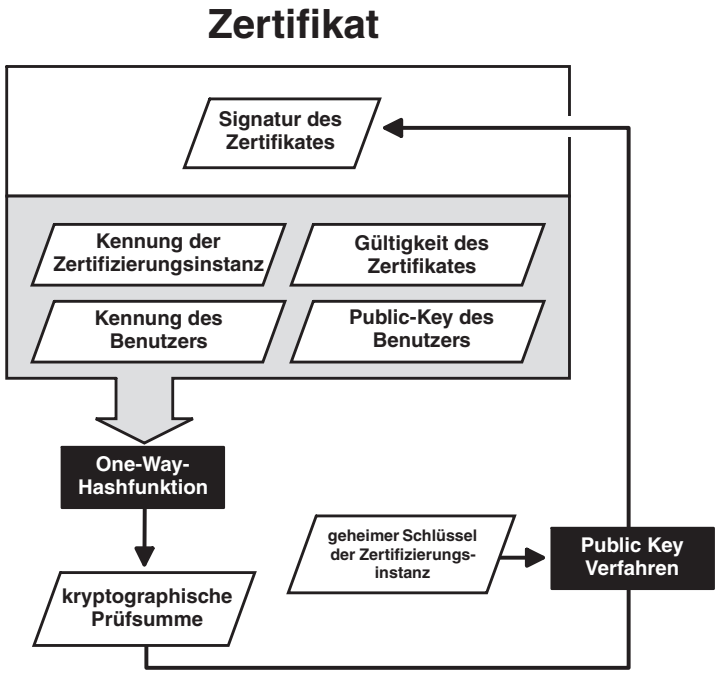


Abb. 7.8: Inhalt und Erstellung eines Zertifikats

Mit anderen Worten: Die Zertifizierungsinstanz veröffentlicht Zertifikate mit öffentlichen Schlüsseln, die die Zugehörigkeit von Benutzern und öffentlichem Schlüssel bestätigen.

Nach dem Erhalt eines Zertifikats wird vom Sicherheitssystem die aktuelle kryptographische Prüfsumme über den Inhalt des Zertifikat berechnet. Außerdem wird aus der Signatur des Zertifikats und dem öffentlichen Schlüssel der Zertifizierungsinstanz unter Verwendung des Public-Key-Verfahrens die ursprüngliche kryptographische Prüfsumme berechnet. Stimmen die beiden Prüfsummen überein, sind die Unversehrtheit und die Echtheit des öffentlichen Schlüssels des Benutzers, mit dem man eine Kommunikation durchführen möchte, bewiesen (siehe Abb. 7.9).

Voraussetzung ist, dass alle Benutzer des Sicherheitssystems der Zertifizierungsinstanz vertrauen können. Dazu muss die Zertifizierungsinstanz bestimmten Sicherheitsanforderungen genügen. Im Gesetz zur Digitalen Signatur werden die Sicherheitsanforderungen beschrieben, die eine Zertifizierungsinstanz erfüllen muss, die rechtlich anerkannte Zertifikate ausgeben möchte. Dazu zählen unter anderem vertrauenswürdiges Personal, zertifizierte Sicherheitskomponenten und eine vertrauenswürdige Systemumgebung. In einem globalen Sicherheitssystem können parallel oder hierarchisch verteilte Zertifizierungsinstanzen zusammengefasst sein.

neuKap07.fm Seite 226 Freitag, 18. Oktober 2002 3:52 15

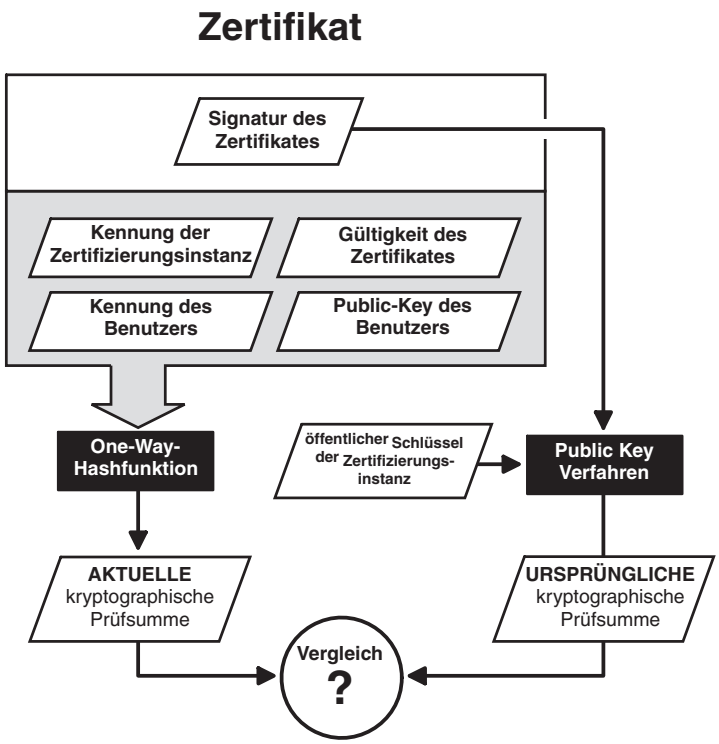


Abb. 7.9: Verifikation eines Zertifikats

Das hierarchische Schlüsselverteilverfahren ist die Grundlage für den Aufbau eines komplexen Sicherheitssystems.

7.1.7 Chipkarte (SmartCard)

Eine »intelligente Chipkarte« (»SmartCard«) ist ein Rechnersystem in der genormten Größe der EC-Karte (86 x 54 x 0,76 mm), das dem Benutzer Sicherheitsdienstleistungen zur Verfügung stellt.

Eine SmartCard enthält:

- eine CPU
- RAM- und ROM-Speicher
- ein »schlankes« Betriebssystem im ROM
- eine I/O-Schnittstelle, über die die gesamte Kommunikation stattfindet (Kontaktflächen oder kontaktloses Interface)
- ein EEPROM, auf dem die geheimen Schlüssel, z. B. ein privater RSA-Schlüssel oder andere symmetrische Schlüssel, sowie persönliche Daten (Passworte etc.) sicher gespeichert sind

neuKap07.fm Seite 227 Freitag, 18. Oktober 2002 3:52 15

- Sonstiges, beispielsweise einen Co-Prozessor, der symmetrische oder asymmetrische Verschlüsselung sehr schnell durchführt (Krypto-Prozessor)

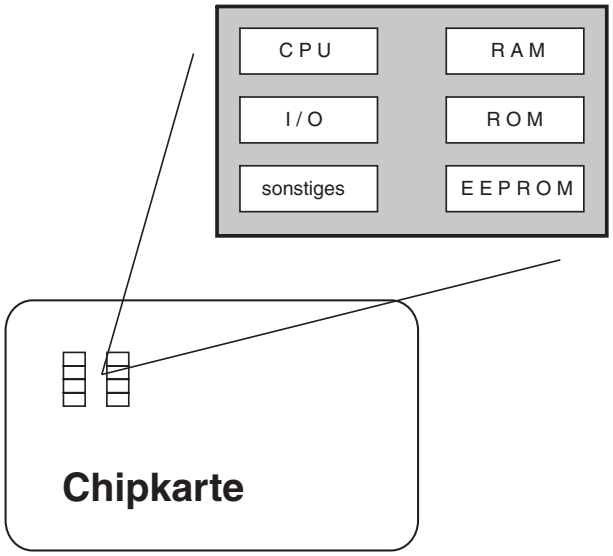


Abb. 7.10: Chipkarte

Eine SmartCard stellt dem Benutzer in der Regel folgende Sicherheitsdienstleistungen zur Verfügung:

- Laden und Entladen von Werteinheiten für elektronisches Bezahlen (auch ohne Krypto-Prozessor)
- Kryptographische Anwendungen wie Digitale Signaturen usw.
- Identifikation/Authentikation des Benutzers (Aktivieren der Chipkarte)
- Single Sign On-Anwendungen (z. B. Passwort und PIN für unterschiedliche Anwendungen)
- Sicheres Speichern von Daten auf der Chipkarte
- Lesen gespeicherter Servicedaten
- Ausführen sonstiger Rechenoperationen

In Anwendungen wie dem Sicherheitssystem zum Schutz von elektronischen Dokumenten werden der öffentliche Schlüssel der Zertifizierungsinstanz und der geheime Schlüsselteil des Benutzers gesichert in eine »intelligente Chipkarte« geladen. Die Chipkarte wird dann dem Benutzer vertrauenswürdig übergeben.

Aktivierung der Chipkarte

Die Chipkarte kann z. B. durch ein Passwort geschützt werden. Wenn ein Benutzer die Sicherheitsfunktionen in Anspruch nehmen will, muss er seine Chipkarte mit-

neuKap07.fm Seite 228 Freitag, 18. Oktober 2002 3:52 15

hilfe seines persönlichen Passworts aktivieren. Verliert der Benutzer seine Chipkarte, kann ein Finder diese nicht verwenden, da er das Passwort nicht kennt. Kennt jemand das individuelle Passwort eines anderen Benutzers, kann er keinen Nutzen daraus ziehen, sofern er nicht auch die Chipkarte besitzt. Außerdem kann ein Benutzer sein Passwort jederzeit ändern.

Sicherer als ein Passwort sind biometrische Identifikationsverfahren, die Körpermerkmale – z. B. einen Fingerabdruck, die Stimme oder Gesichtszüge – zur eindeutigen Identifikation von Personen nutzen. Im Gegensatz zu einem Passwort kann ein solches Merkmal nicht gestohlen, verloren, vergessen oder weitergegeben werden.

Im englischsprachigen Bereich verwendet man häufig die Schlagworte »What you know« (Passwort), »What you have« (Chipkarte) und »What you are« (Biometrik) und fordert, bei einer Authentikation mindestens zwei dieser drei Verfahren zu kombinieren.

Multifunktionalität

Die Chipkarte ist so konzipiert, dass mit ihr mehrere Anwendungen möglich sind. Je nach Anwendung werden kontaktlose Chipkarten (z. B. für Zutrittssysteme) oder Chipkarten mit Kontakten verwendet.

Möglich ist z. B. das Bezahlen an öffentlichen Telefonen oder an Point-of-Sales-Systemen (POS-Systemen), die Digitale Signatur von Dokumenten oder die Zugangskontrolle zu Gebäuden.

Mögliche Sicherheitsmechanismen einer SmartCard

SmartCard Hardware:

- Unter- und Überspannungsdetektion
- Erkennung niedriger Frequenzen
- gescramblete Busse
- Sensoren für Licht, Temperatur usw.
- Passivierungs- bzw. Metallisierungsschichten über Bus- und Speicherstrukturen oder über der gesamten CPU
- Zufallszahlengenerator in der Hardware
- spezielle CPU-Befehle für kryptographische Funktionen
- Speicherschutzfunktionen

SmartCard Software (z. B. Betriebssystem nach ISO 7816-4):

- Zugriffskontrolle auf Objekte
- Zustandsautomaten, die in Abhängigkeit von Identifikations- und Authentikationsmechanismen Befehle zulassen

neuKap07.fm Seite 229 Freitag, 18. Oktober 2002 3:52 15

Vorteile von SmartCards:

- Die kryptographischen Operationen werden ausschließlich auf der SmartCard ausgeführt. Der geheime Schlüssel verlässt die Karte niemals und kann nicht ausgelesen werden.
- SmartCards sind so klein wie Kredit- oder ec-Karten und können leicht überallhin mitgenommen werden.
- SmartCards sind flexibel für verschiedene Anwendungen einsetzbar.
- SmartCards sind mit Stückpreisen von ca. 1,50 EUR bis 18,- EUR (je nach Stückzahl und Aufdruck) bedeutend preisgünstiger als andere Sicherheitsmodule.

Einsatzumfeld einer SmartCard

SmartCards werden typischerweise als Sicherheitskomponenten für Personen eingesetzt.

7.2 E-Mail Security

Der Austausch von E-Mails ist die am häufigsten genutzte Anwendung im Internet. Dabei werden in E-Mails und Attachments Informationen übermittelt, die hohe Werte darstellen können, wie z.B. Vertragsentwürfe, in denen es durchaus um Millionen- oder gar Milliardenbeträge gehen kann.

In diesem Kapitel wird beschrieben, wie diese Informationswerte angemessen geschützt werden können, indem auf Benutzerebene für eine vertrauenswürdige E-Mail-Kommunikation gesorgt wird.

Ein Vergleich zwischen dem schriftlichen Austausch von Informationen, wie er noch vor kurzer Zeit üblich war, und der heutigen elektronischen Verarbeitung zeigt, welche Sicherheitsmechanismen gebraucht werden. Noch vor kurzem wurden Informationen wie Bestellungen, Rechnungen oder Entwicklungsdaten in schriftlicher Form auf dem Medium Papier ausgetauscht.

Eine Information wurde entweder auf einer Schreibmaschine getippt oder mithilfe eines Textverarbeitungssystems eingegeben und anschließend ausgedruckt. Der Ausdruck wurde unterschrieben, in einen Briefumschlag gesteckt und vertraulich an den gewünschten Empfänger gesendet. Der Empfänger erkannte an der Unversehrtheit des Umschlags, dass die Information vertraulich übermittelt worden war. Nach dem Öffnen des Briefes konnte der Empfänger an der handgeschriebenen Unterschrift die Echtheit des Absenders oder des Autors überprüfen. Die handgeschriebene Unterschrift ist zudem rechtsgültig.

Heute werden Informationen zunehmend elektronisch verarbeitet. Briefe, Dokumente und Überweisungen existieren nicht mehr in Papierform, sondern werden elektronisch verarbeitet und versendet.

neuKap07.fm Seite 230 Freitag, 18. Oktober 2002 3:52 15

Abb. 7.11: Brief und Unterschrift

Welche einem unversehrten verschlossenem Umschlag und einer handgeschriebenen Unterschrift vergleichbaren Sicherheiten hat der Empfänger einer elektronischen Nachricht? Wer garantiert ihm, dass die empfangene Nachricht authentisch ist?

7.2.1 »Briefumschlag« und »Unterschrift« für die elektronische Post

Ein Beispiel soll die Arbeitsweise eines Sicherheitssystems zum Schutz von elektronischen Dokumenten erläutern. Damit das vorgestellte Sicherheitssystem funktioniert, wird das normale Kommunikationssystem um eine Zertifizierungsinstanz erweitert, die für die Benutzer personalisierte Chipkarten ausgibt und das System mit Zertifikaten ausstattet.

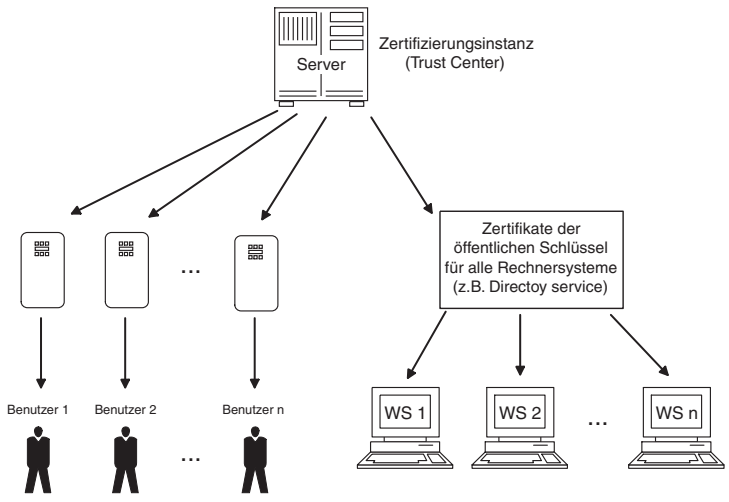


Abb. 7.12: Die Zertifizierungsinstanz gibt für die Benutzer personalisierte Chipkarten und Zertifikate aus

neuKap07.fm Seite 231 Freitag, 18. Oktober 2002 3:52 15

Signatur eines Dokuments

Ein Benutzer erstellt mit einem Editor (Textverarbeitungssystem, Browser, Mail-Programm, ...) eine elektronische Information, die er vertrauenswürdig versenden will. Anschließend ruft er die Signatur-Funktion auf. Als Erstes muss er mithilfe seines Passworts die Chipkarte, auf der der geheime RSA-Schlüssel gespeichert ist, aktivieren. Die Signatur-Funktion berechnet mithilfe der One-Way-Hashfunktion aus dem vom Benutzer angegebenen Dokument eine kryptographische Prüfsumme.

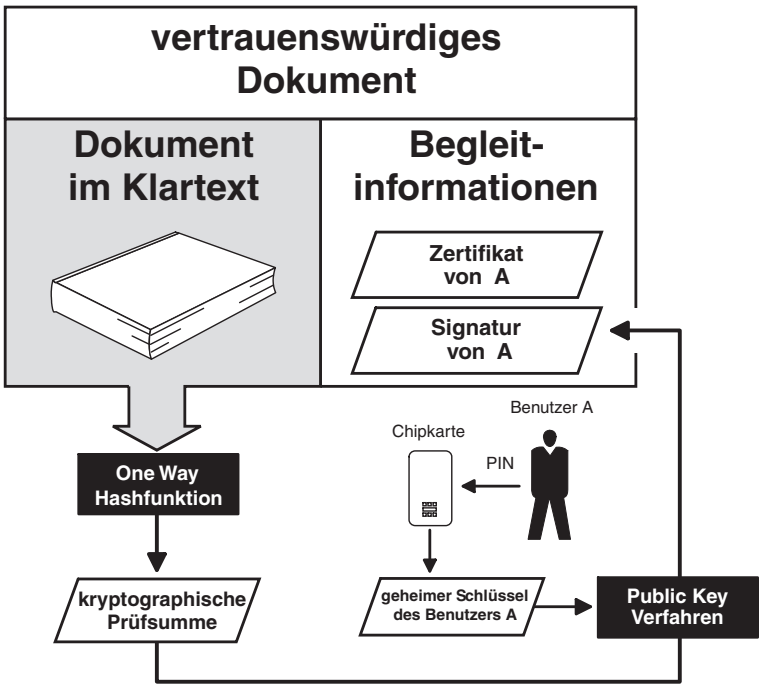


Abb. 7.13: Die Signatur-Funktion

Diese kryptographische Prüfsumme wird mit dem Public-Key-Verfahren unter Verwendung des auf der Chipkarte des Benutzers gespeicherten geheimen Schlüssels digital signiert. Als Ergebnis erhält man eine Signatur, die dem Dokument als Begleitinformation hinzugefügt wird. Außerdem schreibt die Signatur-Funktion das Zertifikat des Benutzers in die Begleitinformationen.

Wenn ein Dokument (wie im täglichen Büroleben) von mehreren Benutzern unterschrieben werden muss, kann auch eine Signatur von mehreren Benutzern generiert werden. Alle Signaturen eines Dokuments stehen in der Begleitinformation des entsprechenden Dokuments.

neuKap07.fm Seite 232 Freitag, 18. Oktober 2002 3:52 15

Digitaler Zeitstempel

Die Beweiskraft eines elektronischen Dokuments hängt häufig vom Zeitpunkt seiner Erstellung ab. Da man bei handelsüblichen Computern und Betriebssystemen die Uhrzeit problemlos verstellen kann, sind diese Zeitangaben nicht vertrauenswürdig. Ein Zeitstempel benötigt eine digitale Bescheinigung einer Zertifizierungsstelle. Diese bestätigt, dass ihr das Dokument zum angegebenen Zeitpunkt vorgelegen hat, indem sie den Zeitstempel digital signiert.

Verschlüsselung eines Dokuments

Nachdem eine oder mehrere Benutzer das Dokument signiert haben, kann es mithilfe der Verschlüsselungs-Funktion für die Übertragung verschlüsselt werden.

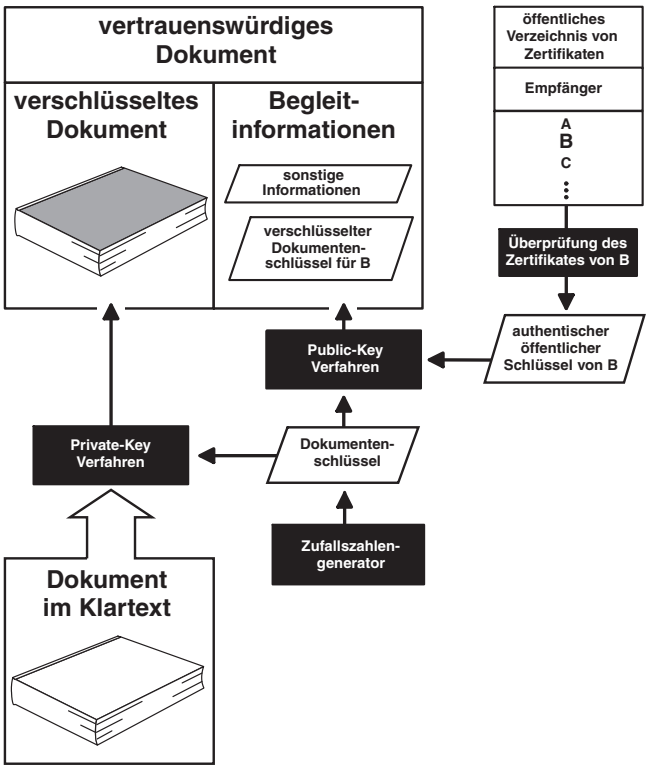


Abb. 7.14: Verschlüsselung des Dokuments

Dazu wird vom Sicherheitssystem als Dokumentenschlüssel eine Zufallszahl berechnet. Das Dokument wird dann unter Verwendung des Dokumentenschlüssels mit dem Private-Key-Verfahren (z. B. Triple-DES) verschlüsselt. Der Dokumentenschlüssel wird unter Verwendung des öffentlichen Schlüssels des Empfängers

neuKap07.fm Seite 233 Freitag, 18. Oktober 2002 3:52 15

mit dem Public-Key-Verfahren verschlüsselt und der Begleitinformation hinzugefügt. Der Dokumentenschlüssel kann mithilfe des Sicherheitssystems für mehrere Empfänger verschlüsselt werden, es stehen dann aber mehrere verschlüsselte Dokumentenschlüssel für die Empfänger in den Begleitinformationen. Das vertrauenswürdige Dokument wird nun an den/die Empfänger gesendet.

Prüfung der Vertrauenswürdigkeit des Dokuments und seine Entschlüsselung

Nachdem das Dokument beim Empfänger eingetroffen ist, kann dieser mithilfe der Begleitinformation erkennen, ob und von wem das Dokument digital signiert worden ist. Außerdem ist erkennbar, ob das Dokument verschlüsselt wurde und wer in der Lage ist, es zu entschlüsseln.

Mithilfe der Entschlüsselungs-Funktion kann das Dokument entschlüsselt und anschließend im Klartext gelesen werden (Abb. 7.15).

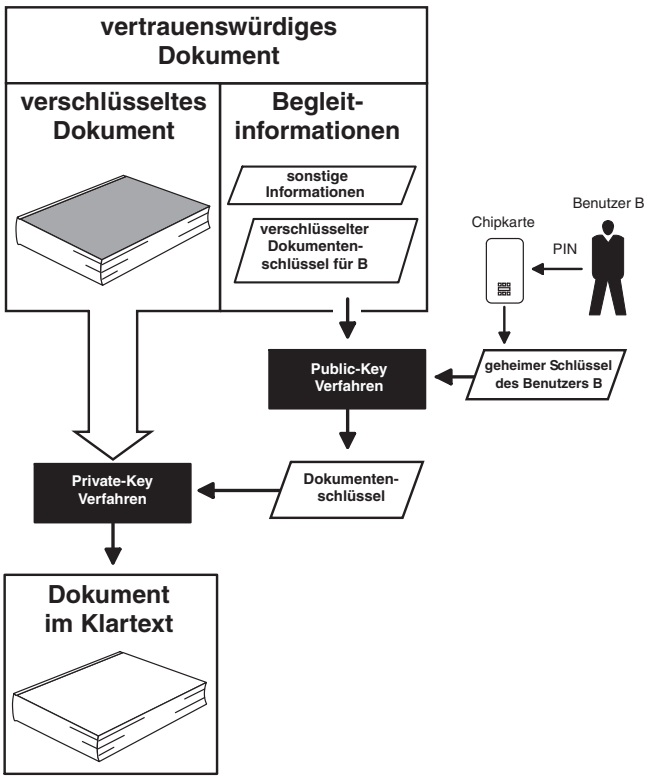


Abb. 7.15: Entschlüsselung eines Dokuments

Zuerst wird der Empfänger aufgefordert, mit seinem Passwort die Chipkarte zu aktivieren. Zur Entschlüsselung wird der für den Empfänger verschlüsselte Doku-

neuKap07.fm Seite 234 Freitag, 18. Oktober 2002 3:52 15

mentenschlüssel den Begleitinformationen entnommen und mit dem geheimen Schlüssel, der sich auf der Chipkarte des Empfängers befindet, mit dem Public-Key-Verfahren entschlüsselt. Anschließend wird das Dokument unter Verwendung des Private-Key-Verfahrens mit dem Dokumentenschlüssel entschlüsselt und steht im Klartext zur Verfügung.

Verifikation von Signaturen

Liegt das Dokument im Klartext vor, kann mithilfe der Verifikations-Funktion die Signatur (bzw. die Signaturen) überprüft werden (Abb. 7.16).

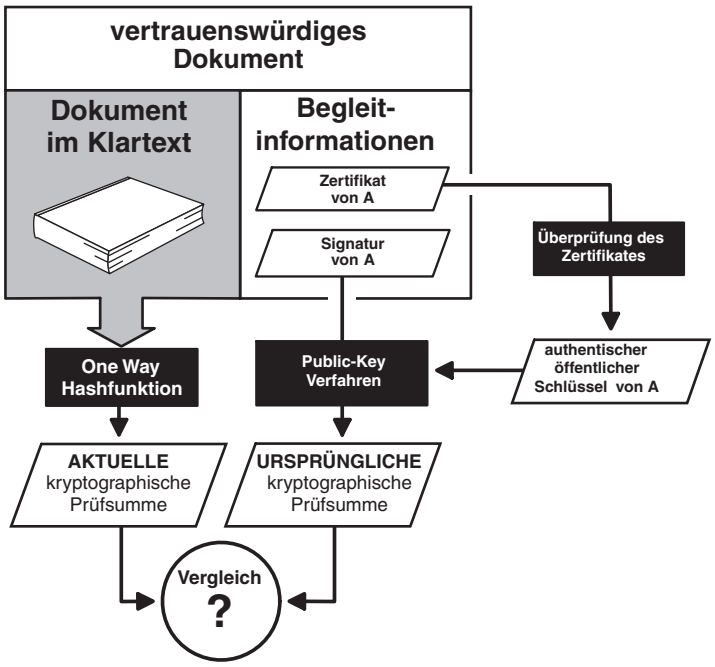


Abb. 7.16: Überprüfung der Signaturen

Zur Überprüfung der Signatur wird mithilfe der One-Way-Hashfunktion die aktuelle kryptographische Prüfsumme über das Dokument berechnet. Danach werden die Signaturen den Begleitinformationen entnommen, um mit dem Public-Key-Verfahren unter Verwendung des öffentlichen Schlüssels des entsprechenden Benutzers die ursprüngliche kryptographische Prüfsumme zu erlangen. Sind beide kryptographischen Prüfsummen gleich, so ist das empfangene Dokument unversehrt, und der Benutzer, der die Signatur durchgeführt hat, ist authentisiert.

neuKap07.fm Seite 235 Freitag, 18. Oktober 2002 3:52 15

7.2.2 Sicherheitsdienste des E-Mail-Sicherheitssystems

Nach erfolgreicher Überprüfung der Signatur ist sichergestellt, dass das Dokument unversehrt übertragen worden ist. Das bedeutet:

- Niemand hat das Dokument manipuliert (Gewährleistung der Datenunversehrtheit).
- Die Zeitangabe der Signatur des Dokuments wurde nicht geändert. Daran kann man erkennen, ob abgefangene Dokumente zu einem späteren Zeitpunkt wieder in die Kommunikation eingeschleust wurden.
- Nur die Benutzer, die in den Begleitinformationen angegeben sind, konnten die entsprechende Signatur durchführen, da nur diese über die entsprechenden Chipkarten mit dem passenden geheimen Schlüssel verfügen.

Diese Funktionen machen die Digitale Signatur zum elektronischen Äquivalent der handgeschriebenen Unterschrift.

Als zusätzliche Sicherheitsfunktion steht die Verschlüsselung des Dokuments zur Verfügung, die seine Vertraulichkeit garantiert. Vertraulichkeit bedeutet, dass keiner außer den in den Begleitinformationen explizit angegebenen Benutzern des Sicherheitssystems das Dokument entschlüsseln und im Klartext lesen kann.

7.2.3 E-Mail Security aus Sicht des Benutzers

Die Sicherheitsfunktionen Digitale Signatur und Objektverschlüsselung werden in die Anwendungsprogramme auf Benutzerseite integriert. Anwendungen sind z. B. Mail-Software (Windows Mail, Windows Exchange, Lotus Notes, usw.), Browser und andere Software. Der Benutzer kann dann durch einfachen Mausklick die Sicherheitsfunktionen aufrufen und die entsprechenden Dienstleistungen nutzen. Je einfacher die Sicherheitsfunktionen genutzt werden können, desto höher wird die Akzeptanz bei den Benutzern sein.

Außerdem ist denkbar, dass die Firewall als zentrale E-Mail-Annahmestelle fungiert, die eingehende E-Mails entschlüsselt und intern verteilt und ausgehende E-Mails signiert, damit die Empfänger sicher sein können, dass diese Mails wirklich von der entsprechenden Organisation stammen.

7.2.4 Objektverschlüsselung und Firewall-Systeme

Durch Objektverschlüsselung werden die Objekte bzw. Dateien bei Anwendungen wie Mail oder FTP statt im Klartext in verschlüsselter Form übertragen. Die Verschlüsselung hat auf die Verfügbarkeit der Sicherheitsfunktionalitäten des Firewall-Systems keinen Einfluss. Jede Übertragung verschlüsselter Daten wird ebenso wie die unverschlüsselter Daten protokolliert. Aufgrund der Objektverschlüsselung werden jedoch Sicherheitsdienste wie Datenunversehrtheit, Urhebernach-

neuKap07.fm Seite 236 Freitag, 18. Oktober 2002 3:52 15

weis und Verschlüsselung auf der Anwenderebene zusätzlich über das Firewall-System zur Verfügung gestellt.

7.2.5 Der elektronische Vertrag: Die Rechtsform der Zukunft?

Zu den altbekannten Vertragsformen »mündlicher Vertrag« und »schriftlicher Vertrag« hat sich fast unbemerkt – rechtlich noch nicht optimal abgesichert, aber in der Praxis bereits häufig angewandt – eine dritte Vertragsform gesellt: der elektronische Vertrag.

Während ein mündlicher Vertrag sich gewöhnlich auf einfache Abmachungen mit geringem Umfang bezieht, ist für den Anwendungsbereich schriftlicher Verträge ein bestimmtes Feld definiert. Bestimmte Dinge dürfen nur schriftlich geregelt werden (vgl. Verbraucherkreditgesetz u. Ä.), und die Vertragskonditionen müssen ausführlich festgelegt werden. Die neue Vertragsform »elektronischer Vertrag« bietet im Unterschied zum althergebrachten mündlichen und schriftlichen Vertrag andere Besonderheiten: Ihr Kennzeichen sind die einfache Handhabung und die Möglichkeit der Versiegelung aller Informationen.

Sicherheitsvorteile

Wenn man die Sicherheitsvorteile der drei Vertragsformen betrachtet, ergeben sich wieder deutliche Unterschiede: der mündliche Vertrag hat so gut wie keine Sicherheiten, während die Vorteile schriftlicher Vertragsabwicklung tief im allgemeinen Bewusstsein verankert sind, denn sie sind über Jahrhunderte gewachsen. Beim schriftlichen Vertrag gibt es auch einen gewissen Warneffekt: Man sollte ein Schriftstück vor der Unterzeichnung sorgfältig lesen, vor allem auch das Kleingedruckte.

Sicherheitsvorteile elektronischer Verträge liegen auf der Hand:

- Alle Informationen können versiegelt werden.
- Die Algorithmen, die der Verschlüsselung zugrunde liegen, sind das Ergebnis jahrzehntelanger Forschung von Experten und daher mathematisch ausgereift.
- Der elektronische Vertrag auf der Basis des Chipkartensystems ist technisch hoch entwickelt.

Risiken elektronischer Verträge

Die Risiken der verschiedenen Vertragsformen lassen sich schnell aufzeigen: Bei einem mündlichen Vertrag entsteht das Problem der Nachweisbarkeit, weshalb mündliche Verträge nur bei einem besonderen Vertrauensverhältnis der beteiligten Vertragspartner empfehlenswert sind. Die Sicherheit von Papierurkunden lässt ebenfalls zunehmend nach, weil sich mit modernen Kopierverfahren, Graphikprogrammen und Robotersystemen sogar eigenhändige Unterschriften fälschen lassen.

neuKap07.fm Seite 237 Freitag, 18. Oktober 2002 3:52 15

Auch bei elektronischen Verträgen sind gewisse Risiken einzukalkulieren. So muss beachtet werden, dass je nach Systemumgebung ein falsches Dokument signiert werden kann. Ein weiterer Risikofaktor ist die organisatorische Umgebung, in der die Möglichkeit besteht, dass jemand sich des Vertragscharakters nicht bewusst ist. Wird die Chipkarte mit Passwort – freiwillig oder unfreiwillig – weitergegeben, gleicht dies einer Generalvollmacht.

7.2.6 Unterschiedliche Konzepte für objektorientierte Sicherheit (S/MIME, PGP)

S/MIME (»Secure MIME«) und PGP (»Pretty Good Privacy«) sind zwei Konzepte, mit denen eine objektorientierte Sicherheit realisiert werden kann. Obwohl auf ähnlichen kryptographischen Verfahren beruhend, verfolgen S/MIME und PGP doch grundsätzlich verschiedene Ansätze. Beide Verfahren werden in diesem Abschnitt vorgestellt und verglichen.

Überblick

S/MIME (Secure Multi-Purpose Internet Mail Extension) und PGP (Pretty Good Privacy) sind Konzepte zur sicheren Übertragung von E-Mails über das Internet. Beide basieren auf der Verschlüsselung und Signatur von Nachrichten vor der Übertragung über ein unsicheres Netzwerk, unterscheiden sich jedoch in der Verwaltung der Schlüssel. Nach der Übernahme der Vermarktungsrechte an PGP durch Network Associates haben sich die Verfahren der Schlüsselverwaltung zwar angenähert, die verbleibenden Unterschiede sind jedoch groß genug, um Kaufentscheidungen zu beeinflussen.

Gemeinsamkeiten von S/MIME und PGP

S/MIME und PGP basieren maßgeblich auf Public-Key-Verfahren. Jeder Benutzer solcher Verfahren benötigt zunächst ein Schlüsselpaar, das er selbstständig generiert. Einer der beiden Schlüssel ist der öffentliche Schlüssel des Benutzers, der veröffentlicht werden soll. Er gibt anderen Benutzern im Netzwerk die Möglichkeit, verschlüsselte Nachrichten an den Schlüsselbesitzer zu senden. Der andere Schlüssel muss geheim gehalten werden. Mit dem geheimen Schlüssel werden verschlüsselte Nachrichten entschlüsselt sowie eigene Nachrichten signiert.

S/MIME und PGP nutzen die oben beschriebenen Kombinationen verschiedener kryptographischer Verfahren. Integrität und Authentizität werden erreicht, indem zunächst eine kryptographische Prüfsumme über den vorgesehenen Text gebildet wird und diese kryptographische Prüfsumme anschließend mit dem eigenen geheimen Schlüssel signiert wird. Bei der Verschlüsselung einer Nachricht wird von der Software eine Zufallszahl als Dokumentenschlüssel gebildet, der nur für diese eine Nachricht gültig ist. Die Nachricht wird dann mit einem symmetrischen Verschlüsselungsalgorithmus unter Zuhilfenahme des Dokumentenschlüssels verschlüsselt.

neuKap07.fm Seite 238 Freitag, 18. Oktober 2002 3:52 15

Danach wird der Dokumentenschlüssel mit dem öffentlichen Schlüssel des vorgesehenen Empfängers verschlüsselt und zusammen mit der verschlüsselten Nachricht übermittelt. Nur der vorgesehene Empfänger kann mit seinem geheimen Schlüssel den Dokumentenschlüssel wieder herstellen und den Nachrichtentext entschlüsseln.

Bei mehreren Empfängern einer Nachricht wird für jeden vorgesehenen Empfänger eine verschlüsselte Version des Dokumentenschlüssels erzeugt und mit der Nachricht versendet. Die Nachricht muss also nicht für jeden Empfänger einzeln verschlüsselt werden.

Zum Signieren und Entschlüsseln einer Nachricht muss der Benutzer auf den eigenen geheimen Schlüssel zugreifen.

Secure MIME – S/MIME

S/MIME ist eine Erweiterung des Mailstandards MIME, der das alte Verfahren UUENCODE/UUDECODE zum Anfügen von Attachments an E-Mails praktisch abgelöst hat. Innerhalb von MIME werden Objekte mit bestimmten Attributen definiert (z. B. Text, Graphik, Audiodaten), die beim Empfänger eine gezielte Weiterverarbeitung erfordern (z. B. das Abspielen einer Audio-Botschaft). S/MIME spezifiziert den Einsatz diverser Kryptoalgorithmen, die der Benutzer bzw. seine Software nach Bedarf auswählen kann. In erster Linie sind dies Triple-DES, RSA und SHA-1, der alte Hash nach MD5 wird aus Kompatibilitätsgründen noch unterstützt. Eine Erweiterung um andere Algorithmen ist problemlos möglich. Die Benutzung von anderen Algorithmen setzt voraus, dass beide Kommunikationspartner über die gleiche Lösung verfügen.

Die Erstellung einer S/MIME-Nachricht beinhaltet die Vorbereitung der S/MIME-Objekte (Digitale Signatur, Verschlüsselung, Codierung) und Einbettung als Attachments in eine MIME-Nachricht als Tranformationsschritte. Die gebildeten S/MIME-Objekte in der Nachricht können signiert, verschlüsselt oder signiert und verschlüsselt sein. S/MIME bietet die Möglichkeit, signierte Nachrichten in einem clear-signed-Format zu verschicken, in dem die Digitale Signatur von der Nachricht getrennt wird, so dass die Nachricht auch von E-Mail-Programmen verarbeitet werden kann, die zwar MIME, aber nicht S/MIME unterstützen. Die von S/MIME verwendete Datenstruktur kann auch die Identität des Senders schützen, denn die Signatur und die Nachricht können in einem verschlüsselten »digitalen Umschlag« verschickt werden.

Schlüsselmanagement

S/MIME schreibt kein Vertrauensmodell vor, daher ist theoretisch auch der Aufbau eines Web-of-Trust möglich. In der Regel wird jedoch ein zentrales oder hierarchisches Vertrauensmodell verwendet. Es besteht somit die Möglichkeit, eine eigene PKI aufzubauen oder mithilfe von vertrauenswürdigen Dritten öffentliche Schlüs-

neuKap07.fm Seite 239 Freitag, 18. Oktober 2002 3:52 15

sel Personen zuzuordnen. Dabei erhält der Benutzer ein Zertifikat nur auf Anfrage (nach PKCS#12), nachdem er sich nach genau definierten Verfahren gegenüber einer CA authentifiziert hat. Die Vertrauenswürdigkeit des Zertifikats hängt von der Art dieses Verfahrens ab. Abhängig davon, ob lediglich die E-Mail-Adresse geprüft wird oder ein amtlicher Personalausweis vorzulegen ist, können unterschiedliche Klassen von Zertifikaten ausgestellt werden.

S/MIME setzt bei der Verwendung von Zertifikaten auf vorhandene Standards. Beide S/MIME-Versionen unterstützen das X.509-Format in den Versionen 1 und 3, die im Internet weit verbreitet sind. Die Gültigkeit der von der CA ausgestellten Zertifikate kann anhand des Zertifikats der so genannten Root-CA (Wurzel-CA) überprüft werden, das einmalig verifiziert werden muss.

S/MIME bietet die Möglichkeit, einen digitalen Fingerabdruck des öffentlichen Schlüssels zu erstellen, sodass die CA diesen zur Überprüfung ihrer eigenen Zertifikate veröffentlichen kann. Da S/MIME somit nicht auf ein bestimmtes Vertrauensmodell festgelegt ist, hat der Benutzer den Vorteil, sich das für ihn am besten geeignete Modell aussuchen zu können. Sicherheitsbewusste Organisationen wählen ein zentrales Vertrauensmodell, da sie so die Organisation der Zertifizierung selber kontrollieren können.

Ein hierarchisches Vertrauensmodell behält die Funktion eines zentralen Vertrauensmodells bei, ermöglicht jedoch eine über die firmeneigene CA herausgehende Überprüfung der Zertifikate. Es eignet sich besonders für Benutzer, die ein weniger starres Modell bevorzugen und eine Signatur-konforme Unterschrift erreichen wollen.

Falls eine geringe Vertrauenswürdigkeit der Zertifikate akzeptiert werden kann, bietet ein Web of Trust die Möglichkeit, von vertrauenswürdigen Dritten unabhängig zu bleiben. Der Austausch der öffentlichen Schlüssel ist sehr einfach möglich, denn das Zertifikat ist in jeder signierten E-Mail vorhanden, sodass es, falls es von einer bekannten CA ausgestellt wurde, überprüft und der öffentliche Schlüssel des Absenders gespeichert werden kann.

Einige der S/MIME-Produkte bieten zusätzlich die Möglichkeit, Zertifikate mittels LDAP über öffentliche Schlüssel abzufragen.

Pretty Good Privacy/PGP

1991 wurde in den USA von Phil Zimmermann die Verschlüsselungs-Software PGP entwickelt. Zeitweise gab es aufgrund der US-amerikanischen Exportbeschränkungen mehrere internationale PGP-Versionen, die sich von den US-Versionen durch abweichende kryptographische Routinen unterschieden. Die verwendeten Schlüssel und Nachrichten der verschiedenen Versionen sind kompatibel. Seit Anfang 2000 darf PGP wieder ohne Beschränkungen aus den USA exportiert werden, sodass nicht mehr zwischen US- und Export-Versionen unterschieden werden muss.

neuKap07.fm Seite 240 Freitag, 18. Oktober 2002 3:52 15

PGP basiert auf den symmetrischen Verfahren Triple-DES, IDEA und Cast, wobei die symmetrischen Schlüssel mittels Diffie-Hellman oder RSA ausgetauscht werden. Zur Berechnung des Hashs sind SHA-1 und MD5 implementiert.

Wie S/MIME generiert auch PGP bei der Bearbeitung von Klartexten einen Header, der aber nicht vor den Text kopiert, sondern an die Nachricht angefügt wird. Außerdem liegt der Header beim klassischen PGP als Block vor, es gibt keine einzelnen Einträge. Nachricht und Header werden in (je nach Nachrichtentyp unterschiedliche) Begrenzungszeilen eingeschlossen.

Ein PGP-Benutzer wird mit einer frei wählbaren Benutzeridentifikation identifiziert. Aus dem öffentlichen Schlüssel, dem eine eindeutige ID zugewiesen wird, wird eine kryptographische Prüfsumme – der »Fingerprint« – berechnet, anhand derer man die Authentizität des Schlüssels überprüfen kann.

Schlüsselmanagement

Auch PGP beruht auf dem Prinzip der Public-Key-Zertifikate, die in diesem Fall aus der Benutzeridentifikation und dem korrespondierenden öffentlichen Schlüssel gebildet werden. Die Zertifikate werden in verschlüsselten Dateien, so genannten Keyrings, abgelegt, die beliebig an andere Benutzer verteilt werden können. Der geheime Schlüssel ist bei PGP in der Regel mit einem Rechner oder einer E-Mail-Adresse verknüpft.

Bei PGP ist der Zertifizierungsvorgang nicht geregelt. Um den öffentlichen Schlüssel eines Benutzers zu prüfen, vergleicht man ihn mit dem »Fingerprint« des entsprechenden Benutzers, den man auf alternativem Weg (Telefon, Visitenkarte) erhalten hat. Außerdem gibt es vertrauenswürdige Personen (»Introducer«), von denen Zertifikate der öffentlichen Schlüssel anderer Benutzer bestätigt werden.

Im Internet sorgen Public-Key-Server für die Verteilung der öffentlichen Schlüssel. Hier kann jeder Benutzer mit einfachen Kommandos per E-Mail seinen eigenen öffentlichen Schlüssel speichern lassen und die öffentlichen Schlüssel aller anderen Benutzer abrufen. Die einzelnen Server gleichen ihre lokalen Datenbanken in regelmäßigen Abständen miteinander ab.

Dabei übernehmen die Public-Key-Server jedoch lediglich eine Speicherfunktion und überprüfen die gespeicherten Schlüssel nicht. Die Korrektheit der Zertifikate muss jeder Benutzer nach Erhalt eines Zertifikats selbst überprüfen. Daher sollte ein Zertifikat nur in den eigenen Keyring aufgenommen werden, wenn seine Authentizität garantiert ist.

Sowohl S/MIME als auch PGP können signierte und verschlüsselte Nachrichten im ASCII-Format erzeugen, die anschließend in jede normale E-Mail eingebunden und verschickt werden können.

neuKap07.fm Seite 241 Freitag, 18. Oktober 2002 3:52 15

Neue Tendenzen bei PGP

Nach der Übernahme der kommerziellen Vermarktungsrechte an PGP hat Network Associates eine Reihe von Neuerungen eingeführt, um PGP auch für Netze von Firmen oder anderen Organisationen attraktiv zu machen. Die bisher gemachten Überlegungen zu PGP gelten aber unverändert für die Freeware-Version. Die wichtigsten Neuerungen sind:

- Kompatibilität von PGP mit dem Zertifizierungsmechanismus von X.509. PGP-Clients können beide Klassen von Zertifikaten akzeptieren, sodass mit PGP wahlweise eine hierarchische Struktur von Zertifikaten analog zu S/MIME aufgebaut werden kann.
- Erweiterungen der Möglichkeiten der Public-Key-Server. Diese können jetzt auch Hierarchien von Zertifizierungen bilden, die aber gegenüber X.509 flexibler sind. So können Zertifikate von mehreren Instanzen beglaubigt werden und der Client akzeptiert diese Signaturen, wenn die gewichtete Summe der Zertifikate einen Schwellwert überschreitet. So kann der Abteilungsleiter die öffentlichen Schlüssel seiner Mitarbeiter beglaubigen, der Bereichsleiter die der Abteilungsleiter etc. Wie im herkömmlichen Schriftverkehr ist es somit beispielsweise möglich, ein Dokument nur dann zu akzeptieren, wenn es vom Prokuristen und dem zuständigen Bereichsleiter unterschrieben ist.
- PGP sieht Mechanismen zum Key-Recovery vor, mit denen innerhalb einer Organisation geheime Schlüssel ermittelt werden können. So können verloren gegangene Schlüssel oder Schlüssel ungetreuer Mitarbeiter mithilfe bestimmter, firmenintern an sicherer Stelle verwahrter Daten rekonstruiert und die damit verschlüsselten Dokumente entschlüsselt werden.
- Außerdem erlauben die in RFC2015 definierten neue MIME-Objekte ganz analog zu S/MIME eine Einbettung von PGP in den mittlerweile zum Standard gewordenen E-Mail-Verkehr mittels MIME.

Abschließender Vergleich zwischen S/MIME und PGP

Die Lösungen S/MIME und PGP definieren beide Sicherheitsmechanismen, mit denen sich beliebige Dokumente verschlüsseln und signieren lassen. Die kryptographischen Algorithmen sind bei beiden etwa gleich stark. Unabhängig vom darunter liegenden Transport-Protokoll lassen sich die erzeugten Nachrichten bearbeiten, in E-Mails einbinden und verschicken.

Im Schlüssel-Management gibt es grundsätzliche Unterschiede zwischen S/MIME und PGP. Schlüssel in S/MIME und dem kommerziellen PGP werden von Zertifizierungsinstanzen signiert. Die Hierarchie von Instanzen ermöglicht eine einfache und zuverlässige Überprüfung fremder öffentlicher Schlüssel. Ohne die Infrastruktur der Zertifizierungsinstanzen ist eine sinnvolle Nutzung der Verfahren nicht möglich. Eine Infrastruktur wird in Deutschland im Rahmen des Signaturgesetzes aufgebaut. Freeware-PGP ist unabhängig von Hierarchien, weil jeder

neuKap07.fm Seite 242 Freitag, 18. Oktober 2002 3:52 15

Benutzer selbst entscheidet, welchen Schlüsseln er traut. Er kann sofort mit anderen Benutzern kommunizieren, wenn er deren Public Key kennt und als authentisch nachgewiesen hat.

Bewertung von S/MIME und PGP

Im Internet stellen die beiden Applikationen S/MIME und PGP keine Konkurrenzprodukte dar, sondern finden verschiedene Einsatzgebiete.

Kleinen Benutzergruppen, die sichere Kommunikationskanäle suchen, bietet Freeware-PGP die Möglichkeit der objektorientierten Verschlüsselung: es setzt keine Infrastruktur voraus, aber das gegenseitige Vertrauen der Benutzer ohne eine übergeordnete Instanz.

In Netzen von Firmen oder anderen größeren Organisationen bietet das kommerzielle PGP mit seinen flexiblen Optionen die Möglichkeit, die jeweilige Organisationsstruktur mit ihren vielfältigen Beziehungen der Personen untereinander auf die Struktur der Zertifizierung abzubilden. Auch der mögliche Zugriff auf die von den Mitarbeitern verschlüsselten Mails und andere Dateien nach dem Motto »Unternehmensdaten gehören der Firma« steigert die Attraktivität des kommerziellen PGP in diesem Bereich.

In einem großen, unüberschaubaren Netzwerk mit vielen unbekannten Benutzern bietet sich die Benutzung einer strengen Struktur bei der Zertifizierung an, wie sie S/MIME oder PGP mit X.509 bieten. Ist die Zertifizierungsinfrastruktur aufgebaut und etabliert, stellen beide Produkte gute Werkzeuge für die sichere Übertragung von Objekten über ein unsicheres Netz wie das Internet dar. Eine weltweit funktionierende Infrastruktur muss noch etabliert werden. Im Hinblick auf die rasch wachsende Zahl der Teilnehmer im Internet und die Unterstützung des S/MIME-Standards durch Microsoft (Outlook, Exchange) ist S/MIME aus heutiger Sicht sicherlich die Lösung mit den größeren Chancen.

7.2.7 Der Markt bestimmt den Erfolg

Leider dauern Normungsaktivitäten oft zu lange für den sich immer schneller entwickelnden IT-Markt. Die Erfahrung hat gezeigt, dass Anwendungen, die in der Praxis funktionieren und bezahlbar sind, vom Markt akzeptiert werden und sich als de-facto-Standard etablieren.

Da aber im Bereich der IT-Sicherheit gerade die amerikanischen Technologieunternehmen nicht in der Lage sind, Sicherheitsprodukte anzubieten, die den Sicherheitsanforderungen genügen, die wir als Informations- und Know-how-Gesellschaft in Deutschland und Europa benötigen, muss in Europa ein eigenständiger und praktikabler Sicherheitsstandard realisiert werden. Dabei sollten wir ein wirklich sicheres und zugleich praktikables Systemkonzept wählen.

neuKap07.fm Seite 243 Freitag, 18. Oktober 2002 3:52 15

7.2.8 TeleTrusT – ein interdisziplinärer Verein zur Förderung der Vertrauenswürdigkeit in der Informations- und Kommunikationstechnologie

TeleTrusT Deutschland – siehe: www.teletrust.de – ist ein eingetragener Verein, der sich die Förderung von Wissenschaft, Normung und Bildung im Bereich der Entwicklung einer verlässlichen Informations- und Kommunikationstechnik zum Ziel gesetzt hat. Im Mittelpunkt der Aktivitäten von TeleTrusT steht die rechtliche Anerkennung der »digitalen Signatur«.

Der Verein besteht aus Herstellern, Anwendern, Forschungsinstituten, Bundesbehörden, Verbraucherverbänden, Beratungsunternehmen, Netzbetreibern, Serviceanbietern und auch Unternehmen des Mittelstands. Unter den über 100 Mitgliedern finden sich so namhafte Unternehmen wie Siemens, Alcatel SEL, Microsoft, Telekom, SNI, Datev und die Kassenärztlichen Vereinigungen.

Bei TeleTrusT diskutieren diese in unterschiedlichen Arbeitsgruppen mit unterschiedlichen Schwerpunkten, wie gemeinsam vertrauenswürdige Kommunikationssysteme geschaffen und eingesetzt werden können.

Die Arbeit von TeleTrusT macht den Weg frei für erfolgreiche und vertrauenswürdige Anwendungen von bereichs- und standortübergreifender Informationstechnologie:

- Brücken zwischen Forschung und Praxis: Die Forschung soll schnell die Sicherheitsmechanismen anbieten können, die wirklich notwendig sind, und nicht allzu ehrgeizige Fernziele in Aussicht stellen, die auf absehbare Zeit nicht einzulösen sind.
- Brücken zwischen Entwicklern und Anwendern: Die Sicherheitsinstrumente müssen für den Anwender einfach bedienbar sein. Die Sicherheit muss direkt in die Anwendung oder in die Geschäftsprozesse eingebunden werden – nur dann wird der Anwender bereit sein, die Umsetzung einer Sicherheitspolitik in seinen Arbeitsalltag zu integrieren.
- Lückenschluss zwischen theoretischer Sicherheit und marktgerechten Sicherheitslösungen: Nicht alles, was theoretisch möglich ist, wird auch vom Markt gefordert. Die ersten 80% der Sicherheit sind schnell eingeführt. Auf 90% kommt man mit bezahlbaren Mitteln. Wer aber – unbezahlbare – 100% erreichen will, verhindert möglicherweise jegliche Sicherheit. Ein Grundmaß an Sicherheit muss zuallererst praktikabel sein.

Maßnahmen zur IT-Security arbeiten mit kalkulierbaren Restrisiken – nicht anders als etwa Sicherheitsmaßnahmen beim Autoverkehr. Verschiedene Klassen von Autos bieten verschiedene Sicherheitsausstattungen. Kein Auto aber bietet völlige Unfallsicherheit. Marktgerechte Sicherheitslösungen bestehen oft aus überlappenden und ergänzenden Sicherheitslösungen – mit anderen Worten: Wir müssen ein kalkulierbares Restrisiko akzeptieren, um überhaupt zu Ergebnissen für

neuKap07.fm Seite 244 Freitag, 18. Oktober 2002 3:52 15

die Praxis zu kommen. Dieses Restrisiko muss mit weiteren, nicht-technischen Sicherheitsmaßnahmen reduziert werden.

Dazu gehört an erster Stelle eine **Security Policy**, in der u. a. definiert wird, dass eine Organisation vertrauenswürdige Informationen hat, die entsprechend geschützt werden müssen. Dazu gehört auch eine Definition, wann was verschlüsselt und/oder digital signiert werden muss. Damit erhält jeder Anwender eine genaue Anweisung bezüglich des Umgangs mit sensiblen Informationen. Diese Anweisung sollte mithilfe einer Arbeitsanweisung in der Organisation kommuniziert werden, damit eindeutige Richtlinien für die einzelnen Mitarbeiter vorhanden sind. Außerdem müssen die Mitarbeiter geschult werden, um die Sicherheitsprodukte korrekt und effektiv einsetzen zu können.

Schließlich ist wichtig, dass die Mitarbeiter angewiesen werden, die vorhandenen Sicherheitsmechanismen auch einzusetzen und dass sie für den Einsatz entsprechend der Security Policy verantwortlich sind. Auch müssen die Mitarbeiter darüber informiert werden, welche rechtlichen Konsequenzen der Einsatz von Sicherheitsmechanismen mit sich bringt.

7.2.9 MailTrusT – interoperable Sicherheitslösung

In einem Sicherheitssystem, das organisationsübergreifend genutzt werden soll, ist die Infrastruktur von besonderer Bedeutung. Die folgende Grafik zeigt, dass bei der Realisierung viele unterschiedliche Schnittstellen zu berücksichtigen sind. Die gemeinsame Sicherheitsinfrastruktur geht bei virtuellen Welten wie dem Internet über alle geographischen, politischen, gesetzlichen und kulturellen Grenzen hinaus und stellt somit eine völlig neue Herausforderung dar. |Pohl 99b|

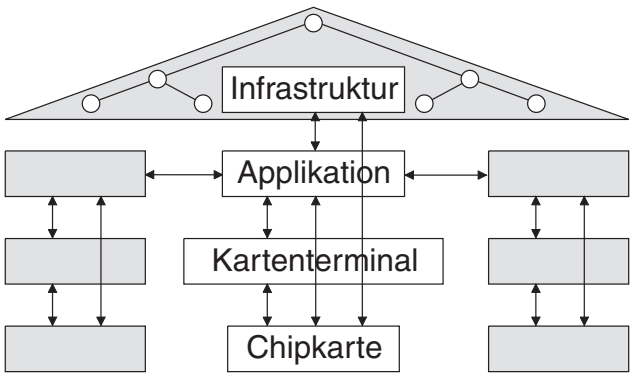


Abb. 7.17: MailTrusT-Architektur

Um eine Anwendung vertrauenswürdig realisieren zu können, muss eine Sicherheitstechnologie – ein Sicherheitsprodukt – integriert werden, die die notwendigen Sicherheitsfunktionen wie z. B. Vertraulichkeit durch Verschlüsselung und Digi-

neuKap07.fm Seite 245 Freitag, 18. Oktober 2002 3:52 15

tale Signatur zur Verfügung stellt. Typischerweise benötigt der Benutzer hierzu ein Security Token, das eine Chipkarte oder eine spezielle Diskette sein kann. Wenn es sich um eine Chipkarte handelt, muss an die Anwendung ein Chipkartenleser angeschlossen werden.

Eine Grundvoraussetzung für eine organisationsübergreifende Sicherheit ist eine gemeinsame Infrastruktur, die dafür sorgt, dass alle an dem Sicherheitssystem beteiligten Personen einen eindeutigen Namen und einen elektronischen Ausweis – in der Terminologie: ein Zertifikat – haben, in dem der öffentliche Schlüssel eines Public-Key-Verfahrens beglaubigt wird. Außerdem muss die Applikation auf Verzeichnisdienste zugreifen können, die stetig darüber informieren, ob bestimmte Benutzer, mit denen eine Kommunikation durchgeführt werden soll, noch gültige Zertifikate haben oder ob sie in eine Sperrliste aufgenommen worden sind. All diese Schnittstellen müssen in einem Systemkonzept spezifiziert werden. Genau hier liegt der Ansatz von MailTrusT (MTT).

MailTrusT ist ein Systemkonzept für den vertrauenswürdigen Austausch von E-Mails und anderen elektronischen Objekten sowie der notwendigen Sicherheitsinfrastruktur in offenen Systemen. Die Leistung von MailTrusT ist es, eine Teilmenge der Möglichkeiten der einzelnen Industriestandards definiert und in Kombination unterschiedlicher Standards ein sinnvolles und praktisch einsetzbares Ganzes geschaffen zu haben.

Zielvorgaben des MailTrusT-Systemkonzepts

Das MailTrusT-Systemkonzept besteht aus einer Reihe von Teilspezifikationen und umfasst die im Folgenden dargestellten und für eine erfolgreiche Anwendung notwendigen Zielvorgaben:

- **Interoperabilität**
  Das MailTrusT-Sytemkonzept gewährleistet, dass Produkte unterschiedlicher Hersteller, die diesem Systemkonzept genügen, ohne Modifikationen oder weitere Abstimmungen direkt interoperabel sind.
- **Minimalität**
  Das MailTrusT-Systemkonzept ist minimal, um Produktherstellern eine maximale Gestaltungsfreiheit zu erhalten. Es ist im Wesentlichen auf die für die Interoperabilität verschiedener Komponenten erforderlichen Festlegungen für einen in der Regel ausreichenden Funktionsumfang beschränkt (»*Soviel wie nötig, so wenig wie möglich*«). Herstellern bleibt somit noch Spielraum, um auf Marktanforderungen einzugehen.
- **Kontinuität**
  Sowohl für die Hersteller als auch für die Kunden MailTrusT-konformer Komponenten wird durch Kontinuität Investitionssicherheit in größtmöglichem Umfang gewährleistet. Dieser Ansatz wird auch in Zukunft weiter verfolgt werden.

neuKap07.fm Seite 246 Freitag, 18. Oktober 2002 3:52 15

- **Universalität**
  Das MailTrusT-Systemkonzept setzt kein bestimmtes Modell einer Public Key Infrastruktur voraus; es unterstützt zentrale, dezentrale und kombinierte Modelle. Das MailTrusT-Systemkonzept ist auch nicht auf bestimmte Anwendungen beschränkt. Es ist vielmehr für eine breite Palette von Anwendungen entworfen.

- **Modularität**
  Das MailTrusT-Systemkonzept besteht aus mehreren aufeinander abgestimmten Modulen, die Teile eines umfassenden Systemkonzepts sind. Nicht jeder Hersteller muss alle Module realisieren, um ein MailTrust-konformes Produkt anbieten zu können. Da die Module aufeinander abgestimmt sind, können Module verschiedener Hersteller miteinander kombiniert werden. Durch die Token-Schnittstelle können z. B. Komponenten eines Herstellers Chipkarten eines anderen Herstellers verwenden.

- **Standardkonformität**
  Das MailTrusT-Systemkonzept basiert soweit wie möglich auf etablierten und verbreiteten Standards. Neben S/MIME, PEM, X.509 und PKCS#11 (»Cryptoki«) werden insbesondere auch die Spezifikation der PKIX-Arbeitsgruppen der IETF und die Signatur-Interoperabilitätspezifikation zum Signaturgesetz berücksichtigt. Auf dieser Basis werden Profile definiert, die die Standards interoperabel machen und den Zielen von MailTrusT gerecht werden.

- **Unabhängigkeit**
  Das MailTrusT-Systemkonzept wurde auf der Grundlage von Praxiserfahrungen von verschiedenen Anwendern, Providern, Forschungseinrichtungen, Verbraucherverbänden und Herstellern erstellt. Proprietäre Lösungen einzelner Produkthersteller waren dabei ausdrücklich kein Maßstab für das MailTrusT-Systemkonzept.

Aufbau und Komponenten des MailTrusT-Systemkonzepts

Die vorliegende Spezifikation des Systemkonzeptes setzt kein festes Modell einer Zertifizierungsinfrastruktur voraus. Der Aufbau einer Zertifizierungsinfrastruktur kann deshalb wesentlich flexibler den jeweiligen Anforderungen angepasst werden.

Jede MailTrusT Public-Key-Infrastruktur (PKI) besteht aus folgenden Grundkomponenten:

- Teilnehmer-Komponenten (TN)
- Zertifizierungsstellen (CA)
- Registrierungsstellen (RA)
- Verzeichnisdiensten (DIR)

neuKap07.fm Seite 247 Freitag, 18. Oktober 2002 3:52 15

Jede dieser Komponenten hat innerhalb der Public-Key-Infrastruktur eine bestimmte Funktion und dementsprechend bestimmte Aufgaben zu erfüllen. Die Aufgabenzuweisung soll möglichst flexibel an die Anforderungen der jeweiligen Public-Key-Infrastruktur angepasst werden können. Deshalb erfolgt keine feste Zuweisung von Aufgaben zu Komponenten. Es werden lediglich Empfehlungen gegeben.

Zwischen den Komponenten gibt es eine Vielzahl spezifizierter online-Schnittstellen für die wesentlichen Interaktionen. Schnittstellen sind auch für die Kommunikation zwischen verschiedenen Teilen einer Grundkomponente definiert.

Die folgende Abbildung stellt exemplarisch den prinzipiellen Aufbau einer MailTrusT Public-Key-Infrastruktur mit ihren Komponenten und den Schnittstellen dar:

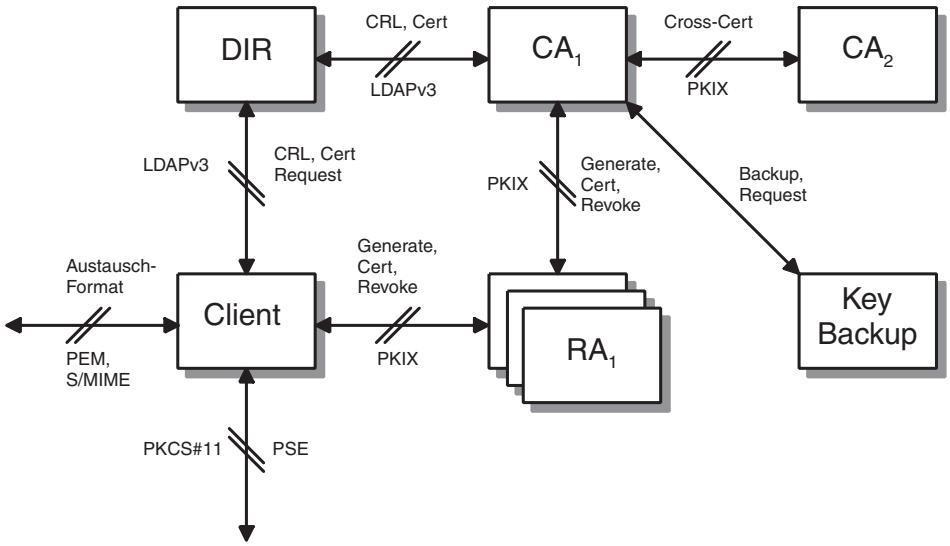


Abb. 7.18: MailTrusT – Kommunikation und Schnittstellen

Systemspezifische Vorteile des MailTrusT-Standards

Für den MailTrusT-Standard sprechen zahlreiche Vorteile:

- herstellerübergreifender Standard von derzeit acht europäischen Herstellern; weitere Hersteller können jederzeit an der Weiterentwicklung des Standards mitwirken und eigene MTT-kompatible Produkte herstellen
- Kompatibilität und Interoperabilität der MTT-Produkte haben sich in verschiedenen Projekten im Gesundheitswesen und bei Bundes- und Landesbehörden (Projekt SPHINX) in Deutschland bewährt
- höchster Sicherheitsstandard durch den Einsatz europäischer Technologie

neuKap07.fm Seite 248 Freitag, 18. Oktober 2002 3:52 15

- Kryptographie ist in Deutschland und Europa keinen gesetzlichen Restriktionen, etwa bezüglich der Schlüssellänge, unterworfen.
- die Erweiterung um S/MIME öffnet den MailTrusT-Standard hin zum US-amerikanischen Markt
- Anlehnung an das deutsche Signaturgesetz, was die gesetzliche Grundlage für den Einsatz der Digitalen Signatur sicherstellt
- Unterstützung Signaturgesetz-konformer Trustcenter
- flexible Anbindung an unterschiedliche PKI-Modelle
- regelmäßige Pflege und Weiterentwicklung des Standards: in den entsprechenden TeleTrusT-Arbeitsgemeinschaften (AG8 & SPHINX) wird offen über die Fortschreibung des MTT-Standards zwischen Herstellern, Benutzern und Mentoren, Verbraucherverbänden und Forschungseinrichtungen etc. diskutiert und die neu auftretenden Kunden- und Marktanforderungen werden in den Standard implementiert
- Gewährleistung der Investitionssicherheit, da mehr als ein Unternehmen den Standard weiterentwickelt
- durch das modulare Konzept werden verschiedene kundenspezifische Realisierungen ermöglicht

MailTrusT-Produkte sind für viele Plattformen und Applikationen verfügbar und bieten somit plattformübergreifende und applikationsunabhängige Kommunikationsssicherheit.

Praktische Realisierung – das Projekt SPHINX

Heute ist die MailTrusT-Spezifikation europäischer Standard für ein herstellerunabhängiges, interoperables System der Ende-zu-Ende-Sicherheit in offenen IT-Systemen. Im Sinne einer konsequenten Praxisorientierung bei der Entwicklung von Sicherheitsmechanismen war ein realer Anwendungstest im großen Rahmen ein wichtiges Mittel zur Etablierung der MailTrusT-Spezifikation. Das SPHINX-Projekt stellte genau diesen Testlauf dar und brachte im Wesentlichen die erhofften Ergebnisse.

Das SPHINX-Projekt unterzog Anfang 1999 E-Mail-Sicherheitstechnologien einem großangelegten Praxistest: Es zeigte sich: Herstellerübergreifende Sicherheit in großen Informationsverbünden funktioniert. Für die Interoperabilität der Produkte sorgt die gemeinsame Orientierung am MailTrusT-Standard von TeleTrusT.

Im SPHINX-Projekt wurden E-Mail-Sicherheitsprodukte verschiedener Hersteller in einem Rahmen erprobt, der für die Einführung einer Zertifizierungshierarchie wie geschaffen ist: im Bereich oberer Bundes- und Landesbehörden. Mehr als 30 Institutionen der oberen Bundes- und Landesbehörden nutzen Sicherheitsmechanismen von unterschiedlichen Anbietern. Beteiligt waren unter anderem Stellen im Bundeskriminalamt, im Bundesamt für Sicherheit in der Informationstechno-

neuKap07.fm Seite 249 Freitag, 18. Oktober 2002 3:52 15

logie, der Innenministerien von Sachsen und Schleswig-Holstein bis hin zur Bundesdruckerei. Acht europäische Hersteller testeten in diesem Projekt ihre Technologien, darunter auch drei verschiedene Trust-Center-Technologien.

Dieses Projekt hat überzeugend gezeigt, dass auch komplexere Systeme kompatibel betrieben werden können. Die Ergebnisse des Pilotprojektes erfüllten die Erwartungen im Wesentlichen und waren ermutigend für Teilnehmer und Betreiber. »SPHINX« bewies, dass das MailTrusT-Konzept eine tragfähige Lösung darstellt – das System funktionierte wie erhofft und wurde von den Teilnehmern angenommen. Bei der Beurteilung der Einsetzbarkeit der Sicherheitstechnologien vergaben 81% der Befragten gute Noten; 90% hielten den abverlangten Aufwand für vertretbar. Den Organisatoren wurde deutlich, wie wichtig eine gute Betreuung der Teilnehmer ist. Von großer Bedeutung ist auch die Vermittlung von Hintergrundinformationen, speziell was die Notwendigkeit des Einsatzes von Sicherheitstechnologien betrifft. Gerade hier lässt sich die Anwenderakzeptanz deutlich erhöhen, indem man noch stärker an der Sensibilisierung der Teilnehmer arbeitet.

Die Fortsetzung des Projekts sieht eine Erweiterung des Funktionsumfangs der Produkte sowie die Behebung von kleineren Problemen hinsichtlich der Interoperabilität vor. Weiterhin wird die Teilnehmerzahl vergrößert werden. In der nun anstehenden Phase werden über 500 Teilnehmer aus verschiedenen oberen Bundesbehörden beteiligt sein. Insgesamt zeigte sich das SPHINX-Projekt als vielversprechender Ansatz, der sich als Keimzelle einer umfassenden Sicherheitsinfrastruktur für E-Mails erweisen könnte. In den kommenden Jahren sind grundlegende Schritte in Richtung eines Sicherheitssystems zu erwarten, das bald zum Geschäftsalltag gehören wird. Unter diesen Entwicklungen muss das SPHINX-Projekt als besonders beachtenswert gelten. Nach dem großen Erfolg von SPHINX ist zu hoffen, dass MailTrusT auch in anderen großen Anwendungsfeldern wie bei Banken und Versicherungen, in der Industrie und im Gesundheitswesen Vertrauenswürdigkeit in die standortübergreifenden IT-Geschäftsprozesse bringt.

7.2.10 ISIS-MTT-Spezifikation für Interoperabilität und Testsysteme

Für den sicheren E-Mail Austausch, die Anwendung von elektronischen Signaturen und das IT-Security-Management sind auf Public-Key-Infrastrukturen gestützte Lösungen erforderlich. Um deren flächendeckende Einführung für E-Government-Anwendungen, in Behörden, in der Wirtschaft und im Finanzsektor zu unterstützen, wurde TeleTrusT Deutschland vom Bundesministerium für Wirtschaft und Technologie (BMWi) der Auftrag erteilt, gemeinsam mit der Gruppe T7 e.V. die Grundlagen für Entwicklung und Test von interoperablen Lösungen zu schaffen.

neuKap07.fm Seite 250 Freitag, 18. Oktober 2002 3:52 15

Folgende Kriterien werden hierbei zugrunde gelegt:

- Investitionssicherheit für Anwender und Anbieter durch Kompatibilität zu internationalen Standards und bereits verwendeten Zertifikatsformaten, durch langfristige Stabilität der Spezifikation und problemlose Interoperabilität von Produkten verschiedener Hersteller
- Anpassungsfähigkeit des Sicherheitsniveaus an die unterschiedlichen Anwendungsfelder
- Berücksichtigung aller für den elektronischen Geschäftsverkehr relevanten Formvorschriften (z. B. des Privat- und Verwaltungsrechts)

Die ISIS-MTT-Spezifikation basiert auf internationalen Standards (S/MIME, PKIX, PKCS, X.509, ETSI, CEN ESI etc.) und integriert die aus der bisherigen Anwendung gewonnenen Erfahrungen. Sie besteht aus einer Kernspezifikation, die die Grundanforderungen aller Anwendungskategorien abdeckt, und Erweiterungen für die verschiedenen Anwendungen (z. B. elektronische Signatur, E-Mail-Verschlüsselung mit unterschiedlichen Sicherheitsniveaus). Darin werden ausschließlich Festlegungen getroffen, die in den bestehenden Standards nicht hinreichend eindeutig geregelt sind.

Um die Voraussetzungen für die Entwicklung interoperabler Anwendungen auf internationaler Ebene zu schaffen, wird die Akzeptanz von ISIS-MTT in den europäischen und weltweiten Standardisierungsgremien angestrebt. Auch die enge Verzahnung mit der Bridge-CA-Initiative bietet eine Möglichkeit, ISIS-MTT-Anwendungen schnell auf eine breite Basis zu stellen (siehe auch `http://www.teletrust.de`).

7.2.11 Bridge-CA

Mit der zunehmenden Verbreitung von PKI-basierten Dienstleistungen erhalten die Anwender eine Vielzahl von verschiedenen Zertifikaten für spezielle Applikationen mit einem spezifischem Verwendungszweck und einem spezifischen Vertrauensmodell. Die Handhabung dieser Zertifikate in den verschiedenen Stadien ihres Lebenszyklus (Ausgabe, Nutzung, Verlängerung, Rücknahme) entwickelt sich zu einer zunehmend komplexen und aufwändigen Aufgabe.

Um diesen Aufwand zu verringern, ist die gegenseitige Akzeptanz von Zertifikaten der verschiedenen PKIs erstrebenswert. Dazu müssen nicht nur technische, sondern auch organisatorische (die Policy betreffende) Unterschiede überwunden werden. An dieser Stelle setzt die Initiative »European Bridge-CA« an, die sich das Ziel gesetzt hat, die Vertrauenslücken sowohl zwischen existierenden als auch zu noch einzurichtenden PKIs pragmatisch zu überbrücken. Damit sollen sichere Transaktionen, z. B. sicherer E-Mail-Verkehr, über Unternehmensgrenzen hinweg ermöglicht werden /Pohl2001/.

neuKap07.fm Seite 251 Freitag, 18. Oktober 2002 3:52 15

Das Ziel der europäischen Bridge-CA-Initiative ist es, weltweit eine »Brücke des Vertrauens« zwischen unterschiedlichen PKIs herzustellen. Dazu müssen minimale Policy-Anforderungen und technische Vorbedingungen definiert werden, die sichere Kommunikation über organisatorische Grenzen hinweg erlauben. Gleichzeitig gilt es, ein gemeinsames Verständnis für den Gebrauch von digitalen Signaturen in Prozessen und Applikationen bei allen Beteiligten sicherzustellen.

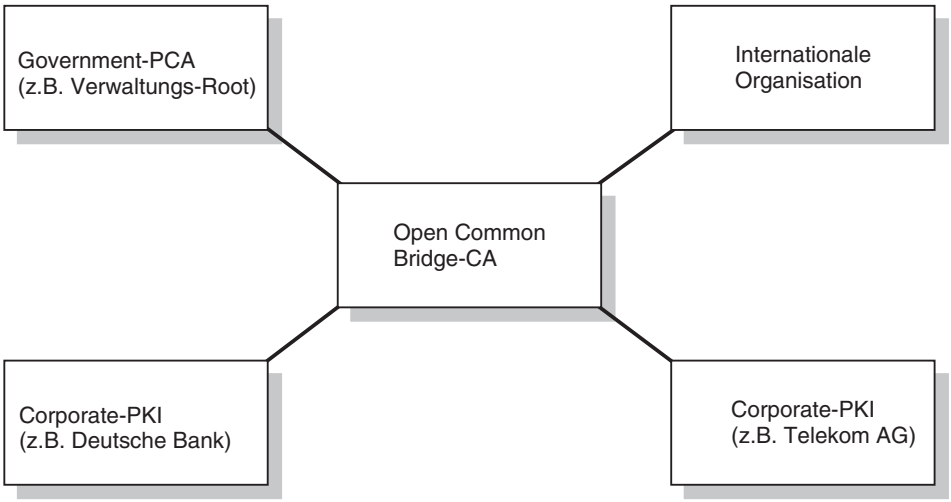


Abb. 7.19: Stern-Topologie der Bridge-CA

Die Bridge-CA-Initiative wurde von der Deutschen Bank und der Deutschen Telekom ins Leben gerufen. Nach kurzer Zeit wurde die industrielle Vereinigung TeleTrusT Deutschland e.V. Betreiber der Initiative, die zurzeit von über 20 großen Organisationen unterschiedlicher Industriezweige und der öffentlichen Verwaltung unterstützt wird. Sie ist eine herstellerunabhängige vom Nutzer angetriebene Non-Profit-Initiative. Im Zuge der gemeinsamen Standardisierung nimmt die Bridge-CA die Rolle eines neutralen Mittlers ein, der einerseits die unterschiedlichen Interessen aller Teilnehmer integriert und andererseits den Austausch von Erfahrungen sicherstellt. Die Praktikabilität, die Flexibilität der vereinbarten Lösungen und der Schutz der getätigten Investitionen in die Sicherheits-Infrastruktur stehen im Mittelpunkt der Aufmerksamkeit.

Die Initiative wird von einem internationalen Komitee mit Repräsentanten aus der Wirtschaft, der Verwaltung und der Wissenschaft überwacht. Dieses Komitee entscheidet, welche existierenden PKIs an die Bridge-CA angeschlossen werden und wie diese Integration stattfinden soll. Grundsätzlich sind alle hardware- und Software-basierten Zertifikate sowie alle Grade der Verbindlichkeit von Zertifikaten bis hin zu rechtsverbindlichem PKIs willkommen und zulässig.

neuKap07.fm Seite 252 Freitag, 18. Oktober 2002 3:52 15

Ausgehend von der weiten Verbreitung der Kommunikation via E-Mail hat die Bridge-CA-Initiative ihre kurzfristigen Bemühungen auf die Bereitstellung einfach handhabbarer PKI-Lösungen fokussiert, die diese Kommunikationsform sichern. Die folgenden Kapitel beschreiben daher die Architektur und technische Details dieses Ansatzes. Weitere Anwendungen wie Web-Zugriff, sicheres Einkaufen und Virtual Private Networks (VPNs) werden zu einem späteren Zeitpunkt folgen.

Im Januar 2001 hat die Bridge-CA den Betrieb aufgenommen und seither wurde ihre Anwendung stetig erweitert.

Konzeption und Design der Bridge-CA

Die meisten heute betriebenen CAs sind auf die Mitglieder einer einzelnen Organisation begrenzt. Obwohl erhebliche Kosten für die Entwicklung einer Firmen-CA investiert werden müssen, ist die Nutzbarkeit der digitalen Zertifikate auf den internen Gebrauch begrenzt. Aus technischen oder organisatorischen Gründen ist die Anwendung von Verschlüsselung und digitalen Signaturen über die Grenzen einer Organisation hinaus häufig nicht praktikabel. Um dieses Problem zu lösen, müssen zwei Bedingungen erfüllt werden:

- Der Empfänger einer Meldung muss in der Lage sein, die Gültigkeit des Zertifikats zu verifizieren. Folglich muss er auf die notwendigen Informationen des Zertifizierers (der CA) zugreifen können.
- Der Empfänger muss in der Lage sein, das Wurzelzertifikat der ausstellenden PKI zu identifizieren und daraufhin zu überprüfen, ob dieses Wurzelzertifikat gültig und vertrauenswürdig ist.

Die Bridge-CA ermöglicht dies, indem sie eine allgemeine Plattform zur Verfügung stellt, die die teilnehmenden CAs auf eine sichere, aber einfache Weise verbindet. Sie basiert auf einem standardisierten technischen und organisatorischen Regelwerk, das die Integration neuer CAs in die Bridge-CA-Infrastruktur erleichtert. Sobald ein neuer Teilnehmer (eine Firmen-, Organisations- oder Regierungs-PKI) sich anschließt, können alle Mitglieder seiner PKI mit allen Mitgliedern der anderen Bridge-CA-Partner sicher kommunizieren.

Das Bridge-CA-Konzept erlaubt es Empfängern von signierten oder verschlüsselten Nachrichten, die fremden Wurzelzertifikate einfach und sicher zu beziehen und deren Vertrauenswürdigkeit zu überprüfen. Um weder die Vertrauenswürdigkeit der teilnehmenden CAs noch die der Bridge-CA zu reduzieren oder gar zu gefährden, müssen alle Teilnehmer bestimmte Minimalanforderungen erfüllen und eine formale Registrierungsprozedur durchlaufen.

Um das Ziel der PKI-Interoperabilität auch kurzfristig zu erreichen, wurde bei der Implementierung der Bridge-CA auf bereits verfügbare Technologie zurückgegriffen. Obwohl die Verteilung der Zertifikate an die Teilnehmer und weiter innerhalb der Organisationen zunächst einen erhöhten Arbeitsaufwand verursacht, war es möglich, die Bridge-CA in kürzester Zeit produktiv zu machen.

neuKap07.fm Seite 253 Freitag, 18. Oktober 2002 3:52 15

Interoperabilität: Teilnahme an der Bridge-CA

Wenngleich der Anspruch, eine hochgradig sichere interne und externe Übertragung von E-Mails zu gewährleisten, einen bestimmten Grad an Interoperabilität hinsichtlich Technik und Policy notwendig macht, sind diese Anforderungen minimal gehalten worden, um einer breiten Klientel den einfachen und schnellen Zugang zu ermöglichen.

Folgende Mindestanforderungen werden an die Policy von Bridge-CA-Teilnehmern gestellt:

- Persönliche Identifikation und Registrierung des Zertifikatsinhabers
  Um die Kopplung zwischen einem öffentlichen Schlüssel und einer Person zu garantieren, wird die persönliche Identifikation und Registrierung des Zertifikatsinhabers gefordert. Massenregistrierung ist nur zulässig, wenn die jeweiligen Datenquellen vertrauenswürdig genug sind.
- Zugang zu Statusinformation des Zertifikats via CRLs oder OCSP
  Statusangaben zu Zertifikaten müssen sowohl für die Bridge-CA als auch für deren Teilnehmer zur Verfügung gestellt werden. Zu beachten ist, dass es nur notwendig ist, Statusangaben von jenen Zertifikaten zur Verfügung zu stellen, die extern benutzt oder verteilt werden.
- Die Distinguished Names in den Zertifikaten müssen eindeutig zugewiesen werden und dürfen sich nicht mit Namen anderer teilnehmender Organisationen überschneiden. Das ist für zukünftige Bridge-CA Entwicklungen besonders wichtig, da diese die Verkettung von Verzeichnissen und die Kreuzzertifizierung beinhalten wird.
- RSA Schlüssellänge von mindestens 1024 Bit
- Schlüsselgebrauch ist »Signature« und/oder »Encryption«

Während die folgenden Eigenschaften aktuell nicht zwingend für die Teilnahme an der Bridge-CA Initiative vorausgesetzt werden, müssen sie für die Teilnahme an weiteren Bridge-CA Entwicklungen erfüllt sein:

- Die CA-Software sollte PKCS #10 Zertifikatsanträge an die Bridge-CA ausgeben können.
- Das Verzeichnis des Teilnehmers sollte Attribute, die sich auf Kreuzzertifizierung beziehen, X.500-Verkettungen oder andere geeignete Verteilungsmechanismen verarbeiten können.
- Die E-Mail Clients sollten in der Lage sein, mit LDAPv3 (RFC2251)-Empfehlungen umzugehen.
  Die bisherige Forschung hat gezeigt, dass diese Anforderung wegfällt, wenn X.500 kompatible Verzeichnisse benutzt werden. Besonders wenn einige der Verzeichnisse der Teilnehmer nicht X.500-kompatibel sind, ist es wichtig, dass die E-Mail Clients mit LDAPv3-Referrals für den CRL-Bezug umgehen können. Deswegen arbeitet das NIST mit größeren Herstellern von Mail-Clients zusammen, um die aktuellen Mängel zu beheben.

neuKap07.fm Seite 254 Freitag, 18. Oktober 2002 3:52 15

Um der Bridge-CA als vertrauenswürdiger Partner beizutreten, muss ein zukünftiges Mitglied die folgenden Schritte absolvieren:

- **Untersuchung der Policy**
  Der erste Schritt ist die Überprüfung, ob die PKI des Beitrittskandidaten die minimalen Anforderungen an die Policy erfüllt, die vom Bridge-CA Board definiert wurden.

- **Kontaktaufnahme**
  Sobald die Überprüfung erfolgreich abgeschlossen wurde, kann der zukünftige Teilnehmer mit den Bridge-CA Executives in Kontakt treten. Ein Formular mit weiteren Informationen kann unter `http://www.bridge-ca.org`. bezogen werden.

- **Interoperabilitäts-Tests**
  Der nächste größere Schritt sind technische Interoperabilitäts-Tests mit der Bridge-CA. Dieser Prozess wird vom Personal der Bridge-CA unterstützt und ist gewöhnlich nicht sehr aufwändig.

- **Vertragsabschluss**
  Wenn die komplette Interoperabilität aller Schlüsselelemente der PKI sichergestellt ist, kann der zukünftige Teilnehmer den formalen Beitritt durch die Unterzeichnung des Teilnehmervertrags vollziehen.

- **Nutzung der signierten Zertifikatsliste**
  Damit ist das neue Mitglied betriebsbereit und kann sicher mit allen anderen Teilnehmern der Bridge-CA kommunizieren. Dazu müssen die Root-Zertifikate der anderen Teilnehmer in die eigene PKI eingefügt werden.

Weitere Aspekte der Bridge-CA

- **Standards**
  Trotz der weit reichenden Standards für verschiedene Elemente der PKI bleibt ein gewisser Grad an Interpretationsmöglichkeiten, die zu heterogenen Implementierungen führen. Diese Abweichungen im Detail stören die Interoperabilität oft empfindlich. Die Vereinbarung über ein gemeinsames Verständnis dieser Standards ist und bleibt essenziell.

- **Die Notwendigkeit eines Geschäftsmodells**
  Eine PKI zu implementieren, ist eine komplexe und kostspielige Aufgabe. Ein wesentlicher Erfolgsfaktor hierbei ist eine kontinuierliche Unterstützung durch den Markt. Die Investition in die Sicherheit muss sich bezahlt machen, das ist eine wesentliche Bedingung für ein solides Geschäftsmodell. Eine positive Kostenbilanz hängt stark von dem durch Sicherheit induzierten Optimierungspotenzial ab. Dieses Potenzial ist in der Automation und Optimierung von Geschäftsprozessen zwischen Organisationen am größten.

neuKap07.fm Seite 255 Freitag, 18. Oktober 2002 3:52 15

- **Konzentration auf das Wesentliche**
  Sicherheit ist eine umfassende Aufgabe. Jedes System hat Schwächen, die beseitigt werden können und müssen. Aber bevor man das System komplettiert, ist es ratsam, eine minimale Konfiguration fertig zu stellen und in den produktiven Betrieb zu überführen. Mit offenen Anforderungen kann man umgehen, während das System in Versionszyklen perfektioniert wird. So kann die Bridge-CA-Initiative eine ideale Basis für die pragmatische Entwicklung einer zeitgemäßen Sicherheitstechnologie sein.

Schlussfolgerungen

Die Bridge-CA bietet eine praktikable Lösung, um voneinander unabhängige PKIs zu verbinden. Nutzer dieser PKIs können sicher miteinander kommunizieren, indem sie Zertifikate anderer PKIs ohne Schwierigkeiten integrieren.

Obwohl die wichtigste Anwendung, die heute genutzt wird, sichere E-Mail ist, ist es in Zukunft durchaus möglich, dass die Bridge-CA-Infrastruktur auch für die Absicherung anderer Anwendungen verwendet wird. Die nächsten notwendigen Schritte zur Verbesserung der Bridge-CA sind die Einführung der Kreuzzertifizierung zwischen der Bridge-CA und ihren Teilnehmern, um den Verwaltungsüberhang zu reduzieren, und die Vereinfachung der Integration von zukünftigen Teilnehmern. Durch diese Weiterentwicklung kann sich die Zahl der potenziellen Teilnehmer vergrößern und die Initiative somit einen weiteren Aufschwung erhalten (siehe auch *http://www.bridge-ca.org*).

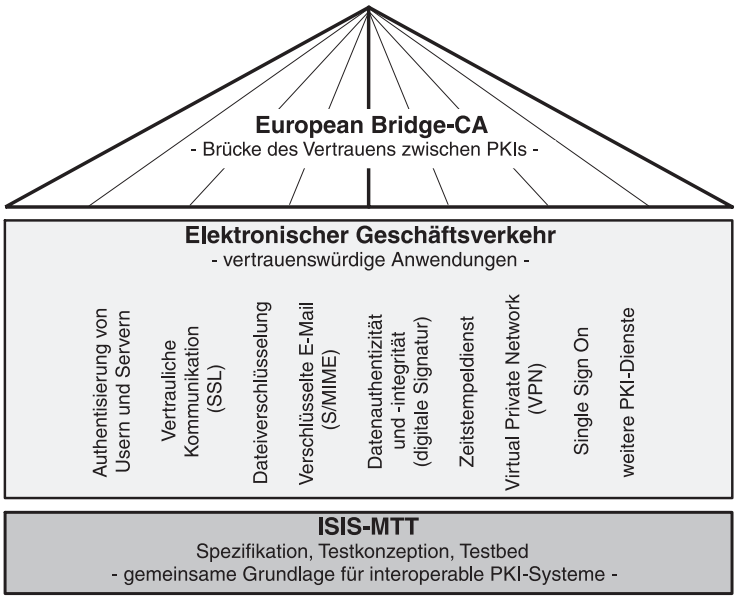


Abb. 7.20: Migration und Interoperabilität – ISIS-MTT und European Bridge-CA

neuKap07.fm Seite 256 Freitag, 18. Oktober 2002 3:52 15

7.3 Virtual Private Networks (VPN)

In diesem Kapitel werden allgemeine Aspekte von VPNs behandelt. Eine umfassende Darstellung dieses wichtigen Themas finden Sie im MITP-Fachbuch »Virtual Private Networks« von Markus a Campo und Norbert Pohlmann /aCam2001/.

7.3.1 Grundlagen

Die grundsätzliche Idee von Virtual Private Networks (VPNs) ist, die Vorteile einer offenen Kommunikationsinfrastruktur zu nutzen – z.B. der kostengünstigen, weltweit verfügbaren »shared infrastructure« des Internets –, aber dabei allen Gefährdungen der Informationssicherheit sinnvoll und angemessen entgegenzuwirken.

Ein VPN soll gewährleisten, dass sensible Daten während der Übertragung über Netzwerke (LANs und WANs, private und/oder öffentliche Netze) vertrauenswürdig übertragen werden, sodass nur die dazu berechtigten Personen auf die sensiblen Daten zugreifen können. Damit diese Ziele erreicht werden, setzt man kryptographische Verfahren und andere Sicherheitskomponenten ein. VPN-Systeme können entweder vollständig im Verantwortungsbereich einer Organisation liegen oder auch unterschiedliche Verantwortungsbereiche über eine gemeinsame bzw. öffentliche Sicherheitsinfrastruktur miteinander verbinden.

Zum Begriff »V... P... N...«

- **»Virtual«** bedeutet, dass es sich – aus Anwendersicht – scheinbar um nur »ein« Netzwerk handelt, auch wenn sich viele reale Teilnetzwerke hinter »einem« VPN verbergen.
- **»Private«** bedeutet, dass die Kommunikation vertrauenswürdig – also nicht öffentlich – durchgeführt und das Risiko eines Schadens bei der Übertragung minimiert wird.
- **»Network«** bedeutet, dass eine definierte Gruppe von Rechnersystemen miteinander verbunden wird und mithilfe eines Protokolls (typischerweise ist das die TCP/IP-Protokollfamilie) kommuniziert.

Analogien

Um die grundsätzliche Idee eines VPN zu verdeutlichen und so das Verständnis zu erleichtern, werden im Folgenden zwei Analogien erläutert: zum einen ein Sicherheitstransporter und zum anderen eine Pipeline. Beide schützen die zu übertragenden Werte elektronisch vor Diebstahl, Einsichtnahme und Veränderung.

neuKap07.fm Seite 257 Freitag, 18. Oktober 2002 3:52 15

- **Sicherheitstransporter**
  Anders als normale LKWs, bei denen die zu transportierenden Werte nicht explizit geschützt sind, dient ein Sicherheitstransporter dazu, die auszutauschenden Werte während des Transports wirkungsvoll gegen Angriffe zu schützen. Dabei nutzen die Organisationen die gemeinsame öffentliche Infrastruktur der Straßen (Landstraßen, Autobahnen etc.), ohne eine eigene Infrastruktur (Privatstraßen) aufbauen zu müssen.

  Entsprechend dient ein VPN dazu, Daten (elektronische Werte, so genannte E-Assets) sicher über die öffentliche Infrastruktur von Netzwerken (LANs und WANs) zu transportieren, ohne dass Unbefugte die Daten einsehen oder manipulieren können.

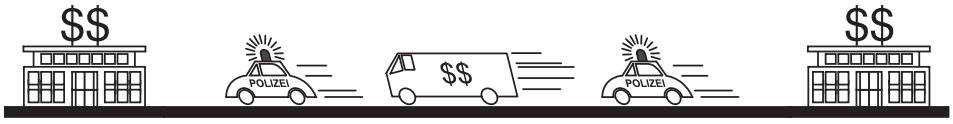


Abb. 7.21: Sicherheitstransporter

- **Pipeline und Rohrpost**
  Durch eine Pipeline werden Güter, z. B. Öl, sicher von einem festgelegten Ort zu einem anderen transportiert. Zum Beispiel unterhält die NATO das – in der Öffentlichkeit weitgehend unbekannte – Central European Pipeline System (CEPS); es ist das weltweit umfangreichste und komplizierteste militärische Kraftstoffversorgungssystem.

  Durch Beobachtung einer Pipeline kann man allenfalls erkennen, wie hoch der absolute Durchfluss ist, nicht aber, woher der Inhalt stammt und wohin er gelangt.

  Bei einem VPN muss zwischen allen Endpunkten sichergestellt sein, dass tatsächlich alle Daten durch die »VPN-Pipeline« laufen, d. h., dass sie nicht abgezweigt werden können, und dass kein Unbefugter in die »VPN-Pipeline« eindringen kann.

  Schon vor mehr als 100 Jahren wurde der Pipeline-Ansatz für die gesicherte Übertragung von Schriftgut – also von Information – verwendet: Die Rohrpost in Berlin und anderen Großstädten hatte ihre Blütezeit zwischen 1875 und 1945. Seine größte Ausdehnung hatte das Berliner Netz 1944 mit mehr als 300 offiziellen und rund 100 streng geheimen Kilometern /Arno2000/.

  Auch heutzutage befördern Rohrpostanlagen – meist aber nur innerhalb von Unternehmen – Bargeld, Schecks, Dokumente, gefährliche Güter oder auch »nur« Produktionsmittel (übrigens bis 15 kg Gewicht, 30 cm Durchmesser, kilometerweit und bis zu 90 km/h schnell).

neuKap07.fm Seite 258 Freitag, 18. Oktober 2002 3:52 15

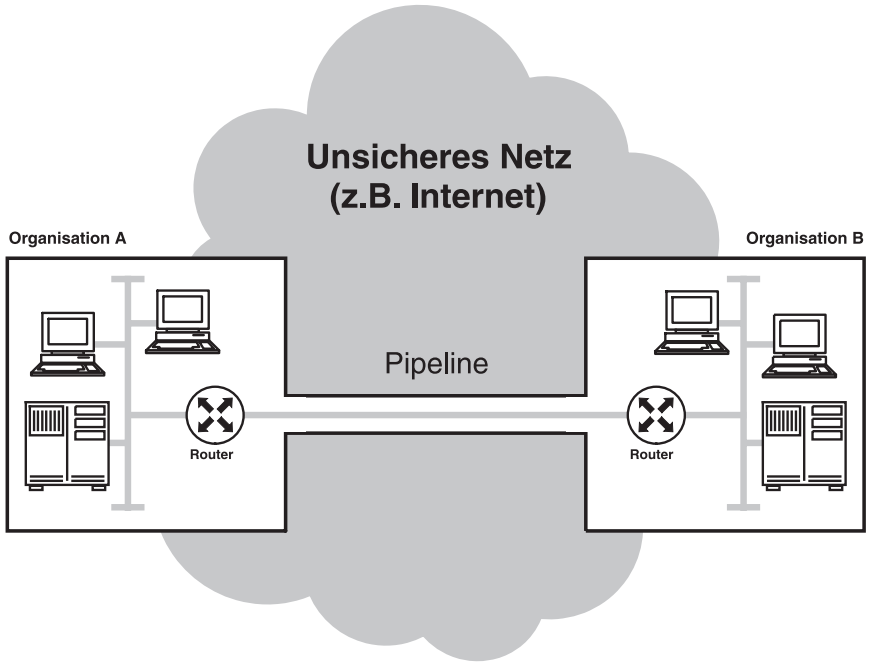


Abb. 7.22: Pipeline

Es ist dabei nicht möglich, durch die Beobachtung einer Rohrpost-Hauptleitung zu erkennen, wie sich die Werte bei den Absendern zusammenstellen und bei den Empfängern wieder aufteilen. Außerdem können die Sendungen durch eine Versiegelung der Transportbehälter zusätzlich geschützt werden.

- **Tunnel**
  Der Vollständigkeit halber sei hier auch der Begriff »Tunnel« erwähnt, der insbesondere in der amerikanischen Fachliteratur verwendet wird (»tunneling«). Diese Analogie bedeutet »Zugriffsschutz« – wie bei der virtuellen Pipeline durch das Internet.

Sicherheitstechniken von VPNs

Um die Daten auf ihrem Weg über öffentliche Kommunikationsnetze so zu schützen, dass die Vertraulichkeit und Informationssicherheit eines privaten Netzwerks gewahrt bleibt, werden in VPNs folgende Sicherheitsmechanismen verwendet:

- Verschlüsselung
- Authentikation
- Digitale Signaturen für die Unversehrtheit der Daten
- Tunneling
- Firewalling

neuKap07.fm Seite 259 Freitag, 18. Oktober 2002 3:52 15

7.3.2 Anwendungsformen von VPNs

Verschiedene Anwendungsformen von VPNs stellen spezifische Anforderungen hinsichtlich Connectivity (Verbindlichkeit), Verfügbarkeit, Datendurchsatz, Einsatz von Standards und Schlüsselmanagement. Optimal wäre ein VPN, das alle Anforderungen abdeckt und auch den unterschiedlichen Ansprüchen an die Kosten gerecht wird.

Unternehmensweites VPN

Darunter versteht man »private« Netzwerkverbindungen zwischen verschiedenen LAN-Standorten eines Unternehmens (Zentrale und Niederlassungen), die dazu dienen, Unternehmensdaten vertrauenswürdig über ein unsicheres Netz wie das Internet austauschen zu können. Hier spielt die Transparenz der Lösung eine wichtige Rolle.

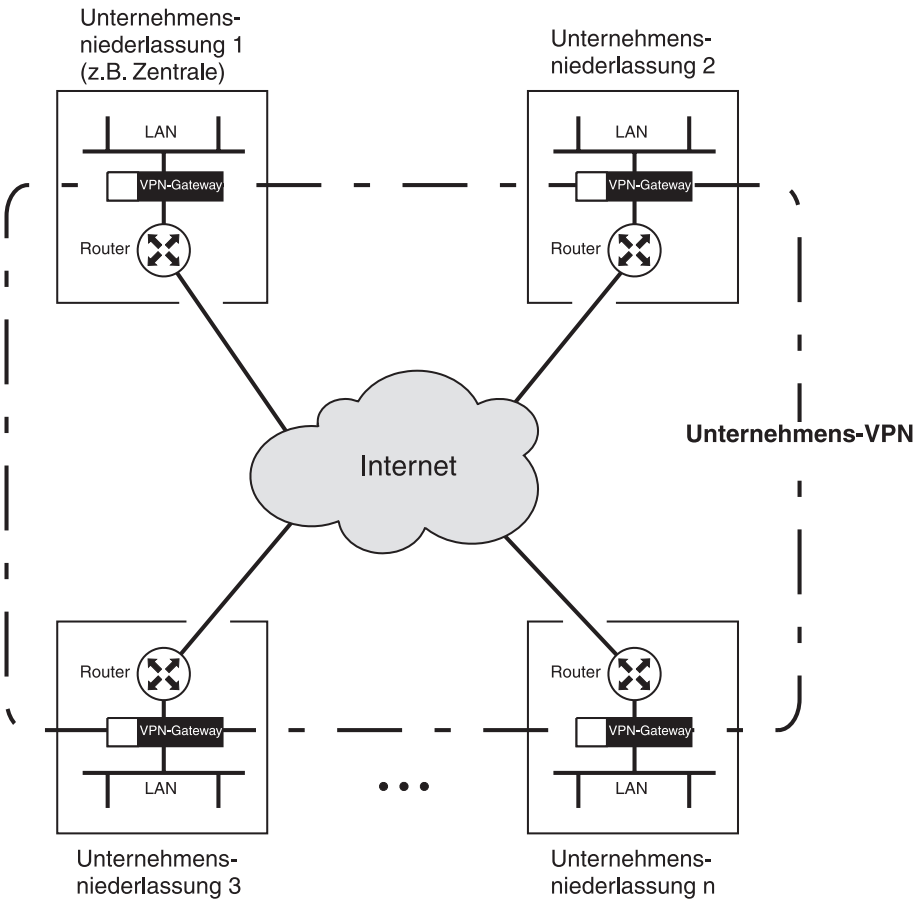


Abb. 7.23: Unternehmensweites VPN

neuKap07.fm Seite 260 Freitag, 18. Oktober 2002 3:52 15

Sichere Remote-Ankopplung

Heim- und/oder Mobil-Arbeitsplätze greifen innerhalb eines VPN über ein öffentliches Netzwerk (z. B. das Internet) geschützt auf die zentral gespeicherten Unternehmensdaten zu. Hier spielt die Identifikation und Authentikation des Nutzers, der auf die Daten zugreifen möchte, eine besondere Rolle.

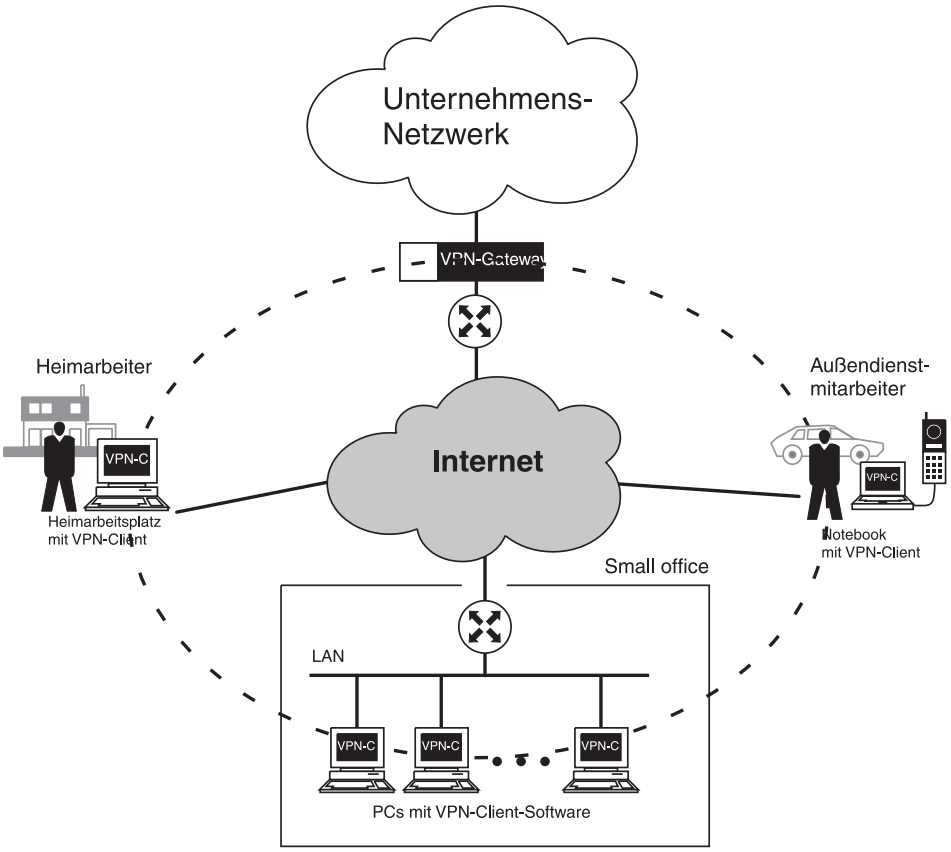


Abb. 7.24: Remote-Ankoppelung mithilfe eines VPN

VPN zwischen verschiedenen Unternehmen

In einer definierten Gruppe von Unternehmen – beispielsweise von Automobilherstellern und -zulieferern – können alle Partner miteinander mithilfe von VPNs eine vertrauenswürdige, untereinander und nach außen hin geschützte Kommunikation realisieren. Hier spielt das unternehmensübergreifende Sicherheitsmanagement eine besondere Rolle.

neuKap07.fm Seite 261 Freitag, 18. Oktober 2002 3:52 15

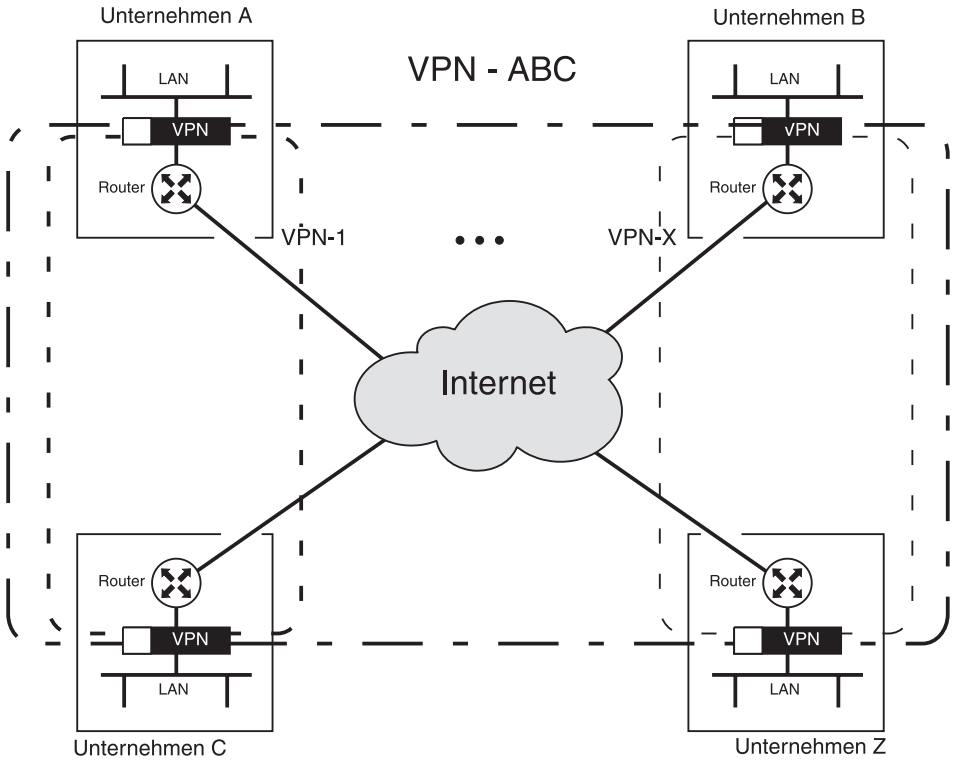


Abb. 7.25: Kooperatives VPN verschiedener Unternehmen

Kombinationen der Anwendungsformen

Natürlich gibt es auch Kombinationen der oben beschriebenen Anwendungsformen. Wichtig ist hierbei die Verwendung eines einheitlichen Standards und die Möglichkeit eines flexiblen und unternehmensübergreifenden Sicherheitsmanagements.

neuKap07.fm Seite 262 Freitag, 18. Oktober 2002 3:52 15

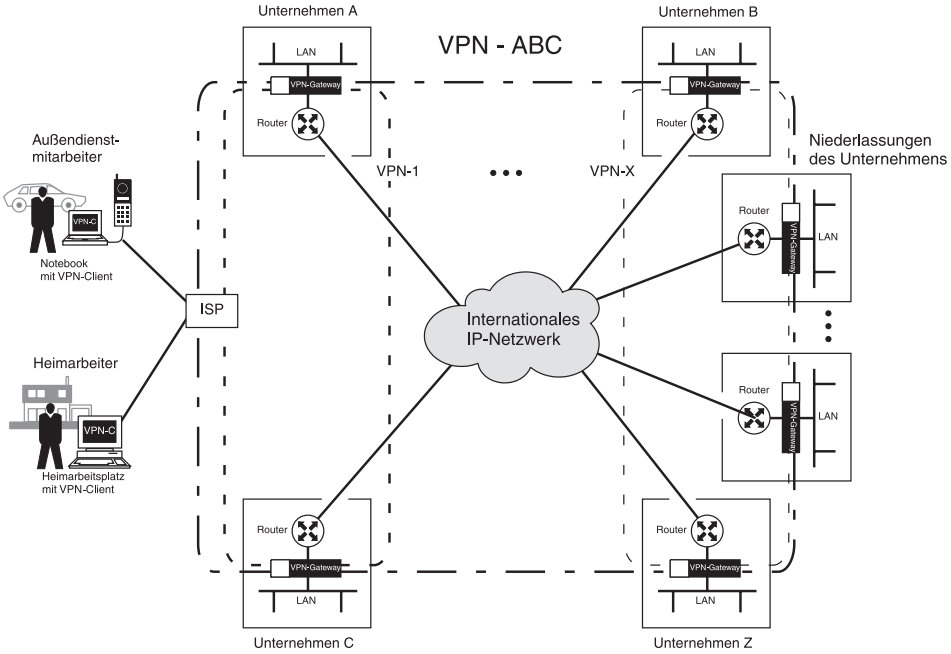


Abb. 7.26: VPN-Kombinationen

7.4 Secure Socket Layer (SSL)

Das von Netscape entwickelte Protokoll SSL wird auch TLS (Transport Layer Security) bezeichnet. Es setzt auf der Transportschicht des Netzwerk-Stack auf. Prinzipiell könnte es mit jedem Protokoll dieser Ebene kooperieren, doch in der Praxis sind nur Implementierungen für TCP bekannt.

SSL nimmt alle für Authentikation, Vertraulichkeit und Unversehrtheit der Daten benötigten Aufgaben wahr. Dazu verhandeln Client und Server über Algorithmen zur Datenkompression, Verschlüsselung und digitalen Signatur. Basis dieser »Vorverhandlungen« sind öffentliche Schlüssel des Servers und optional des Clients, die mithilfe von Zertifikaten über Zertifizierungsinstanzen (Certification Authorities, CAs) bestätigt werden. Wie bei VPNs werden asymmetrische Verfahren (Public-Key-Algorithmen) mit symmetrischen Verfahren kombiniert.

Beschreibung des Verfahrens

SSL ist ein zustandsbehaftetes Protokoll. Mit ihm können zwischen zwei Rechnern ein oder mehrere Sitzungen aufgebaut werden, die ihrerseits jeweils eine oder mehrere Verbindungen enthalten können. Die Nutzdaten werden vor dem Senden fragmentiert, komprimiert, um eine digitale Signatur ergänzt und verschlüsselt.

neuKap07.fm Seite 263 Freitag, 18. Oktober 2002 3:52 15

Der Empfänger kehrt die Reihenfolge der Operationen um und führt die Nutzdaten der nächsthöheren Ebene des Netzwerkstacks zu. Diese Aufgaben werden im SSL Record Layer wahrgenommen.

Zusätzlich zu diesem transparenten Teil setzen auf dem SSL Record Protocol drei weitere Protokolle auf, die aber nicht in höhere Schichten übermittelt werden:

- Das *SSL Handshake Protocol* nimmt interne SSL-Kommunikations- und Verwaltungsaufgaben auf den beteiligten Rechnern wahr, wie etwa die (gegenseitige) Authentikation oder die Wahl des Verschlüsselungsverfahrens.
- Das *»change cipher spec«-Protokoll* teilt dem Partner den Wechsel in den zuvor ausgehandelten Verschlüsselungsalgorithmus mit. Vom Prinzip her hätte dieses Protokoll in die Familie des SSL Handshake gehört, doch bestünde dann die Gefahr von Deadlocks.
- Das *Alert Protocol* schließlich wird im Fehlerfall aktiv.

Zum Austausch von Schlüsseln während des Handshakes stehen die Verfahren RSA, Diffie-Hellman und Fortezza zur Verfügung.

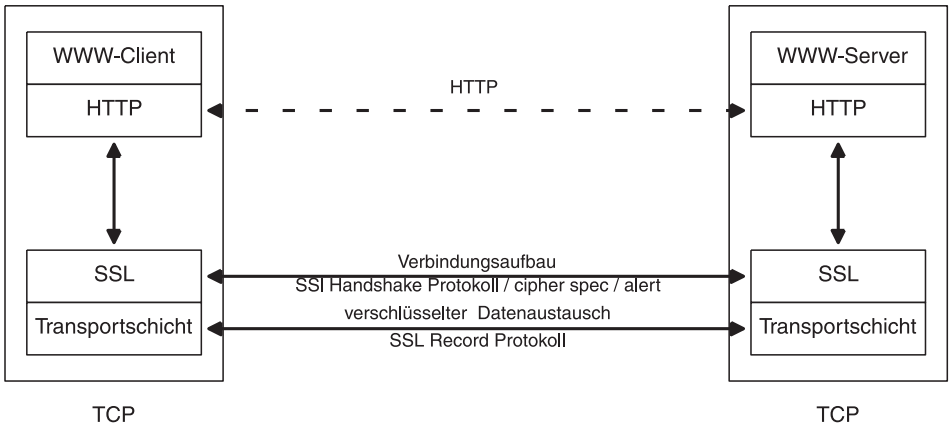


Abb. 7.27: Das Prinzip von SSL

Die SSL-Kommunikation wird über reservierte TCP/IP-Ports abgewickelt:

- Port 443 lässt SSL-Verbindungen zu Web-Servern zu. Diese Art der Verbindung ist die am häufigsten implementierte.
- Port 465 ist für SSL in Verbindung mit dem E-Mail-Protokoll SMTP reserviert.
- Port 563 schließlich ist für SSL in Verbindung mit Newsgroups reserviert.

neuKap07.fm Seite 264 Freitag, 18. Oktober 2002 3:52 15

Hier zeigt sich der Unterschied zwischen SSL und einer allgemeinen VPN-Definition: Ein VPN stellt eine für die verschiedenen Applikationen transparente Netzwerkverbindung zwischen beliebigen Netzwerkknoten her. Das sitzungsorientierte SSL ist hingegen nur für bestimmte Client Server-Applikationen definiert, mit denen die wichtigsten Dienste im Internet abgedeckt werden (für weitere Informationen siehe Anhang A2).

SSL hat drei grundlegende Protokollfunktionen:

- SSL Server Authentication
  Der Teilnehmer (Client) ist in der Lage, den Server zu authentisieren.
- SSL Client Authentication
  Der Server ist in der Lage, den Client zu authentisieren (siehe auch Kap. 8).
- Verschlüsselte SSL-Verbindung
  Es findet eine verschlüsselte Kommunikation zwischen Client und Server statt.

Umsetzungskonzept

Eine explizite Datenschutzanforderung lautet, die Kommunikation zwischen Client und Server vertraulich zu gestalten, damit die ausgetauschten Daten weder mitgelesen noch manipuliert werden können (z. B. für Homebanking, Depotabfragen etc.).

Alle hierfür notwendigen Voraussetzungen sind gegeben. Die technische Infrastruktur für SSL ist bereits heute schon vorhanden, Clients (Web-Browser) unterstützen den Standard, Web-Server sind für die SSL-Verschlüsselung vorbereitet und PKIs (VeriSign, GlobalSign etc.) stehen zur Verfügung. Dem Markt stehen etablierte SSL-Bibliotheken als Open Source zur Verfügung und auch die Industrie hat den Markt erkannt: SSL-Accelerator-Lösungen für die Beschleunigung der gesicherten Verbindung stehen bereit.

Stellt man den Aspekt der leichten Anwendbarkeit (integrierte Zertifikate in Browsern) in den Mittelpunkt, so müssen selbstverständlich die Sicherheitsanforderungen dagegen abgewogen werden. Nach Abschluss dieser Analyse wird eine Vielzahl von Organisationen feststellen, dass die Umsetzung der o. g. Anforderungen zeitnah und problemlos möglich ist.

SSL zur verschlüsselten Kommunikation zwischen Client und Firewall-Systemen

Um den geschützten Zugriff von Heim- und Mobil-Arbeitsplätzen über ein unsicheres Netz wie das Internet auf Unternehmensdaten zu ermöglichen, kann eine SSL-Realisierung in das Firewall-System integriert und diesem ein Server-Zertifikat zugewiesen werden, welches entsprechend im Browser unterstützt wird.

neuKap07.fm Seite 265 Freitag, 18. Oktober 2002 3:52 15

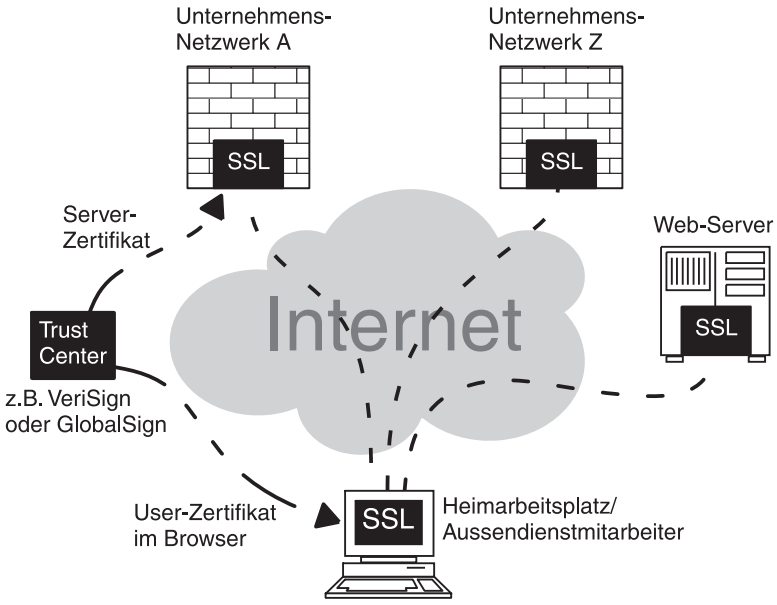


Abb. 7.28: SSL-verschlüsselte Kommunikation zwischen Client und Firewall-Systemen

7.5 Virtual Private Networks, Secure Socket Layer und Firewall-Systeme

Durch ein VPN oder eine SSL-Verbindung werden die Daten statt im Klartext in verschlüsselter Form über die Kommunikationsnetze übertragen. Vor einem Firewall-System muss eine Entschlüsselung stattfinden, damit das entsprechende Firewall-Element in der Lage ist, die Analysen der Kommunikationsdaten oberhalb der Netzzugangs- bzw. Netzwerkebene durchzuführen.

Die Einbindung von Verschlüsselungs-Systemen wie z. B. IPSec oder SSL dient nicht nur dazu, die Vertraulichkeit der Daten zu sichern. Sie kann auch dazu beitragen, weitere konzeptionelle Unsicherheiten von Firewall-Systemen, z. B. Trittbrettfahrer oder die gezielte Manipulation von Datenpaketen, auszuschließen (siehe auch *»Theoretische Grundlagen von Firewall-Systemen«*, Kap. 14.5.12 und 14.6).

Der Zusammenhang von Firewall-Systemen und Verschlüsselung (VPN oder SSL) ist insofern wichtig, als dass damit eine hohe Gesamt-Sicherheit für die Kommunikation über das Internet gewährleistet werden kann.

Verschlüsselung als Schutzmaßnahme gegen Trittbrettfahrer

Im Folgenden wird der Angriff eines Trittbrettfahrers (»Man-in-the-middle-Attack«) auf ein Firewall-System veranschaulicht und gezeigt, wie ein derartiger Angriff durch Verschlüsselung verhindert werden kann /Rula94/.

neuKap07.fm Seite 266 Freitag, 18. Oktober 2002 3:52 15

Die Workstation darf durch das unsichere Netz kontrolliert über das Firewall-System auf den Server im zu schützenden Netz zugreifen. Dazu muss der Benutzer zuerst eine Identifikation und Authentikation mit dem Firewall-System durchführen. Nach erfolgreicher Ausführung der Authentikation kann er innerhalb des ihm erlaubten Zeitrahmens die Dienste nutzen, zu denen er berechtigt ist. Hier liegt ein potenzieller Angriffspunkt verborgen: Ein Angreifer aus dem unsicheren Netz kann die bestehende Verbindung des Benutzers aus dem unsicheren Netz übernehmen und ist damit als Trittbrettfahrer in der Lage, die gleichen Aktionen auszuführen wie der berechtigte Benutzer.

Dieses Risiko kann dadurch minimiert werden, dass die Kommunikation zwischen der Workstation und dem Firewall-System in verschlüsselter Form stattfindet. Ein Angreifer aus dem unsicheren Netz kann dann zwar auch noch die Verbindung übernehmen; da er sich jedoch nicht kryptographisch korrekt darstellen kann (er hat keinen Zugriff auf den geheimen Schlüssel), ist er nicht in der Lage, die IP-Pakete so aufzubereiten, dass sie vom Packet Filter mit Verschlüsselungsfunktion richtig entschlüsselt werden.

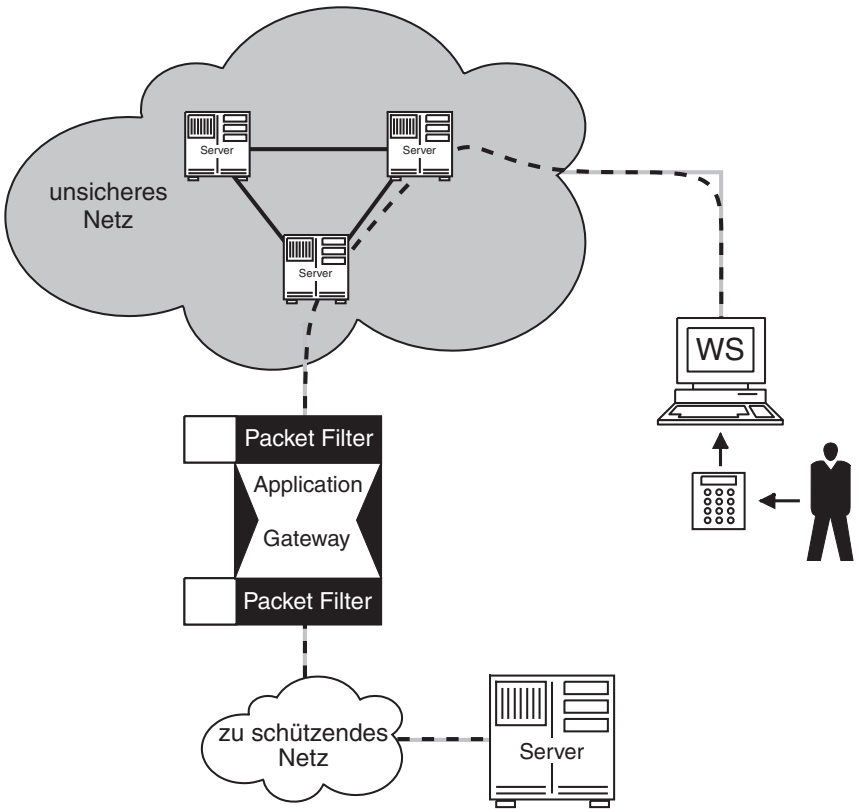


Abb. 7.29: Trittbrettfahrer über ein Firewall-System

neuKap07.fm Seite 267 Freitag, 18. Oktober 2002 3:52 15

Verschlüsselung als Schutzmaßnahme gegen die gezielte Manipulation von Protokollelementen

Durch die Verschlüsselung der Protokollelemente kann ein Angreifer während der Übertragung nicht mehr unmittelbar erkennen, welche Aktion mit einem bestimmten Protokollelement ausgelöst werden soll. Damit ist er auch nicht mehr in der Lage, das Protokollelement so zu beeinflussen, dass eine andere als die gewünschte Aktion durchgeführt wird. So kann die Unsicherheit ausgeschaltet werden, dass Aktionen durchgeführt werden, die zwar erlaubt sind, aber vom eigentlichen Absender nicht gewollt waren /PoRi95/.

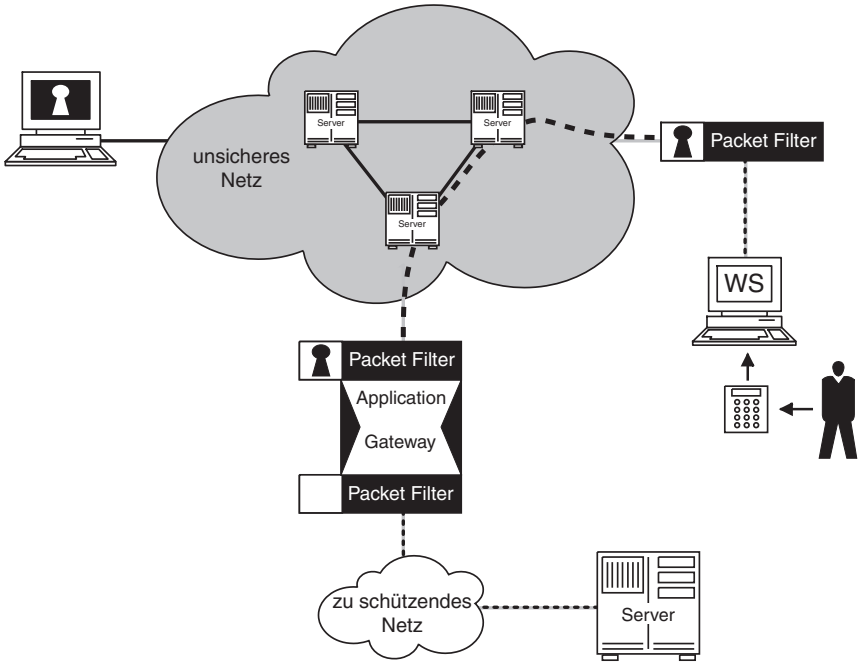


Abb. 7.30: Verschlüsselte Kommunikation gegen Trittbrettfahrer

7.6 Vergleich zweier Konzepte: E-Mail Security versus VPN/SSL-Sicherheit

VPN-Lösungen werden in Form von Black Boxes oder Security Sublayers mit einem Security Management in das Kommunikationssystem integriert. VPNs sind immer dann besonders sinnvoll, wenn die zu schützende Kommunikation innerhalb eines einzigen Verantwortungsbereichs stattfindet, wie dies z. B. bei Intranet-Anwendungen und daran angekoppelten Organisationseinheiten der Fall ist. In diesem Verantwortungsbereich gilt ein und dieselbe Sicherheitspolitik, die unab-

neuKap07.fm Seite 268 Freitag, 18. Oktober 2002 3:52 15

hängig von anderen Vorgaben durchgesetzt wird und damit ein Höchstmaß an Sicherheit garantiert, insbesondere durch Abschottung zu anderen Systemen. VPNs werden üblicherweise im E-Business-Bereich verwendet.

SSL-Lösungen werden auf Client-Seite z.B. im Web-Browser verwendet und als integrale Lösung in Firewall-Systeme eingebunden. Die notwendigen Server-Zertifikate werden von Trustcenter-Anbietern wie VeriSign oder GlobalSign genutzt, um das Security Management einfach realisieren zu können. SSL wird im E-Commerce-Bereich verwendet, da auf eine übergeordnete Public Key Infrastructure zurückgegriffen werden kann. SSL spielt für den Datenschutz eine große Rolle, weil damit personenorientierte Kommunikation vertrauenswürdig realisiert werden kann.

Bei der E-Mail-Sicherheit wird den besonderen Sicherheitsanforderungen von Kommunikationspartnern in verschiedenen Verantwortungsbereichen Rechnung getragen. Die gemeinsame Sicherheitsinfrastruktur wird dabei durch Zertifizierungsinstanzen, die öffentliche Zertifikate zur Verfügung stellen, sowie durch personalisierte Chipkarten geschützt. Ein Anwendungsbeispiel ist die Kommunikation mit Banken, Steuerberatern, Ärzten usw. Eine Abschottung, d.h. ein kontrollierter Übergang von einem unsicheren zu einem zu schützenden Netz, ist in diesem Konzept nicht enthalten und muss ggf. durch andere Sicherheitskomponenten realisiert werden.

7.7 Firewall-Systeme versus VPN/SSL-Systeme

Der Sicherheitsmechanismus Firewall-System wirkt gegen den unerlaubten Zugriff auf die eigenen Rechnersysteme. Die unerlaubte Einsicht der Informationen während der Kommunikation und andere Angriffe müssen ggf. mithilfe zusätzlicher Verschlüsselung verhindert werden (siehe auch *»Theoretische Grundlagen von Firewall-Systemen«*, Kap. 14.5.12 und 14.6).

Grundsätzliche Unterschiede von Firewall- und VPN/SSL-Systemen

In diesem Abschnitt werden die grundsätzlichen Unterschiede von Firewall- und VPN/SLL-Systemen dargestellt.

- **Geltungsbereich**
  - *Firewall-Systeme* schützen eine Organisationseinheit.
  - *VPN/SSL-Systeme* schützen die Kommunikation mehrerer Einheiten (Kommunikationspartner) untereinander.

  Typischerweise werden Firewall-Systeme hinter die VPN-Gateways geschaltet und die SSL-Verschlüsselung im Firewall-System integriert. Die SSL-Verschlüsselung wird im E-Commerce-Bereich verwendet, die VPN-Verschlüsselung im E-Business-Bereich.

neuKap07.fm Seite 269 Freitag, 18. Oktober 2002 3:52 15

- **Ziele**
  - *Firewall-Systeme* schützen vor unerlaubtem Zugriff auf Rechnersysteme und deren Dienste und Daten. Hacker, Cracker, Spione und sonstige Angreifer werden aktiv abgehalten und erlaubte Kommunikationsverbindungen werden auf das für die Aufgabenstellung notwendige Maß reduziert.
  - *VPN/SSL-Systeme* schützen vor unerlaubtem Zugriff auf die Daten während der Übertragung zwischen definierten Kommunikationspartnern.

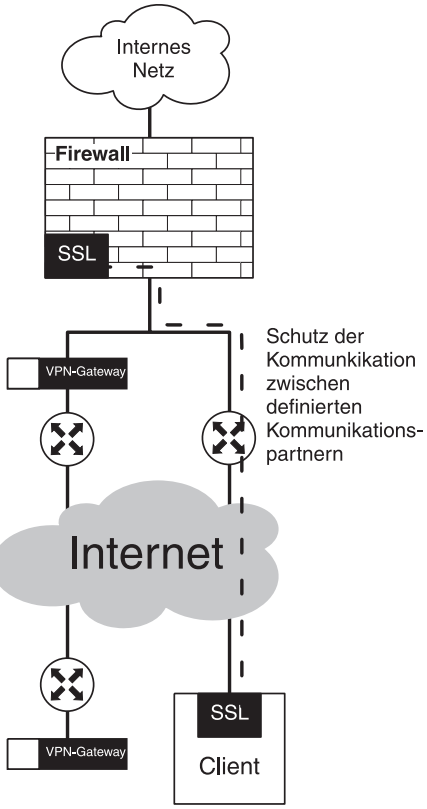


Abb. 7.31: Geltungsbereiche von SSL, VPNs und Firewall-Systemen

- **Unabhängigkeit**
  - Ein besonderer Aspekt bei *Firewall-Systemen* ist, dass sie lokal verwaltet werden können, d.h., bezogen auf die Kommunikationsmöglichkeiten und die Protokollierung kann die eigene lokale Sicherheitspolitik unabhängig von anderen realisiert werden.
  - Bei *VPN/SSL-Systemen* muss die Sicherheitspolitik in Übereinstimmung mit den Kommunikationspartnern realisiert werden, damit eine einheitliche Sicherheit gewährleistet werden kann.

neuKap07.fm Seite 270 Freitag, 18. Oktober 2002 3:52 15

Einige Hersteller bieten in ihren VPN- oder SSL-Lösungen auch Firewall-Funktionalitäten. Diese müssen dann aber auch den Kriterien für den sicheren Aufbau von Firewall-Systemen genügen /Pohl2001a/.

neuKap08.fm Seite 271 Freitag, 18. Oktober 2002 3:52 15

Kapitel 8

Authentikationsverfahren

In diesem Abschnitt werden Authentikationsverfahren exemplarisch dargestellt und diskutiert, die für die Überprüfung der Echtheit der Benutzer, die über ein Firewall-System kommunizieren wollen, verwendet werden können.

8.1 Identifikation und Authentikation

Woher weiß ein Firewall-System, dass Benutzer A, der eine Kommunikationsbeziehung aufbauen möchte, tatsächlich Benutzer A ist?

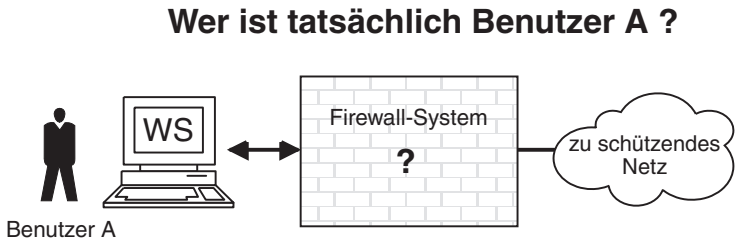


Abb. 8.1: Authentikation der Benutzer

Wenn ein Benutzer eine Kommunikationsverbindung über das Firewall-System aufbauen möchte, muss er sich dem Firewall-System gegenüber

- identifizieren und
- authentisieren.

Die Identifikation ist die Überprüfung eines vorgelegten, kennzeichnenden Merkmals, z. B. des Benutzernamens. Eine Person wird eindeutig durch die Angabe von Vorname, Nachname, Geburtsort und Geburtstag identifiziert. In Deutschland wird die Eindeutigkeit der Identifikation von den Standesämtern garantiert.

Eine Identifikation muss immer innerhalb eines Systems (Organisation) abgesprochen sein, damit sie eindeutig ist. Damit eine solche Absprache mit verschiedenen Benutzern zustande kommt, müssen klar definierte Regeln eingehalten werden.

neuKap08.fm Seite 272 Freitag, 18. Oktober 2002 3:52 15

Ein Beispiel für ein Konzept eindeutiger, kennzeichnender Namen oder »distinguishing identifier« sind die »directory names« aus der CCITT »Recommendation« X.509 bzw. ISO 9594-8 /CCITT/.

Authentikation bezeichnet einen Prozess, in dem überprüft wird, ob »jemand« oder »etwas« echt oder berechtigt ist. Authentikation bedeutet die Verifizierung (Überprüfung) der Echtheit bzw. der Identität. Die Überprüfung des Personalausweises einer Person ist eine solche Authentikation.

Was muss und kann nun innerhalb eines Firewall-Systems identifiziert und authentisiert werden?

- Kommunikationspartner: z. B. Benutzer, Prozesse, Instanzen, das Security Management
- Kommunikationsmedien: z. B. Workstation, Server-Systeme, Firewall-Elemente (Packet Filter, Application Gateway, Proxy, Security Management), Security Token usw.
- Nachrichten: z. B. Mails, Dateien, Java-Applets usw.
- Autorisationen: z. B. Rechte von Benutzern (Uhrzeit/Wochentag, Dienste, Befehle, Rechnersysteme), Zuständigkeiten (z. B. Rollen beim Security Management) usw.

Es gibt einige Anwendungen wie z. B. »elektronisches Geld«, bei denen die Authentikation von Benutzern (Personen) nicht erwünscht ist /Chau87/; daher sollte der Begriff »Identifikation« als der allgemeinere Begriff aufgefasst werden. Es ist zu bedenken, dass auch ein Anonym oder Pseudonym identifiziert und authentisiert werden muss.

Ablauf von Identifikation und Authentikation im täglichen Leben

Zwei Personen A und B, die in verschiedenen Organisationen arbeiten, wollen sich zwecks einer Absprache treffen. Dazu fährt Person A zu Person B. An der Pforte der Organisation, in der Person B arbeitet, wird Person A aufgefordert, eine Besucheranmeldung auszufüllen. Anhand ihrer Angaben (Name, Wohnort, Geburtsdatum, Organisation usw.) wird die Person identifiziert. Mithilfe ihres Personalausweises wird die Echtheit der Identifikation überprüft, d. h. die Person A wird authentisiert. Nun wird Person B vom Pförtner gerufen und die Kommunikation kann beginnen. Die Authentikation von Person B findet indirekt statt: Person B befindet sich im Gebäude einer Organisation und wird vom Pförtner gerufen.

Wenn die Personen A und B über ein rechnergestütztes Kommunikationssystem eine Kommunikation durchführen wollen, benötigen sie Sicherheitsmechanismen, mit denen eine Identifikation und nachfolgend eine Authentikation durchgeführt werden können.

neuKap08.fm Seite 273 Freitag, 18. Oktober 2002 3:52 15

8.2 Generelle Authentikationsverfahren

Für die Authentikation von Benutzern an Firewall-Systemen sind unterschiedliche Authentikationsverfahren möglich.

8.2.1 Passwort-Verfahren

Das einfachste Authentikationsverfahren ist das Passwort-Verfahren. Bei diesem Verfahren wird ein Passwort (String) zwischen dem Benutzer und dem Firewall-System abgesprochen. Der Benutzer weist seine Identität nach, indem er dem Firewall-System beim Authentikationsprozess das Passwort sendet, d.h., der Benutzer authentisiert sich dadurch, dass er das Passwort besitzt und es dem Firewall-System zeigt. Falls das Passwort falsch ist, wird er abgelehnt. Die Stärke dieses Authentikationsverfahren beruht letztlich auf der Geheimhaltung und der Qualität des Passwortes.

Wenn dieses Passwort in der Authentikationsphase im Klartext über das Netz (z.B. Internet) übertragen wird, kann es von Angreifern mitgelesen und missbräuchlich verwendet werden (siehe Kapitel 4.5 *Angriffsmethoden und prinzipielle Gegenmaßnahmen auf der Grundlage der TCP/IP-Protokolle*). Aus diesem Grund darf das Passwort-Verfahren auf keinen Fall über Netze wie das Internet verwendet werden. Eine Ausnahme liegt vor, wenn die Kommunikation über das Netz verschlüsselt wird. Nur die dynamische Verschlüsselung zwischen Benutzer und Firewall-System kann das Mitlesen und Wiedereinspielen von Passworten verhindern.

Auch wenn die Kommunikation verschlüsselt ist, muss bei der Nutzung von Passwörtern beachtet werden, dass die Sicherheit von der »Qualität« der verwendeten Passworte abhängig ist. Der Name der Frau oder Freundin des Benutzers ist für einen Außenstehenden leicht zu erraten.

Passwortregeln

Die wichtigsten Passwortregeln, die unbedingt zu beachten sind, zeigt folgende unvollständige Liste der GDD (Gesellschaft für Datenschutz und Datensicherheit):

- Nirgends notieren! Niemandem mitteilen!
- Das Passwort darf nur dem Benutzer bekannt sein.
- Mindestlänge: 6 Stellen
- Vor- und Familiennamen nie allein verwenden, sondern:
- stets alphanumerisch gestalten (Buchstaben und Zahlen/Zeichen).
- Keine Trivialpassworte (z.B. 4711, 12345 oder andere nebeneinander liegende Tasten) verwenden.
- In angemessenen Zeitabständen ändern; nicht zu oft!
- Automatisch verhindern, dass (aus Bequemlichkeit) als neues wieder das alte Passwort gewählt wird.

neuKap08.fm Seite 274 Freitag, 18. Oktober 2002 3:52 15

- Für besonders wichtige Funktionen/sensible Daten: Zusatzpasswort (»4-Augen-Prinzip«). Oder zwei Personen kennen je das halbe Passwort.
- Passwort des Systemverwalters - nur ihm bekannt - für Vertretungsfall versiegelt aufbewahren.

Viele Angriffe auf Passworte finden heute automatisiert statt, indem alle Begriffe aus einem deutschen oder englischen Wörterbuch ausprobiert werden. Mit einem entsprechenden Programm kann ein solcher Test bereits bei der Definition von Passworten durchgeführt werden, womit einem solchen Angriff vorgebeugt wird.

8.2.2 Einmal-Passwort

Das Konzept »Einmal-Passwort« legt fest, dass ein Passwort nur einmal verwendet werden darf. Das heißt, bei der nächsten Authentikation wird ein neues, anderes Passwort verwendet, um die Wiederverwendung eines bereits eingesetzten Passwortes zu verhindern.

Für die Vergabe von Einmal-Passworten gibt es unterschiedliche Methoden. Entweder bestimmt das Firewall-System selbst die Einmal-Passworte und stellt sie den Benutzern vertraulich zur Verfügung, oder beide, Benutzer und Firewall-System, berechnen nach einem definierten Verfahren das Einmal-Passwort während des Authentikationsprozesses.

Im ersten Fall, in dem das Firewall-System die Einmal-Passworte bestimmt, kann eine Limitierung der möglichen Anmeldevorgänge vorgenommen werden, indem nur eine begrenzte Zahl an Einmal-Passworten zur Verfügung gestellt wird. Falls der Benutzer keine Einmal-Passworte mehr zur Verfügung hat, muss er neue beantragen.

Durch Einmal-Passworte können die Nachteile des Passwort-Verfahrens überwunden werden. In der Praxis ist aber der Aufwand für das Verfahren (Berechnung und Verteilung der Einmal-Passworte) hoch und wird nur für wenige Anwendungen akzeptiert.

8.2.3 Challenge-Response-Verfahren

Das Konzept »Challenge-Response-Verfahren« legt fest, dass ein Benutzer sich gegenüber dem Firewall-System kryptographisch beweisen muss. Bei diesem Verfahren besitzt der Benutzer ein Geheimnis, z. B. einen geheimen Schlüssel, mit dem er spontan eine kryptographische Operation durchführen muss als Beweis dafür, dass er den geheimen Schlüssel besitzt. In der Regel sendet das Firewall-System dem Benutzer eine Zufallszahl, die Challenge, die dann spontan kryptographisch verarbeitet wird und dem Firewall-System als Response gesendet wird. Das Firewall-System überprüft, ob der Benutzer die kryptographische Operation richtig durchgeführt hat. Falls ja, war die Authentikation erfolgreich. Im anderen

neuKap08.fm Seite 275 Freitag, 18. Oktober 2002 3:52 15

Fall gilt die Echtheit des Benutzers als nicht nachgewiesen und eine Kommunikation über das Firewall-System wird nicht zugelassen.

Beim Challenge-Response-Verfahren können aufgezeichnete Informationen wie die Challange und/oder die Response nicht ein zweites Mal verwendet werden.

Bei einer Authentikation über unsichere Netze müssen Challenge-Response-Verfahren eingesetzt werden, um ein Abhören und daraus resultierende missbräuchliche Verwendung zu verhindern!

8.3 Authentikationsverfahren für Firewall-Systeme

Im Folgenden werden exemplarisch einige Authentikationsverfahren vorgestellt, die mit kryptographischen Algorithmen arbeiten und in Firewall-Systemen eingesetzt werden können.

Das Firewall-System kann eine Authentikation nur durchführen, wenn das kryptographische Verfahren für zugreifende Benutzer und das Firewall-System einheitlich sind. Außerdem müssen die Benutzer zur präzisen Identifizierung über einen eindeutigen Namen (»distinguishing identifier«) verfügen.

8.3.1 S/Key (MD5)

Das Einmal-Passwort-Verfahren S/Key, entwickelt von dem amerikanischen Unternehmen Bellcore (Bell Communication Research), basiert auf den One-Way-Hashfunktionen »MD4« und »MD5«. Implementationen sind für fast alle Betriebssysteme und Architekturen erhältlich, sowohl als Server-Implementation wie auch als Client (S/Key-Calculator).

Das Einmal-Passwort-Verfahren (One-Time-Password OTP) ist im »Request for Comment« RFC1938 standardisiert.

Verfahren

Der Einmal-Passwortmechanismus S/Key führt die One-Way-Hashfunktion (z. B. MD5) über einen String aus, der sich aus einem Startwert und dem geheimen Passwort des Benutzers zusammensetzt. Das Ergebnis – eine kryptographische Prüfsumme – wird als Eingabewert für weitere Durchläufe (Runden) verwendet.

Als Ergebnis wird die zuletzt berechnete kryptographische Prüfsumme mit der Anzahl der durchlaufenen Runden und dem Startwert abgespeichert.

Die Sicherheit dieses Authentikationsmechanismus beruht auf der Nicht-Umkehrbarkeit der One-Way-Hashfunktion und der Geheimhaltung des Passworts, das zur Initialisierung verwendet wurde.

neuKap08.fm Seite 276 Freitag, 18. Oktober 2002 3:52 15

Abbildung 8.2 zeigt das Funktionsschema des S/Key-Verfahrens:

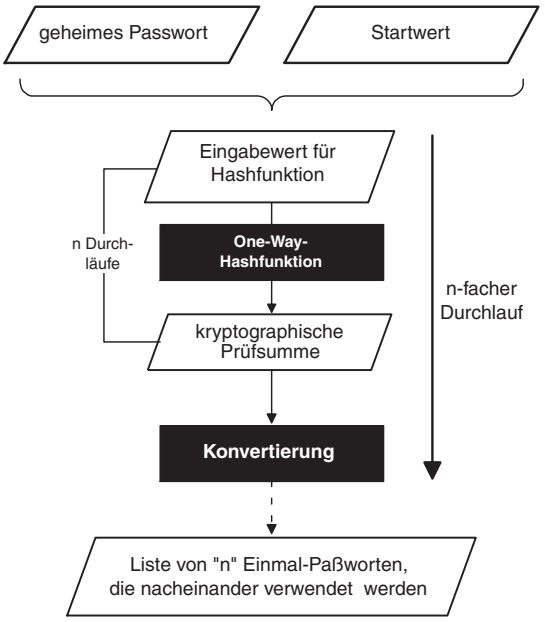


Abb. 8.2: S/Key-Berechnung

Funktionsablauf

- Der Benutzer (S/Key-Benutzer) bekommt vom Firewall-System eine Liste aller Einmal-Passworte oder er generiert jeweils das aktuelle Einmal-Passwort über ein Berechnungsprogramm. Die Berechnungsprogramme sind für fast alle Betriebssysteme erhältlich.

  Das berechnete Passwort präsentiert sich dem Benutzer als eine Liste von sechs englischen Worten, die eine Abbildung des Berechnungsergebnisses auf ein fest definiertes Lexikon mit 2 048 Begriffen darstellen. Das Lexikon ist im RFC1938 nachzuschlagen. Die Zuweisung erfolgt über einen Index.

- Zur Authentisierung wird das »n–1«-te Passwort eingegeben, das dann die One-Way-Hashfunktion durchläuft und mit dem gespeicherten »n«-ten Passwort verglichen wird.
- Nach erfolgreichem Vergleich wird das »n–1«-te Passwort mit der aktuellen Zahl der noch zu durchlaufenden Runden (n–1) und dem gleichgebliebenen Startwert als neuer Vergleichswert abgespeichert.
- Nach n Durchläufen ist der Vorrat an Einmal-Passworten erschöpft, und dem Benutzer muss eine neue Serie zugewiesen werden (Limitierung der Anmeldevorgänge).

neuKap08.fm Seite 277 Freitag, 18. Oktober 2002 3:52 15

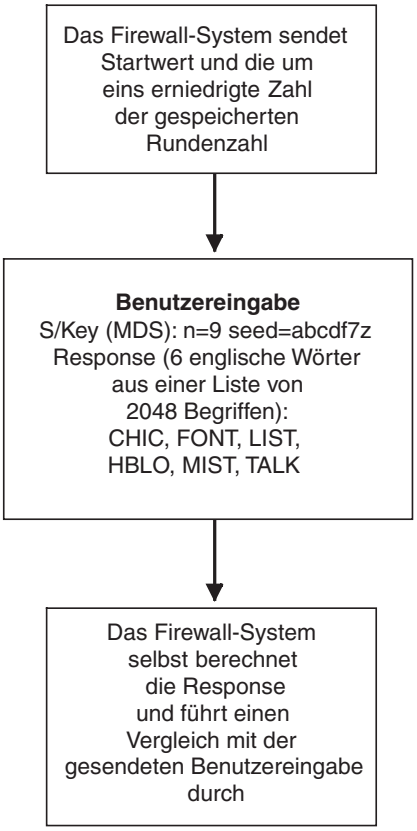


Abb. 8.3: S/Key-Ablauf

Ablauf des Authentikationsverfahrens

Der Benutzer baut eine Kommunikationsverbindung mit dem Firewall-System auf. Nach der Eingabe seines Namens wird das einzugebende Einmal-Passwort durch die Ausgabe der Rundenzahl (n) und des Startwertes (seed) definiert (siehe Abb. 8.3). Mittels der Rundenzahl, des Startwertes und des geheimen Passwortes kann der Benutzer die entsprechende Response (Einmal-Passwort) aktuell berechnen oder aber anhand der Rundenzahl »n« der vorgefertigten Liste entnehmen.

Die Eingabe wird dann auf dem Firewall-System durch die One-Way-Hashfunktion eine Runde weitergerechnet und mit dem gespeicherten Passwort verglichen. Stimmen die Werte überein, speichert der Client das eingegebene Passwort zusammen mit der neuen Rundenzahl (n–1) und dem alten Startwert in der Benutzerdatenbank ab.

Sind die gesendete Response und die selbst berechnete Response des Firewall-Systems verschieden, wird intern ein Vergleich zwischen der aktuellen Anzahl und

neuKap08.fm Seite 278 Freitag, 18. Oktober 2002 3:52 15

der Zahl der maximal erlaubten Authentikationsversuche vorgenommen. Bei Überschreitung des Maximums wird der Benutzer gesperrt.

Vorteile des S/Key-Verfahrens:

- Die Software auf dem Client ist einfach zu handhaben.
- Sie ist für viele Rechnersysteme verfügbar.

Nachteile:

- Die Speicherung der geheimen Informationen beim Client ist problematisch (Passwort).
- Sechs englische Begriffe müssen eingegeben werden.

8.3.2 Authentikationsverfahren mit Security Token

Als Beispiel für ein Authentikationsverfahren mit Security Token wird hier das Digipass-Verfahren vorgestellt. Lacard ist ein Security Token, das mit dem DES-Verfahren arbeitet.

Verfahren

Das Lacard-Authentikationsverfahren beruht auf einem Challenge-Response-Verfahren, bei dem das Firewall-System immer die Challenge vorgibt und die Response vom Benutzer mithilfe des Security Token berechnet wird.

Das zugrunde liegende kryptographische Verfahren, der DES-Algorithmus, wird sowohl im Security Token als auch im Firewall-System zur Verfügung gestellt.

Damit die beiden Instanzen (Security Token und Firewall-System) unabhängig voneinander zum gleichen Ergebnis kommen, benötigen sie den gleichen geheimen Schlüssel. Dieser Schlüssel wird vom Security Management erstellt. Das Security Token wird dann mittels einer Initialisierungsstation mit den Schlüsseln versorgt. Für das Firewall-System wird der Schlüssel über das Security Management zur Verfügung gestellt.

Die Berechnung der Challenge beruht auf einem Zufallsstring (Zufallszahl und Zeitwert), der mit dem vorgegebenen geheimen Schlüssel verschlüsselt und auf das Dezimalsystem abgebildet wird. Zu dieser Challenge berechnet das Security Token eine Response, die mit der im Firewall-System berechneten Response aus der zuvor gespeicherten Challenge verglichen wird.

Die Challenge wird bei jeder Authentisierungsanfrage neu berechnet und zwischen Firewall-System und Benutzer übertragen, ebenso wie die erzeugte Response.

Um das Security Token für diese Aufgabe verwenden zu können, muss der Benutzer es zuvor mithilfe einer PIN aktivieren, d.h., die PIN muss in das Security Token eingegeben werden. Diese PIN kann der Benutzer selbst zu jeder Zeit ändern.

neuKap08.fm Seite 279 Freitag, 18. Oktober 2002 3:52 15

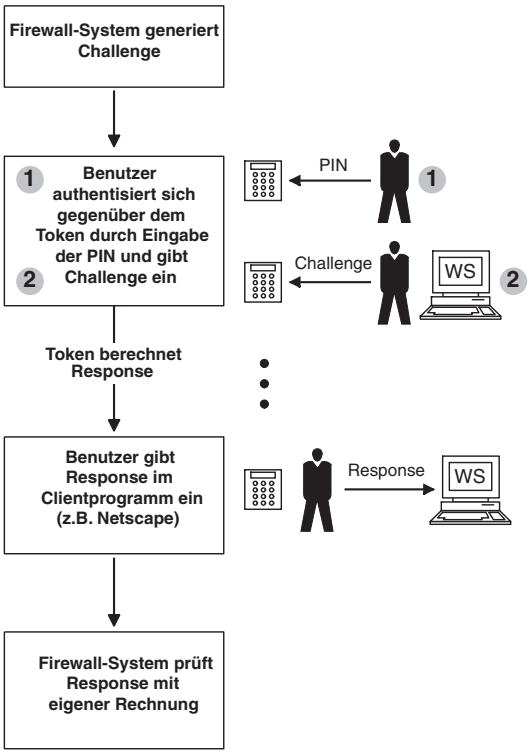


Abb. 8.4: Authentikationsverfahren mit Security Token

Wenn ein Security Token verloren geht, kann ein Finder es ohne Kenntnis der individuellen PIN des Benutzers nicht verwenden. Erlangt jemand Kenntnis von der PIN des Benutzers, dann kann er keinen Nutzen daraus ziehen, wenn er nicht auch das Security Token besitzt. Dadurch wird die Möglichkeit der Authentikation auf doppelte Weise gesichert: durch Wissen (PIN) und Besitz (Security Token).

Ablauf des Authentikationsverfahrens (Abb. 8.4)

Ein Benutzer baut eine Kommunikationsverbindung mit dem Firewall-System auf. Nach Eingabe seines Benutzernamens wird ihm eine Challenge auf dem Bildschirm des Rechnersystems angezeigt. Nun muss der Benutzer mithilfe seiner individuellen PIN das Security Token aktivieren. Dann gibt er die Challenge ein, und im Security Token wird unter Verwendung des dort gespeicherten geheimen Schlüssels die Response berechnet. Der Benutzer gibt die auf dem Security Token angezeigte Response in sein Rechnersystem ein und teilt sie damit dem Firewall-System mit.

Die Response wird auf dem Firewall-System mit einer aus der zuvor gespeicherten Challenge berechneten Response verglichen. Sind die Ergebnisse von Security Token und Firewall-System verschieden, wird der Benutzer erneut zur Berechnung

neuKap08.fm Seite 280 Freitag, 18. Oktober 2002 3:52 15

aufgefordert. Intern wird währenddessen ein Vergleich zwischen der aktuellen Anzahl und der Zahl der maximal erlaubten Authentikationsversuche angestellt. Wird das Maximum überschritten, wird der Benutzer für eine vordefinierte Zeit gesperrt.

Vorteile des Security Token-Verfahrens:

- Das Verfahren stellt keine besondere Anforderung an die Hardware und Software des Benutzers. Der Austausch von Challenge und Response wird über Anzeigen und Tasten des Rechnersystems und des Security Token realisiert.
- Dieses Verfahren ist sicherer als das Einmal-Passwort-Verfahren, da das Security Token eine sichere Hardware ist.

Nachteil:

- Für den Benutzer ist das Security Token-Verfahren aufwendig, da es in mehreren Schritten durchgeführt wird: Aktivieren des Security Token, Eingabe der Challenge und Eingabe der Response.

8.3.3 Signaturkarte (Chipkarte)

Das Signaturgesetz schafft in Deutschland/Europa die Voraussetzungen für eine Sicherheitsinfrastruktur, in der jeder Benutzer eine eindeutige Identifikation bekommt und Zertifikate (elektronische Ausweise) mit öffentlichen Schlüsseln verfügbar gemacht werden. Diese Infrastruktur ermöglicht ein einheitliches Identifikations- und Authentikationsverfahren, das für eine weltweite Lösung beispielhaft und wegweisend sein kann.

In dieser Infrastruktur verfügt jeder Benutzer über eine Chipkarte, mit der er sich gegenüber einem Firewall-System identifizieren und authentisieren kann.

Verfahren

Das folgende Sicherheitsprotokoll nutzt die digitale Signatur, um die Authentizität eines Benutzers überprüfen zu können. Der Benutzer beweist seine Identität durch den Besitz seines geheimen privaten Schlüssels. Das Firewall-System überprüft den geheimen Schlüssel durch die unter bestimmten vorgegebenen Zufallszahlen dynamisch durchgeführte Signatur /ISO 9798/.

Spezielle Voraussetzungen

Authentikationsprotokolle, die mit Public-Key-Verfahren arbeiten, basieren auf folgenden Voraussetzungen:

- Eine Infrastruktur existiert, die dem Firewall-System den öffentlichen Schlüssel der Benutzer authentisch liefert. Diese Voraussetzung kann z. B. ein TrustCenter erfüllen.

neuKap08.fm Seite 281 Freitag, 18. Oktober 2002 3:52 15

- Jeder Benutzer hat einen geheimen privaten Signatur-Schlüssel, den nur er mithilfe seiner Chipkarte nutzen kann.
- Das Firewall-System ist in der Lage, Zufallszahlen zu generieren.

Beschreibung der verwendeten Abkürzungen

= sSX (Y)	Signatur der Daten Y unter Verwendung des geheimen Schlüssels SX
= ePX (Y)	Verschlüsselung der Daten Y unter Verwendung des öffentlichen Schlüssels PX
= A // B	Ergebnis der Konkatenation von A und B
= TX	Zeitstempel von X
= RX	Zufallszahl von X
= TVPX	Zeitabhängiger Parameter von X

Ablauf des Authentikationsverfahrens

Two-Way Authentication:

Mit diesem Authentikationsmechanismus ist das Firewall-System A in der Lage, den Benutzer B zu authentisieren. Die Einmaligkeit und Aktualität der Authentikationsdaten wird mithilfe einer Zufallszahl erreicht.

Aufbau des TokenBA:

TokenBA = R_B // A // R_A // Text3 // sS_B (R_B // A // R_A // Text2)

Text1, Text2 und Text3 sind Textfelder, die von der speziellen Anwendung abhängen.

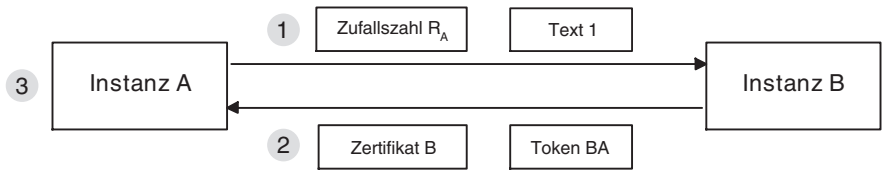


Abb. 8.5: Two-Way Authentication

- A sendet eine Zufallszahl R_A und, optional, ein Textfeld Text1 an B.
- B sendet TokenBA und, optional, das eigene Zertifikat an A.
- Nach Erhalt der Nachricht berechnet die Instanz A folgende Schritte:
  - Die Instanz A überprüft das Zertifikat von B oder stellt sicher, dass sie einen echten öffentlichen Schlüssel von B besitzt.
  - Die Instanz A prüft die Signatur des TokenBA.
  - Die Instanz A überprüft, ob die im Schritt 1 gesendete Zufallszahl mit der im TokenBA unterschriebenen übereinstimmt.

neuKap08.fm Seite 282 Freitag, 18. Oktober 2002 3:52 15

Das Firewall-System A hat den Benutzer B authentisiert, wenn es die Überprüfungen in Schritt (3) akzeptiert.

Vorteile: Dieses Authentikationsverfahren erleichtert den Firewall-Systemen die Authentikation der Benutzer, weil eine bereits vorhandene Infrastruktur verwendet werden kann, um die Eindeutigkeit der Namen zu garantieren. Die Zertifikate der Benutzer, die über das Firewall-System kommunizieren wollen, müssen dem Firewall-System zugänglich gemacht werden. Dies kann z. B. durch eine Abfrage der öffentlichen Zertifizierungsinstanzen (TrustCenter) realisiert werden.

Nachteile: Die Rechnersysteme müssen mit einem Chipkartenleser ausgestattet werden. Dieser Nachteil wird mit hoher Wahrscheinlichkeit in naher Zukunft keine Rolle mehr spielen, weil dann jedes Rechnersystem über einen Chipkartenleser verfügen wird.

8.3.4 SSL Client Authentication

Mithilfe von SSL (Secure Socket Layer) kann auch eine Client Authentication realisiert werden (zu SSL siehe auch Kap. 7 und Anhang A):

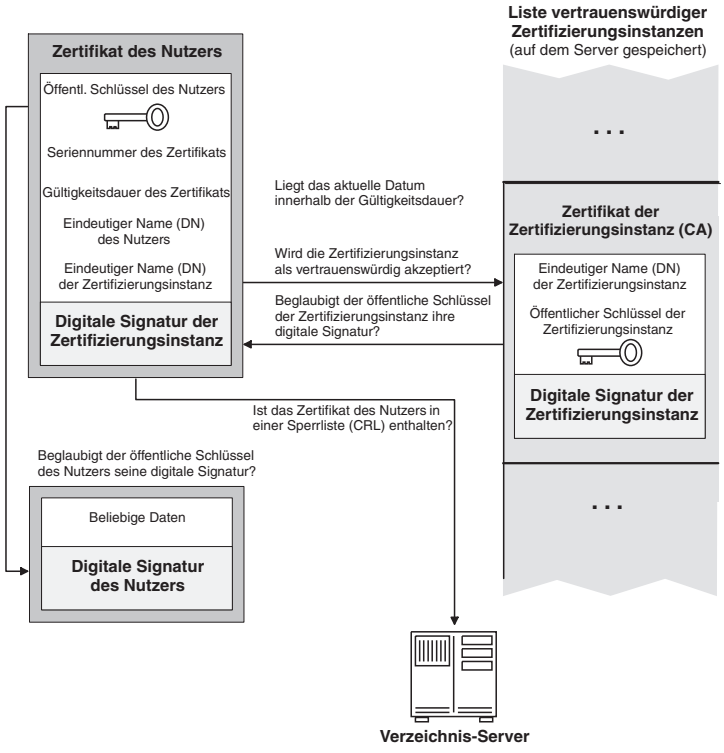


Abb. 8.6: Überprüfung eines Client-Zertifikats

neuKap08.fm Seite 283 Freitag, 18. Oktober 2002 3:52 15

Der Client schickt dem Server seinen öffentlichen Schlüssel in Form eines Zertifikats und zusätzlich Daten, die mit dem geheimen Schlüssel des Clients digital signiert wurden. Das Zertifikat wurde zuvor von einer vertrauenswürdigen unabhängigen Institution, einer Zertifizierungsstelle, ausgestellt und enthält neben dem öffentlichen Schlüssel des Client Informationen, die diesen eindeutig identifizieren. Um die Echtheit und Integrität des öffentlichen Schlüssels zu garantieren, ist das Zertifikat mit dem privaten Schlüssel der Zertifizierungsstelle signiert. (z. B. VeriSign, GobalSign).

Ablauf der Client-Authentikation

1. Der Server überprüft die digital signierten Daten mit dem öffentlichen Schlüssel des Client, der dem Client-Zertifikat entnommen werden kann. Verläuft die Überprüfung erfolgreich, ist die Zusammengehörigkeit des öffentlichen und des geheimen Schlüssels des Clients verifiziert. Außerdem steht damit fest, dass die signierten Daten nach der Signatur nicht verändert wurden. Die Zusammengehörigkeit vom öffentlichen Schlüssel und dem DN (Distinguished Name) des Client-Zertifikats ist damit hingegen nicht bewiesen.
2. Der Server überprüft den Gültigkeitszeitraum des gesendeten Client-Zertifikats.
3. Der Server überprüft anhand des DN (Distinguished Name) und der ihm vorliegenden Liste, ob es sich bei der ausstellenden CA (Certification Authority) um eine bekannte CA handelt.
4. Das Zertifikat des Client wird dann mittels des öffentlichen Schlüssels der ausstellenden CA überprüft. Der öffentliche Schlüssel der CA wird der Liste der bekannten CAs entnommen.
5. Dieser optionale Schritt erlaubt es, eine CRL (Certificate Revocation List) einzubinden. Hier kann überprüft werden, ob das Zertifikat des Client in der Zwischenzeit gesperrt wurde, obwohl der Gültigkeitszeitraum noch nicht abgelaufen ist.

Probleme bei der SSL-Authentikation

Die Qualität der SSL-Client-Authentikation hängt von folgenden Faktoren ab:

- der Vertrauenswürdigkeit der Zertifizierungsinstanz
- dem Level, auf dem die Zertifizierungsinstanz die Authentizität des Teilnehmers überprüft
- der Bereitstellung einer CRL (Certificate Revocation List) durch die Zertifizierungsinstanz

Verschiedene Zertifizierungsanbieter bieten unterschiedliche Klassen von Zertifikaten an. Ein Zertifikat der Klasse 1 bekommt der Teilnehmer schon nach der Zusendung des Namens und der E-Mail-Adresse, ohne dass seine Identität näher geprüft wird. Für ein Zertifikat der Klasse 2 wird z. B. die Zusendung einer Kopie des Ausweises oder des Führerscheins verlangt. Bei höheren Klassen muss der

neuKap08.fm Seite 284 Freitag, 18. Oktober 2002 3:52 15

Teilnehmer sich persönlich (mithilfe des Ausweises) bei einer Registration Authority (RA) authentisieren. Hierbei stellt sich die Frage, wie vertrauenswürdig eine solche Registration Authority (RA) ist.

8.3.5 Authentikationsverfahren mittels Mobiltelefon

Das folgende Authentikationsverfahren nutzt GSM-Mobiltelefone (Handys) als Hardware-Token. Der Authentisierungsdienst erzeugt dabei auf Anforderung ein kryptographisch sicheres und zeitlich begrenztes Einmal-Passwort, das dann über den SMS-Dienst der GSM-Netze dem Benutzer übersandt wird.

Verfahren

Das Authentisierungsverfahren basiert auf einem zentralen Authentisierungsdienst, bestehend aus einer kryptographisch gesicherten Datenbank mit den Benutzerinformationen, einem Hardware-Sicherheitsmodul und einem GSM-Sender. Die Benutzerinformationen liegen in der Datenbank und werden mit geeigneten Verschlüsselungsverfahren gesichert. Bei einer Authentisierungsanfrage wird mithilfe des entsprechenden Nutzerdatensatzes innerhalb des Hardware-Sicherheitsmoduls ein kryptograpisch sicheres Einmal-Passwort generiert und über den GSM-Sender mittels SMS-Dienst übermittelt. Zur gesicherten Übermittlung des Einmal-Passworts an den Benutzer wird ein Public-Key-Algorithmus verwendet. Alle verwendeten Schlüssel auf der Seite des Authentisierungsdienstes sind in dem Hardware-Sicherheitsmodul gesichert abgelegt und somit gegen unberechtigten Zugriff geschützt.

Das Einmal-Passwort ist während der Übertragung zum Handy über ein asymmetrisches Verfahren verschlüsselt. Die zugehörigen Schlüssel befinden sich in der Datenbank (öffentlicher Schlüssel) und auf der SIM-Karte des Handy (geheimer Schlüssel). Zur Entschlüsselung ist die SIM-Karte des Nutzers mit einer PIN-geschützten Zusatzapplikation ausgestattet, die jedoch eine SIM-Karte der neuen Generation erfordert.

In einem einmaligen Anmeldeprozess werden alle notwendigen Daten des Benutzers wie User-ID, Name, Mobilfunknummer, etc. in die Benutzerdatenbank eingetragen. Anschließend erhält er eine Zusatzapplikation für seine SIM-Karte im Mobiltelefon entweder durch Austausch mit einer neuen SIM-Karte oder aber per Daten-SMS.

Der Authentisierungsdienst kombiniert Mechanismen und Kommunikationsdienste aus anderen bestehenden Verfahren und stellt somit eine flexible und gesicherte Benutzerauthentisierung für Firewall-Systeme zur Verfügung.

Die wesentliche Elemente des Authentisierungsdienstes sind:

- Hardware-Sicherheitsmodul zur Speicherung und Anwendung aller kryptographischen Schlüssel

neuKap08.fm Seite 285 Freitag, 18. Oktober 2002 3:52 15

- verschlüsselte Benutzerdaten in einer zentralen Datenbank
  Mindestens vorhanden sind: die User-ID sowie der öffentliche Schlüssel des Nutzers, dessen privater Teil sich im Handy (SIM-Karte) befindet; Felder für das Zeitfenster, die Telefonnummer, Fehlversuche, Berechtigungen etc.
- Einmal-Passwörter
  Die Einmal-Passwörter werden im Hardware-Sicherheitsmodul des Authentisierungsdienstes generiert und im verschlüsselten Nutzerdatensatz gespeichert. Das Einmal-Passwort ist nur für eine bestimmte Zeit nach der Generierung gültig.
- verschlüsselte Übermittlung des Einmal-Passworts
  über den SMS-Dienst der GSM-Netze an das Mobiltelefon des Nutzers
- PIN-geschützte Zusatzanwendung auf der SIM-Karte des Mobiltelefons,
  bei der nach Eingabe einer dem Nutzer bekannten PIN das Einmal-Passwort mit dem geheimen Schlüssel des Nutzers entschlüsselt und im Klartext angezeigt wird

Systemüberblick

Das System besteht aus:

- einem Rechnersystem, das mit dem Internet verbunden ist
  Es führt die Interaktion mit dem Firewall-System durch.
- dem zentralen Firewall-System als Zugangspunkt zum internen Netzwerk des Dienstanbieters
- dem Authentisierungsdienst zur Überprüfung der Berechtigung

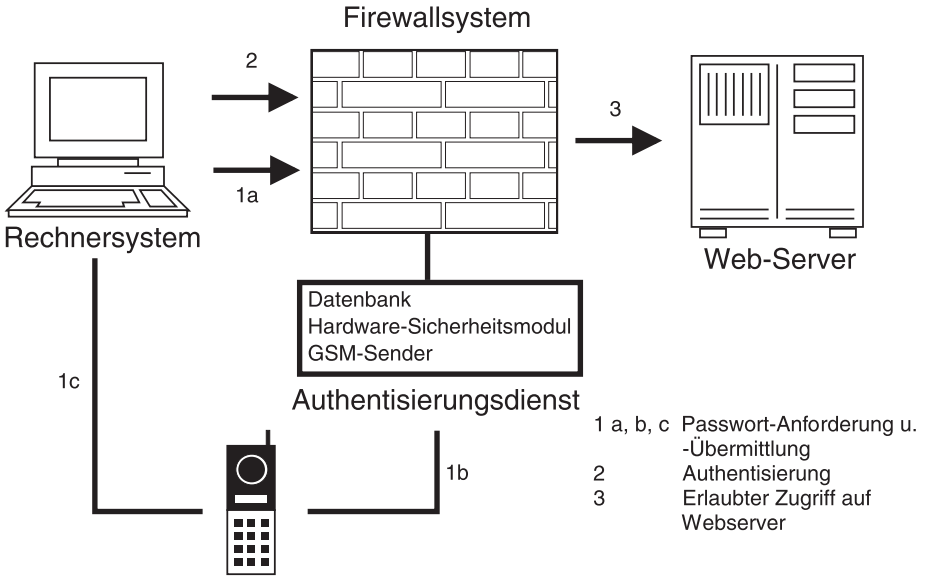


Abb. 8.7: Authentikation mittels Mobiltelefon

neuKap08.fm Seite 286 Freitag, 18. Oktober 2002 3:52 15

Funktionsablauf für die Anmeldung mittels Mobiltelefon

- Von einem beliebigen Rechnersystem im Internet wählt der Benutzer das zentrale Firewall-System an.
- Der Benutzer wird dann auf der Anmeldeseite aufgefordert, seine User-ID einzugeben.
- Der Authentisierungsdienst sucht dann in der Datenbank die User-ID. Ist die User-ID vorhanden, wird der der ID zugehörige, verschlüsselt gespeicherte Datensatz in das Hardeware-Sicherheitsmodul geladen und mit dem dort befindlichen Schlüssel entschlüsselt.
- Das Hardware-Sicherheitsmodul generiert nun ein Einmal-Passwort und trägt dieses in den Userdatensatz ein. Der Userdatensatz wird anschließend wieder verschlüsselt und in der Datenbank des Authentisierungsdienstes abgelegt.
- Das Einmal-Passwort wird im Hardware-Sicherheitsmodul mit dem Public-Key des Nutzers, der Teil des Userdatensatzes ist, verschlüsselt und dann via GSM-Sender an das Mobiltelefon des Benutzers übermittelt.
- Der Benutzer empfängt das verschlüsselte Einmal-Passwort als SMS. Nach Eingabe einer Geheimzahl startet die Zusatzapplikation auf dem Mobiltelefon die Entschlüsselung in der SIM-Karte mit dem Secret-Key des Benutzers.
- Auf der Anmeldeseite trägt der Benutzer nun das übermittelte Einmal-Passwort ein. Beide Informationen gelangen über das Internet erneut zum Authentisierungsdienst.
- Der Authentisierungsdienst übergibt den verschlüsselten Userdatensatz aus der Datenbank an das Hardware-Sicherheitsmodul. Im Sicherheitsmodul wird das Einmal-Passwort, die bisher vergangene Zeit und die Anzahl der Anmeldeversuche überprüft und nur das Ergebnis zurückgemeldet.
- Bei positivem Ergebnis erhält der Benutzer Zugriff auf den gewünschten Dienst über das Firewall-System.
- Bei Überschreitung des Zeitfensters oder mehr als drei Fehlversuchen wird der Zugang verweigert.

Vorteile des Authentisierungsverfahren

- Das Mobiltelefon als Endgerät des zweiten Übertragungskanals (GSM-Netzwerk) ist weit verbreitet und steht damit für einen großen Benutzerkreis zur Verfügung.
- Die Nutzerdaten liegen immer in einer kryptographisch gesicherten Datenbank, die für mögliche Angreifer wertlos ist, da lediglich die frei gewählte User-ID im Klartext lesbar ist.
- Höchste Sicherheit der verwendeten Schlüssel, da sie in einem Hardware-Sicherheitsmodul gespeichert werden.

Anforderungen des Authentisierungsverfahren

- Für die Realisierung des hier vorgestellten Verfahrens werden SIM-Karten benötigt, die um eine Zusatzapplikation ergänzt sind.

neuKap09.fm Seite 287 Freitag, 18. Oktober 2002 3:52 15

Kapitel 9

Verschiedene Firewall-Lösungen und ihre Bewertung

Firewall-Systeme verschiedener Hersteller unterscheiden sich in ihren Lösungsansätzen und Qualitäten. In diesem Kapitel sollen die unterschiedlichen Lösungsansätze diskutiert und bewertet werden. Außerdem werden die Anforderungen an die Sicherheit von Firewall-Produkten diskutiert.

9.1 Public Domain Software oder ein Firewall-Produkt?

Die erste Unterscheidung betrifft die Herkunft der Firewall-Lösungen: Im Internet werden Firewall-Systeme als »Public Domain Software« kostenlos zur Verfügung gestellt, und spezialisierte High-Tech-Unternehmen bieten Firewall-Produkte als Soft- oder Turn-Key-Lösungen an.

9.1.1 Public Domain Software für die Firewall-Application

Einige Firewall-Lösungen werden als »Public Domain Software« im Internet zur Verfügung gestellt. Bei Public Domain Software handelt es sich um Software-Lösungen, deren Urheberschaft oft unklar ist, da sie von verschiedenen Personen geschrieben wurden. Die Rechte und Pflichten von Entwicklern und Benutzern sind nicht immer eindeutig definiert.

Diese Kurzeinführung zeigt schon, wie Public Domain Software einzuordnen ist: Es handelt sich um im Internet kostenlos erhältliche Software, die durchaus ihre Qualitäten haben mag, deren Wirksamkeit (das Wichtigste bei Sicherheits-Lösungen) aber niemand einschätzen oder gar garantieren kann. Insofern ist sie für Privatleute oder Institutionen von Nutzen, für die ein Versagen der Firewall-Software keinen nennenswerten Schaden bedeuten könnte. In den ersten Jahren des Internet-Booms haben auch einige Organisationen solche »Public Domain«-Lösungen eingesetzt, weil es andere Firewall-Produkte noch nicht gab. Inzwischen verlassen sich Benutzer, die Verantwortung für eine Behörde oder ein Unternehmen tragen, nicht mehr auf ungeprüfte Lösungen. Im Business- oder Behördenbereich ist es ratsam, sich nicht auf Public Domain Software zu verlassen, sondern auf geprüfte Soft- und Hardware-Lösungen von Fachfirmen zurückzugreifen, die auch die Verantwortung für ihre Lösung übernehmen und sie pflegen und weiterentwickeln.

neuKap09.fm Seite 288 Freitag, 18. Oktober 2002 3:52 15

Sicherheitserfahrungen

Do-it-yourself-Lösungen sind sehr fehlerträchtig und erfordern fundierte Erfahrungen und Know-how im Security-Bereich. Firewall-Hersteller, die Firewall-Produkte anbieten, investieren in der Regel über zehn Mann-Jahre Aufwand in die Entwicklung ihrer ersten Version. Anschließend müssen mindestens drei bis fünf Ingenieure, Informatiker und Mathematiker die Firewall-Lösung austesten, erweitern und pflegen, damit ihre Sicherheit garantiert werden kann. Ein solcher Aufwand kann bei »Do-it-yourself-Lösungen« von Organisationen nicht betrieben werden, was notwendigerweise Einfluss auf das erzielte Sicherheitsmaß hat.

Eine Public Domain Software bietet soviel Sicherheit wie ein geschenkter Airbag, den man sich selbst ins Auto einbauen soll. Wenn eine Firewall-Lösung im Ernstfall wirklich für Schutz sorgen soll, muss die Entwicklung, Weiterentwicklung, Installierung und Wartung erfahrenen Fachleuten überlassen werden, die den kompletten Aufbau der Lösung kennen.

Bei der Verwendung von Public Domain Software treten weitere Probleme auf:

- *Weiterentwicklung:* Im schnell wachsenden TCP/IP-Markt wird von Firewall-Systemen eine schnelle Weiterentwicklung verlangt, damit neue Dienste genutzt werden können.
- *Wartung:* Die Wartung von Firewall-Systemen verlangt eine fundierte Kenntnis der Art und Weise, wie die Sicherheitsfunktionen in den Firewall-Elementen arbeiten, damit nicht versehentlich sicherheitsrelevante Einstellungen verändert werden und dadurch die Sicherheit der Firewall-Elemente reduziert wird. Solche Kenntnisse sind bei Public Domain Software schwer zu erlangen und benötigen eine intensive Auseinandersetzung mit der Thematik, die einen sehr hohen Personaleinsatz erfordert.

9.1.2 Firewall-Produkte

Firewall-Produkte werden von Fachleuten entwickelt, die viel Erfahrung mit der Realisierung von Sicherheitslösungen in Kommunikationssystemen haben. Die Firmen garantieren die notwendige Weiterentwicklung ihrer Lösung und vor allem die Pflege ihrer Firewall-Produkte.

Die Beschäftigung mit der Sicherheit von TCP/IP-Anwendungen im Internet und Intranet ist eine Aufgabenstellung, die sehr speziell und sehr aufwendig ist, und wird in den Firmen, die Firewall-Produkte anbieten, von hochqualifizierten Mitarbeitern bewerkstelligt. Schon die Beschaffung von Informationen über neue Sicherheitslücken ist sehr arbeitsaufwendig. Diesen notwendigen Aufwand können Organisationen, die diese Technik »nur nutzen« wollen, nicht leisten. Aus

neuKap09.fm Seite 289 Freitag, 18. Oktober 2002 3:52 15

diesem Grund ist der Erwerb eines Firewall-Produktes bei Fachfirmen eine langfristig sinnvolle Investition.

9.1.3 Linux als sicheres Betriebssystem für Firewall-Lösungen

Bis heute gibt es noch kein Betriebssystem, das hinsichtlich der Kommunikationsanforderungen evaluiert und zertifiziert worden ist. Bisher wurden Betriebssysteme ausschließlich in Hinblick auf die Zugangskontrolle und Rechteverwaltung untersucht.

Eine Lösung dieses Problems kann im Einsatz eines Open-Source-Betriebsystems wie Linux liegen, das den Anforderungen entsprechend angepasst wird. Diese Anpassungen können auf einfache Weise evaluiert und untersucht werden, da die Sourcen frei verfügbar sind.

Als Einstieg in die Thematik möge folgende Mitteilung des Heise-Tickers (`www.heise.de/newsticker`) vom 14. Januar 2000 dienen:

> »**NSA macht Linux zum Firewall-System**
>
> *Die amerikanische National Security Agency (NSA) lässt ein renommiertes Firewall-Konzept auf Linux portieren. Die Datenschutzbehörde hat der Secure Computing Corporation den Auftrag erteilt, deren patentierte Technik zum Domain Type Enforcement (DTE) auch auf das Betriebssystem Linux zu portieren. DTE ordnet die Netzwerk-Interfaces von Firewall-Rechnern in getrennten Domains an, die nur durch Proxies miteinander verbunden sind.*
>
> *Security Server dieses Konzepts sind unter dem Markennamen Sidewinder bekannt geworden. Bislang verwendeten diese Rechner ein modifiziertes BSD-UNIX als Betriebssystem. Der NSA-Auftrag weist aber darauf hin, dass Linux in zunehmendem Maße an Vertrauen gewinnt, sodass es auch für den Einsatz bei Sicherheitssystemen für Industrie und Behörden interessanter wird.«*

9.1.4 Anforderungen an ein Firewall-Betriebssystem

Anpassung des Kernels

Um den Kernel den Anforderungen eines Firewall-Systems entsprechend anzupassen, muss dieser zunächst konfiguriert werden. Der Kernel sollte als ein monolithischer Block aufgebaut sein. Somit wird sichergestellt, dass einzelne Module nicht ausgetauscht werden können. Ein Angreifer müsste stattdessen den gesamten Kernel austauschen. Kernelmodule und der dynamische Lader (dynamic loader) müssen aus dem Systemen entfernt werden.

Während der Konfiguration sollten ausschließlich die wirklich nur benötigten Treiber, Netzwerkeigenschaften und Kerneloptionen ausgewählt und in den Kernel kompiliert werden.

neuKap09.fm Seite 290 Freitag, 18. Oktober 2002 3:52 15

Der selektierte und konfigurierte Kernel sollte daraufhin überprüft werden, ob Sicherheitslücken oder funktionelle Fehler bestehen. Dieses Vorgehen stellt sicher, dass der Kernel »schlank«, also auf das Nötigste beschränkt ist, und somit die Gefahr von Sicherheitslücken oder funktionellen Fehlern minimal ist.

Das Konzept einer Kernelevaluierung muss auch die Handhabung von Securitypatches beinhalten, die für den evaluierten Kernel aber auch für spätere Unterversionen herausgegeben werden können. Ebenso sind Updates zu berücksichtigen, die die Funktionalität oder die unterstützten Komponenten/Geräte betreffen.

Eine mögliche Lösung hierbei ist, funktionelle Patches oder Securitypatches in den bestehenden Kernel zu portieren, ohne auf eine neue Version umzusteigen. Dabei sollten die Änderungen genau markiert und dokumentiert werden. Somit wird sichergestellt, dass auch weiter der evaluierte Kernel eingesetzt wird, gleichzeitig aber Verbesserungen der späteren Versionen integriert werden können.

Systemanpassungen

Erster Schritt bei der Anpassungen eines GNU-Systems ist die Identifizierung jeder Datei auf dem System. Die Aufgabe einer jeder Datei ist zu analysieren, überflüssige Dateien sind zu löschen. Für die restlichen Dateien sollte die »Permission« genau überprüft und gegebenenfalls angepasst werden.

Die Entfernung von dynamisch ladbare Objekten, einschließlich des Laders selber, sorgen für eine höhere Sicherheit. Daher sollte jedes Programm statisch an die Bibliotheken angebunden werden.

Das Layout des Dateisystems kann dahingehend geändert werden, dass die meisten Partitionen »read-only« sind. Auf jeden Fall sollten die Systemprogramme und die Firewallapplikationen so eingerichtet werden, dass sie »read-only« sind. Programme zur Systemverwaltung sollten in einer eigenen Partition liegen, sodass sie nur unter bestimmten Bedingungen geladen werden können. Die Administrationsprogramme können auf einem Medium gespeichert werden, das nur gelesen werden kann, wie z. B. eine CD-ROM.

Das so geschaffene Layout ist mit einem dedizierten Prozess zu kontrollieren, um zusätzliche Sicherheit zu gewährleisten.

Eine Kombination der oben beschriebenen Maßnahmen garantiert ein sicheres System.

Zertifizierung und Evaluation eines Kernel Levels

Um die Sicherheit eines Firewall-Systems zu gewährleisten, sollte vom einer unabhängigen Organisation der Kernel Netzwerk-Code evaluiert werden. Da Linux eine offene Source ist, können die Ergebnisse dieser Evaluierung vom Kunden eingesehen und überprüft werden. Entsprechend können Änderungen eingearbeitet werden.

neuKap09.fm Seite 291 Freitag, 18. Oktober 2002 3:52 15

Daher ist Linux/GNU als Open Source für eine vertrauenswürdige und sichere Plattform für Firewallanwendungen verwendbar.

9.2 Software-Lösung oder Turn-Key-Lösung?

Welche Sicherheitsaspekte sind nun bei der Verwendung von Firewall-Produkten zu beachten, besonders bezüglich der alternativen Realisierungsansätze »reine Software-Lösung« oder »Turn-Key Lösung«?

9.2.1 Was bietet eine Software-Lösung?

Von Software-Lösung ist hier die Rede, wenn die vom Hersteller angebotene Firewall-Lösung reine Software ist. Auch wenn die Firewall-Lösung über eine Drittfirma (Software-Haus, Sicherheitsfirma etc.) erworben wird, die dann Hardware, Software und Installation zusammen anbietet, handelt es sich im ursprünglichen Sinne um eine Software-Lösung.

Sicherheitsaspekte bei einer Software-Lösung

Bei der Verwendung reiner Software-Lösungen von Firewall-Systemen sollten einige Sicherheitssaspekte betrachtet werden.

Möglichkeiten der Hersteller

Die Hersteller von Software-Lösungen, die ihre Firewall-Produkte für Standard-Betriebssysteme wie Windows NT, SUN-Solaris und HP-UX anbieten, haben bei der Entwicklung keinerlei Möglichkeiten, das Standard-Betriebssystem den Firewall-Bedürfnissen anzupassen. Die Hersteller müssen ihre Firewall-Software ausschließlich mit Systemcalls programmieren.

Falls das verwendete Betriebssystem bekannte Sicherheitslücken aufweist, muss der Hersteller seine Firewall-Software, die eigentlich dem Schutz von Angriffen aus dem unsicheren Netz (z. B. dem Internet) dienen soll, so programmieren, dass sie auch die Sicherheitslücken des Betriebssystems ausfüllt. Auf der Ebene der Systemcalls ist dies oft nicht möglich, da die Kommunikation die Firewall-Software über interne Relais passieren kann, ohne dass die Firewall-Software dieses bemerken und verhindern kann. So besteht z. B. die Gefahr des IP-Forwarding (Kernel-Funktionalität) von außen.

Bei vielen Software-Lösungen tritt das Problem auf, dass die Sicherheitsmechanismen beim Neustart oder Wiederanlauf des Firewall-Systems nicht sofort wirken, sodass die Kommunikation trotz eines Firewall-Systems für eine gewisse Zeit ungeschützt ist.

neuKap09.fm Seite 292 Freitag, 18. Oktober 2002 3:52 15

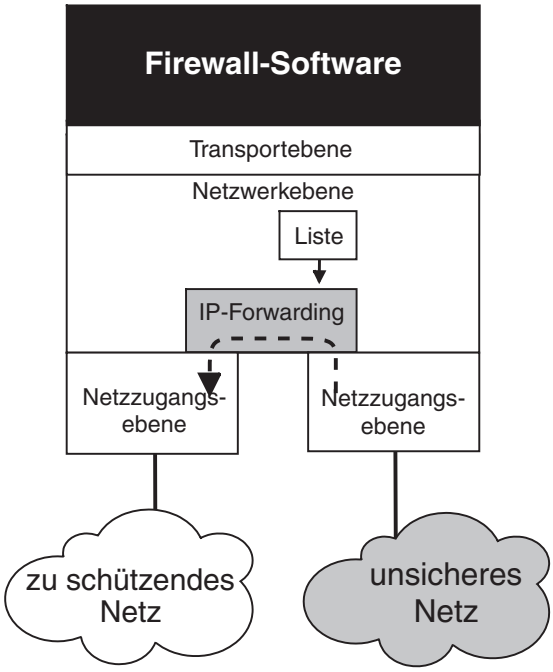


Abb. 9.1: Gefahr des IP-Forwarding

Definition der Firewall-Plattform durch den Anwender

Einige Organisationen möchten für die Betriebssystem-Plattform ihrer Firewall-Lösung nur den Unternehmensstandard (z. B. das Betriebssystem NT) einsetzen. Dieser Ansatz ist falsch und evtl. sehr sicherheitskritisch, da das entscheidende Kriterium für die Wahl eines Betriebssystems in diesem Fall das gewünschte Maß an Kommunikationssicherheit sein sollte und nicht der Unternehmensstandard. Bei der Anschaffung eines Druckers wird ja auch nicht erwartet, dass der Drucker mit dem Unternehmensstandard arbeiten muss, sondern dass die gewünschte Funktion optimal erbracht wird.

Damit eine Firewall-Lösung optimale Sicherheit gewährleisten kann, darf die Plattform keine Rolle spielen, sondern stattdessen müssen die sicheren Designkriterien von Firewall-Systemen beachtet werden (siehe Kapitel 5.1.2 *Designkonzept aktiver Firewall-Elemente*).

Verwendung von zertifizierten Betriebssystemen

Die meisten zertifizierten Betriebssysteme sind für die Sicherheitsfunktionen Identifikation und Authentikation, Rechteverwaltung etc. evaluiert worden. Wenn eine Firewall-Lösung auf ein zertifiziertes Betriebssystem aufbaut, bedeutet dies, dass das zertifizierte Betriebssystem in einer nicht-zertifizierten Umgebung einge-

neuKap09.fm Seite 293 Freitag, 18. Oktober 2002 3:52 15

setzt wird und damit die eigentliche Zertifizierung hinfällig ist. Darüber hinaus ist zu beachten, dass ein Firewall-System eine Kommunikationsanbindung ist und die Kommunikationsmodule der bekannten Betriebssysteme nicht für diesen Einsatzfall evaluiert wurden. Aus diesem Grund vermittelt die Verwendung eines zertifizierten Betriebssystems nur eine scheinbare Sicherheit und muss entsprechend kritisch bewertet werden.

9.2.2 Was ist eine Turn-Key Lösung?

Unter einer Turn-Key-Lösung (schlüsselfertigen Lösung) wird verstanden, dass das vom Hersteller angebotene Firewall-System nicht nur aus Software besteht, sondern auch die dazu passende Hardware beinhaltet. Ein solches Firewall-Produkt ist vorinstalliert und getestet. Eine Turn-Key-Lösung bleibt auch dann eine Turn-Key-Lösung, wenn sie über eine Drittfirma erworben wird, die eventuell auch die Installation durchführt.

Sicherheitsaspekte bei einer Turn-Key-Lösung

- *Fertiglösung:* Eine Turn-Key-Lösung stellt ein vollständiges Sicherheitskonzept zur Verfügung, nicht nur einzelne Module.
- *Verantwortungsbereich der Lösung:* Für die Sicherheitslösung gibt es nur einen verantwortlichen Ansprechpartner für Hardware (Packet Filter, Security Management, Application Gateway usw.), Software (Betriebssystem, Datenbank usw.) und Sicherheitsfunktionen. Die Verantwortung für das Produkt liegt klar in einer Hand, ähnlich wie beim Kauf eines Druckers. Bei einem Update ist dem Servicetechniker die Einsatzumgebung bekannt, weil alle Lösungen auf der gleichen Basis aufbauen und dies nicht dem Anwender überlassen wird.

Bei Software-Lösungen wird die Verantwortung oft zwischen dem Hersteller des Betriebssystems und dem Hersteller der Firewall-Lösung hin und her geschoben, eventuell auch noch der Firma angelastet, die die Firewall-Lösung installiert hat.

Sicherheitsaspekte: Dem Hersteller der Firewall-Lösung ist die technische Einsatzumgebung bekannt; dadurch können auf dieser Ebene durch den Anwender keine Fehler gemacht werden.

Wenn eine Software-Lösung falsch installiert wird, können dadurch möglicherweise alle Sicherheitsfunktionen umgangen werden.

- Bei einer Turn-Key-Lösung ist das Firewall-System schon vorinstalliert, sodass ihre Sicherheit bei der Inbetriebnahme bereits gewährleistet ist. Die Turn-Key-Lösung ist zuverlässig, weil sie auf ein Betriebssystem beschränkt ist (keine

neuKap09.fm Seite 294 Freitag, 18. Oktober 2002 3:52 15

if-else-Anweisungen für die verschiedenen Betriebssysteme). Bei Turn-Key-Lösungen wird nur Software eingesetzt, die wirklich gebraucht wird.

- Jedem Firewall-Element ist eine bestimmte Anwendung zugeordnet (Security Management, Application Gateway, Packet Filter)!
- Das Zusammenwirken der Sicherheitsmechanismen ist analysiert, z. B. für Packet Filter und Application Gateway, da immer die gleichen Firewall-Elemente zusammenspielen.

Betriebssicherheit einer Turn-Key-Lösung

- Anpassung der Systemumgebung
- spezielle Abstimmung für ein System
- optimale Anpassung der Firewall-Elemente aufeinander
- alle Komponenten passen zusammen

Verantwortung

Die Entscheidung für eine Turn-Key-Lösung ist besonders dann nahe liegend, wenn in einer Organisation die Spezialisten und/oder die Personen fehlen, die für das Firewall-System Verantwortung übernehmen können und wollen.

9.3 Kriterien für die Beurteilung der tatsächlichen Sicherheitsleistung eines Firewall-Produktes

Die wichtigsten Sicherheitskriterien für die Auswahl eines Firewall-Produktes sind: die Offenheit und Transparenz der Sicherheit, der Nachweis, dass es sich um geprüfte Sicherheit handelt, und die Gewissheit, dass die Sicherheitsleistung nicht durch staatliche Restriktionen beeinträchtigt wird.

Eine Firewall-Lösung soll nicht nur die Sicherheitsdienste erfüllen, für die sie angeschafft wurde, sondern auch verhindern, was nicht gewollt ist. Deshalb ist die Vertrauenswürdigkeit in eine Firewall-Lösung von besonderer Bedeutung. Dies ist äquivalent zu einem Pförtner, dem eine Organisation vertrauen können muss, damit ihre Sicherheitspolitik umgesetzt werden kann.

9.3.1 Offene und transparente Sicherheit

Die Art und Weise der eingesetzten Sicherheitsmechanismen muss offen gelegt werden, damit für den Betreiber eines Firewall-Systems das erreichbare Sicherheitsniveau überschaubar ist.

Die in einem Firewall-System, und auch in den Security Token, verwendeten Algorithmen für die Benutzerauthentikation sollen standardisierte Sicherheitsmechanismen sein, die allgemein bekannt und grundlegend durch Fachleute erforscht sind, damit die Sicherheitsleistung nachweisbar und transparent ist.

neuKap09.fm Seite 295 Freitag, 18. Oktober 2002 3:52 15

In der Praxis wird davon ausgegangen, dass ein Algorithmus sicher ist, wenn fünf Jahre nach seiner Veröffentlichung für die Verschlüsselung oder Authentikation die Mathematiker der Welt nicht in der Lage waren, ihn zu knacken.

Nicht überprüfte Algorithmen gelten nach der Erfahrung der letzen Jahrhunderte als unsicher.

Außerdem sollten die Designkriterien für Firewall-Elemente dargestellt werden.

9.3.2 Geprüfte, nachweisbare Sicherheit

Analog zu den Sicherheitsmechanismen in anderen Bereichen (z. B. Airbag in einem Auto) müssen die Sicherheitsmechanismen überprüft sein, aber nicht von jedem einzelnen Benutzer (Autofahrer), sondern von Fachleuten (dem TÜV). Dies kann z. B. mit einer IT-SEC-Evaluierung realisiert werden (siehe Kapitel 13.4 *Evaluierung und Zertifizierung von Firewall-Sytemen*).

9.3.3 Sicherheit ohne staatliche Restriktionen

Die Wirksamkeit der Sicherheitsmechanismen darf keinerlei staatlichen Beschränkungen unterliegen, damit ein Firewall-System wirklich sicher realisiert werden kann: mit geeigneter Schlüssellänge für kryptographische Sicherheitsmechanismen wie Verschlüsselung und Authentikation und *ohne* den Einbau irgendwelcher Sicherheitslücken für Geheimdienste oder andere staatliche Stellen (siehe die Exportbeschränkungen der USA).

Hier sollte der Grundsatz gelten: »Lieber keine Sicherheit als eine *Scheinsicherheit!*«

Firewall-Systeme sollen Angriffen aus den unsicheren Netz entgegenwirken und nicht als Alibi-Funktion für die »höheren« Etagen dienen. Diese Art der Scheinsicherheit kann katastrophale Folgen für eine Organisation und die Mitarbeiter haben.

neuKap09.fm Seite 296 Freitag, 18. Oktober 2002 3:52 15

neuKap10.fm Seite 297 Freitag, 18. Oktober 2002 3:52 15

Kapitel 10

Praktischer Einsatz von Firewall-Systemen

Das folgende Kapitel beschreibt exemplarisch eine Intranet-Anwendung mit dem Einsatz von Firewall-Systemen unter verschiedenen Aspekten.

Unter *Intranet* wird die Verwendung der Internet-Technologie für die innerbetriebliche Kommunikation verstanden. Auch die zugriffssichere Kopplung an öffentliche Netze (z. B. an das Internet) sowie die kontrollierte Anbindung externer Anschlusspunkte (z. B. von Telearbeitsplätzen via ISDN) oder von Teilnetzen einer Organisation (z. B. Filialen) werden mit dem Begriff Intranet verbunden.

Die Vorteile der Intranet-Technologie sind offensichtlich:

- Intranets dienen den Organisationen als gemeinsamer Informationspool und universelle Kommunikationsplattform.
- Benutzerfreundliche Browser versprechen eine einfache Handhabung und geringen Schulungsaufwand.
- Informationsverteilungssysteme lassen sich schnell, preiswert, skalierbar und flexibel realisieren.
- Dokumente lassen sich dynamisch aktualisieren, können direkt vom Autor gepflegt werden und brauchen nur an einer einzigen Stelle abgelegt zu werden.
- Intranets bieten Konzepte zur kooperativen Arbeit (z. B. Groupware, Workflow) und zur Unterstützung dezentraler Organisationsstrukturen.

Mit dem Aufbau eines Intranet verfolgen Organisationen konkrete Ziele: Kosten sollen reduziert, Arbeitsprozesse beschleunigt und vereinfacht oder ihre Qualität verbessert werden. Das Intranet dient aber auch dazu, das Wissen einer Organisation zu erfassen, zu organisieren und für jeden Mitarbeiter zugänglich zu machen.

Weitere Vorteile der Intranet-Technologie sind:

- Die Verwendung offener Standards wie des Hypertext Transfer Protocol (HTTP) und der Hypertext Markup Language (HTML) oder von TCP/IP vereinfacht die Anbindung des Intranets an das Internet.
- Die Standardisierung ermöglicht einen bequemen Zugriff externer und mobiler Anwender auf interne Daten einer Organisation.
- Außerdem erlaubt die Standardisierung den unkomplizierten Informationsaustausch zwischen Intranets von Geschäftspartnern via Internet (»Extranet«).

neuKap10.fm Seite 298 Freitag, 18. Oktober 2002 3:52 15

Die Realisierung eines Intranet kann im konkreten Fall so aussehen, dass neben der internen Kommunikation im lokalen Netz die verschiedenen Organisationseinheiten über das eigene Corporate Network miteinander verbunden sind. Telearbeitsplätze (Heimarbeitsplätze) oder Mobilgeräte (Laptops, Notebooks) werden über öffentliche Netze (z. B. ISDN, Fernsprechnetz, Internet, ...) mit dem Intranet verbunden, sodass die Benutzer auf die internen Intranet Server zugreifen und Daten abrufen oder übertragen können (siehe Abb. 10.1).

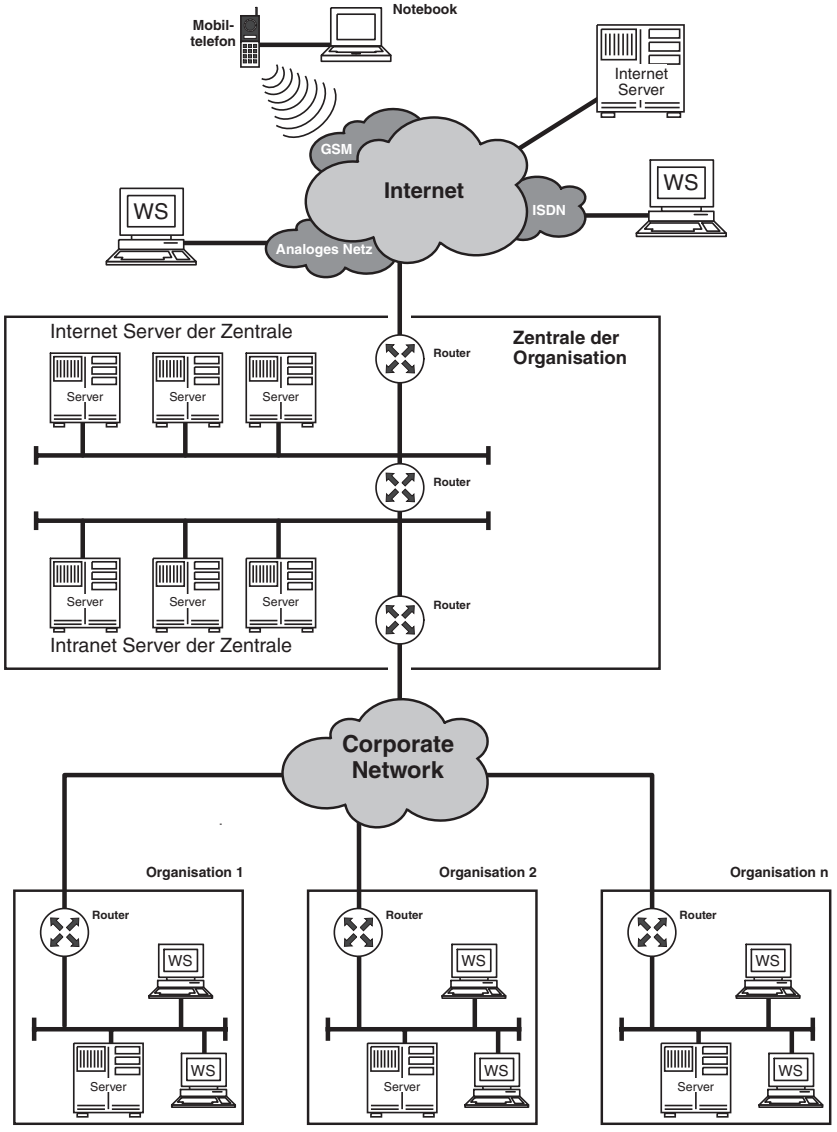


Abb. 10.1: Nutzungsmöglichkeiten des Internet

neuKap10.fm Seite 299 Freitag, 18. Oktober 2002 3:52 15

10.1 Sichere Kopplung des eigenen Intranet an das Internet

Eine sichere Kopplung zwischen dem Intranet von Organisationen und dem Internet ist die Voraussetzung dafür, dass Mitarbeiter auf Informationen und Dienste im Internet zugreifen können, z. B. auf WWW-Seiten, E-Mail, Datenbanken, Herstellerinformationen wie Prospekte, neue Treiber, neue Software etc.

Da beim Anschluss ans Internet das größte Angriffsrisiko und damit das größte Risiko eines Schadens besteht, müssen hier besonders effektive Sicherheitsmechanismen eingesetzt werden. Zur Sicherung dieser Kommunikation wird deshalb ein High-level-Security-Firewall-System eingesetzt, das die Trennung zwischen dem Internet und dem eigenen Intranet in besonders hohem Maße erbringt. Das High-level-Security-Firewall-System stellt den »Common Point of Trust« für den Übergang zwischen dem Internet und dem eigenen Intranet dar, d. h., der einzige Weg vom öffentlichen Netz ins Intranet führt kontrolliert über das High-level-Security-Firewall-System. Die Benutzer werden an dieser Stelle vom Firewall-System eindeutig idenitfiziert und authentisiert, wie von einem Pförtner.

Da alle Organisationseinheiten über das zentrale Firewall-System auf die Dienste des Internets zugreifen, kann die Sicherheitspolitik für die ganze Organisation einheitlich realisiert werden.

Wichtig ist, dass ein Firewall-Konzept verwendet wird, das bei einer Steigerung der Kommunikationsanforderung flexibel reagieren kann (siehe hierzu Kapitel 6 *Konzepte für Firewall-Systeme*).

Die Rechte der Mitarbeiter einer Organisation werden mithilfe eines zentralen Security Management flexibel festgelegt. Mitarbeiter, die auf Dienste im Internet zugreifen, werden bei Bedarf vom Firewall-System identifiziert und authentisiert, und ihre Aktionen werden entsprechend protokolliert und ausgewertet.

Um das Konzept des »Common Point of Trust« zu realisieren, ist es unerlässlich, dass keine weitere Verbindung zwischen der Organisation und dem Internet besteht. Dies setzt weitere infrastruktuelle, personelle und organisatorische Sicherheitsmaßnahmen voraus.

Zusätzlich muss in einem Firewall-Konzept festgelegt werden, welches Authentikationsverfahren verwendet werden soll, ob Java im Intranet, aber nicht im Internet verwendet werden darf (siehe Kapitel 11 *Ein Firewall-System ist mehr als ein Produkt*) etc.

In der Konzeption des Firewall-Systems sollte eine skalierbare Lösung verwendet werden, damit Erweiterungen auf einfache Weise durchgeführt werden können.

neuKap10.fm Seite 300 Freitag, 18. Oktober 2002 3:52 15

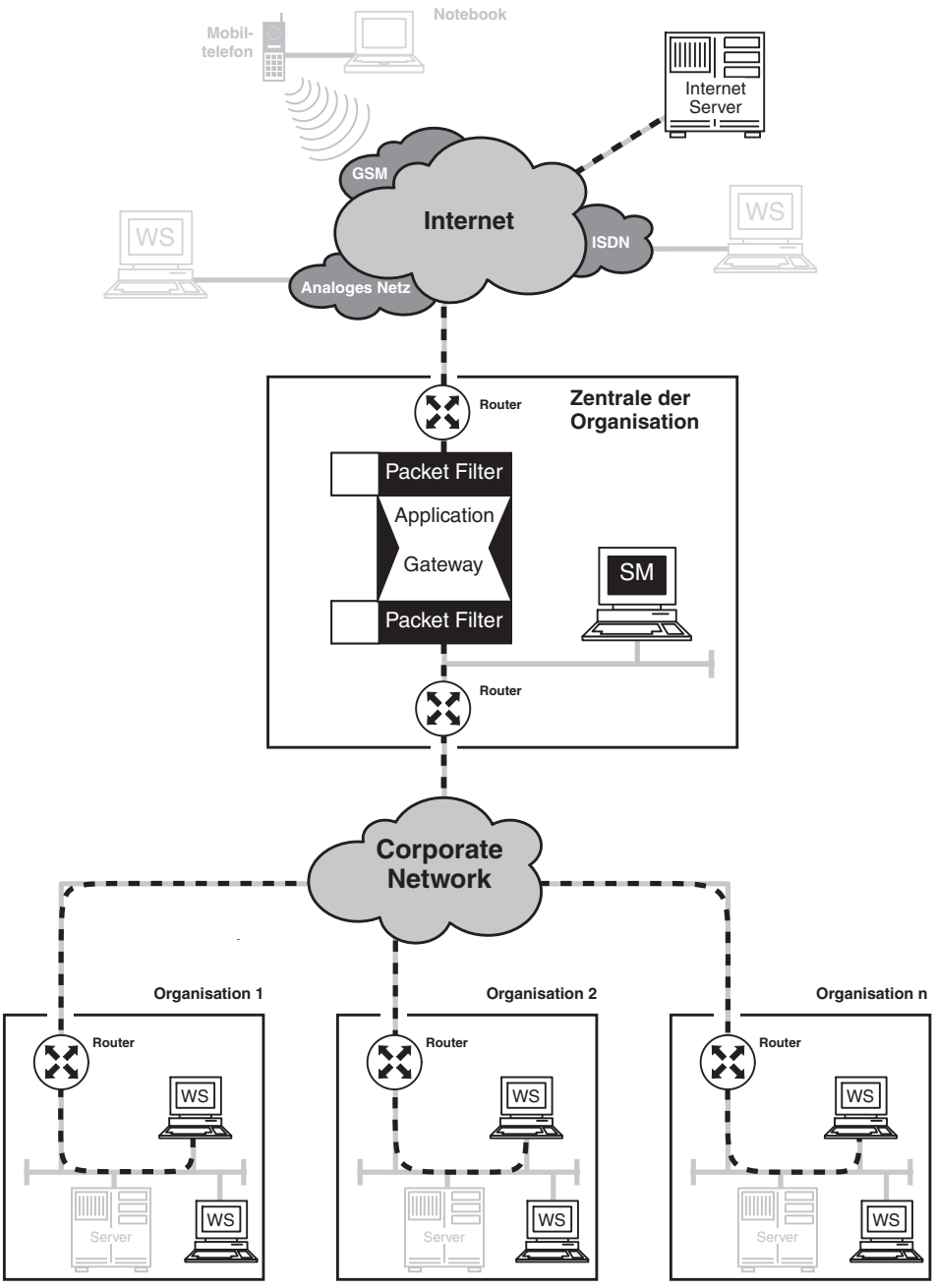


Abb. 10.2: Anbindung eines Intranet an das Internet

neuKap10.fm Seite 301 Freitag, 18. Oktober 2002 3:52 15

10.2 Internet Server

Die Internet Server, die für die Öffentlichkeit bestimmte Informationen oder Dienste zur Verfügung stellen, sind besonders gut vor oder neben einem High-level-Security-Firewall-System positioniert. Mit dieser konzeptionellen Sicherheitsmaßnahme erübrigt sich ein Zugriff von Internet-Benutzern auf das Intranet über das High-level-Security-Firewall-System.

Internet Server werden entweder im äußeren Screened Subnet des High-level-Security-Firewall-Systems oder mit einem separaten Packet Filter angeschlossen (siehe Abb. 10.3 – linke Seite). Die Packet Filter sorgen z. B. dafür, dass nicht über jeden Dienst auf die Internet Server zugegriffen werden kann. Angriffe auf die Internet Server über die Packet Filter werden erkannt, protokolliert und, falls im Regelwerk definiert, als Spontane Meldung an das Security Management gesendet.

Möchte eine Organisationseinheit die Internet Server in ihrer Organisationseinheit selbst bereitstellen, kann dies mit einer verschlüsselten Kommunikation aus dem Internet über das Corporate Network sicher realisiert werden.

Dazu werden Packet Filter mit Verschlüsselungsfunktionen (VPN-Gateways) im zentralen Zugang der Organisation sowie in der Organisationseinheit installiert. Die Kommunikation über das Internet passiert die VPN-Gateways der Zentrale und läuft in verschlüsselter Form weiter durch das Corporate Network bis zur betreffenden Organisationseinheit. Hier werden die Pakete vom VPN-Gateway der Organisationseinheit wieder entschlüsselt und gelangen im Klartext zum Internet Server. Auf diese Weise wird ein »Virtual Private Network« (VPN) realisiert.

Die Internet Server der einzelnen Einheiten der Organisation haben offizielle Internet-Adressen. Damit Angriffe aus dem Internet auf die Komponenten der Organisationeinheit zuverlässig verhindert werden können, dürfen diese Internet Server keine Verbindung zum LAN der Organisationseinheit haben (organisatorische Sicherheitsmaßnahme!). Die Internet Server von Organisationseinheiten im Corporate Network können nur durch Verschlüsselung sicher an das Internet angekoppelt werden.

In Abbildung 10.3 – rechte Seite – scheint der Kommunikationsfluss das High-level Security Firewall-System, den »Common Point of Trust«, zu umgehen. Hier findet die Kommunikation jedoch auf einer anderen logischen Ebene statt, da alle Pakete verschlüsselt werden. Die Vermischung von Paketen wird durch die Verschlüsselung ausgeschlossen.

neuKap10.fm Seite 302 Freitag, 18. Oktober 2002 3:52 15

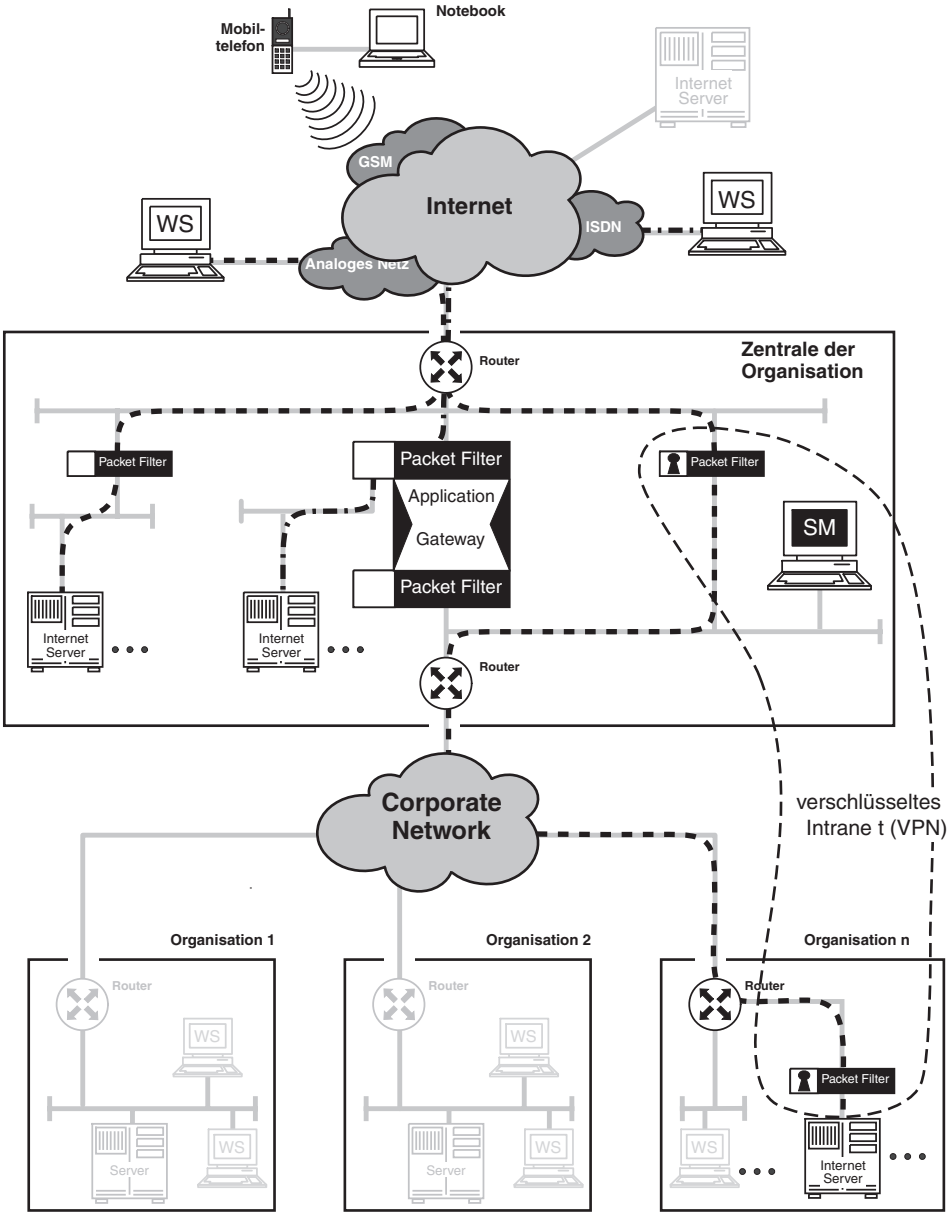


Abb. 10.3: Internet Server

neuKap10.fm Seite 303 Freitag, 18. Oktober 2002 3:52 15

10.3 Intranet Security (VPN)

Die Sicherung des Intranet kann auf folgende Weise realisiert werden:

VPN-Gateways verschlüsseln die Kommunikation über das Corporate Network, sodass keine Daten im Klartext gelesen werden können. Die Verschlüsselung bewirkt eine implizite Authentikation, die beispielsweise Trittbrettfahren und Maskerade-Angriffe verhindert.

In der Rechteverwaltung des VPN-Gateway kann festgelegt werden, von welchen Rechnersystemen (z. B. Internet Servern, Workstations) zu welcher Zeit bestimmte Anwendungen (Dienste) genutzt werden dürfen.

Sicherheitsrelevante Ereignisse werden von den VPN-Gateways erkannt, im Logbuch gespeichert und, falls gewünscht, als Warnmeldung an das Security Management gesendet (siehe Abb. 10.4). Dadurch können Sicherheitsverletzungen festgestellt werden.

In den einzelnen Organisationseinheiten werden die VPN-Gateways direkt hinter den Routern positioniert. In der Zentrale werden die Intranet Server im inneren Screened Subnet des High-level-Security-Firewall-Systems oder mit einem separaten VPN-Gateway angeschlossen.

Für die Intranet Server, die im internen Screened Subnet des High-level-Security-Firewall-Systems positioniert sind, kann die Kommunikation auch über die Proxies des Application Gateway (dann als single homed Application Gateway) geleitet werden. In diesem Fall können zusätzliche Sicherheitsdienste wie Benutzerauthentikation und Protokollierung der Handlungen von Benutzern genutzt werden. Für solche erweiterten Sicherheitsdienstleistungen ist es auch möglich, ein eigenes Application Gateway zur Verfügung zu stellen.

Die Kommunikation der Organisationseinheiten untereinander wird ebenfalls mithilfe von VPN-Gateways kontrolliert und gesichert.

neuKap10.fm Seite 304 Freitag, 18. Oktober 2002 3:52 15

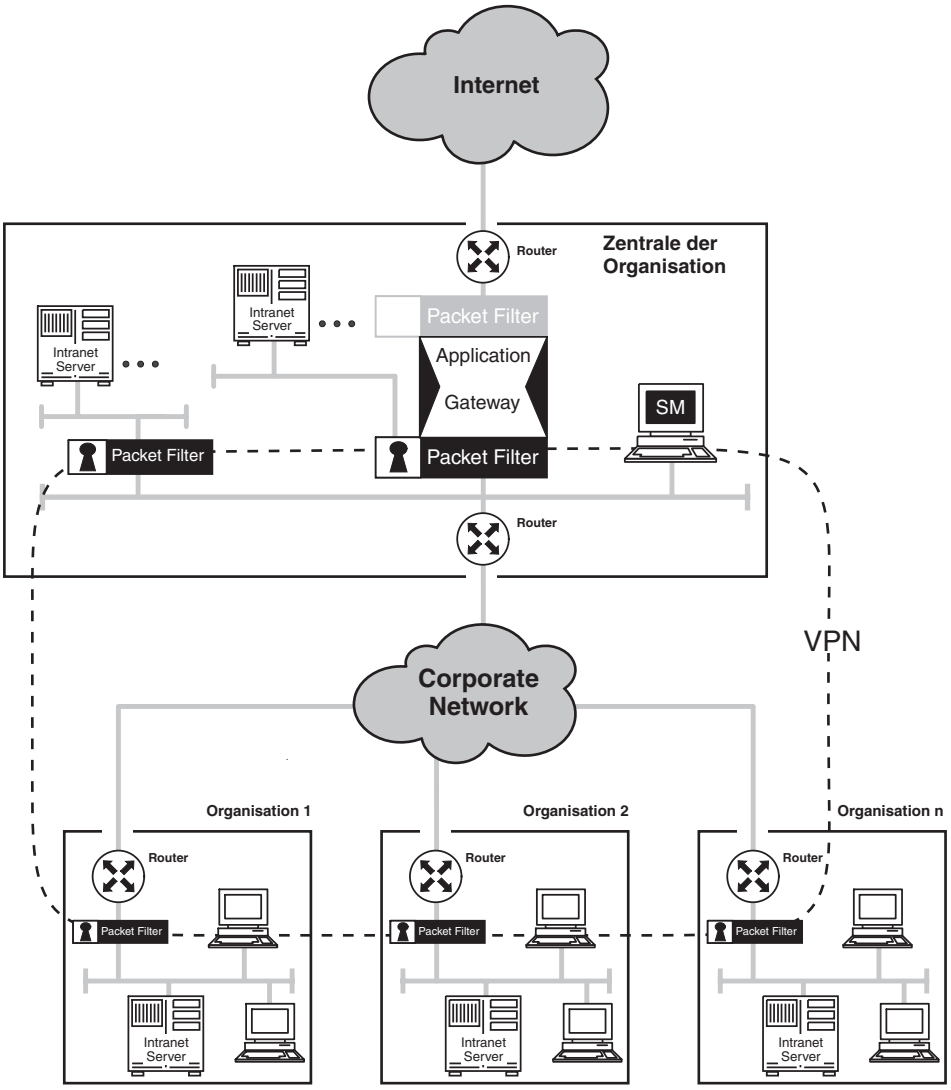


Abb. 10.4: Intranet Security mit VPN-Gateways

10.3.1 Höhere End-to-End-Sicherheit

Je nach Schutzbedarf und Anzahl der Rechnersysteme in einer Organisationseinheit kann es empfehlenswert sein, in den Rechnersystemen PC-Security-Komponenten einzusetzen, sodass direkt im Rechnersystem verschlüsselt werden kann. Damit wird eine höhere oder tiefere End-to-End-Sicherheit erreicht, die den LANs der einzelnen Organisationseinheiten Vertraulichkeit garantiert (siehe Abb. 10.5).

neuKap10.fm Seite 305 Freitag, 18. Oktober 2002 3:52 15

Vertrauliche und kontrollierte Kommunikation kann auch in den Organisationseinheiten selbst mithilfe von PC-Security-Komponenten und VPN-Box »lokal« realisiert werden. Diese Sicherheitskomponenten können entweder vom zentralen Security Management oder von einem lokalen Security Management gesteuert und verwaltet werden.

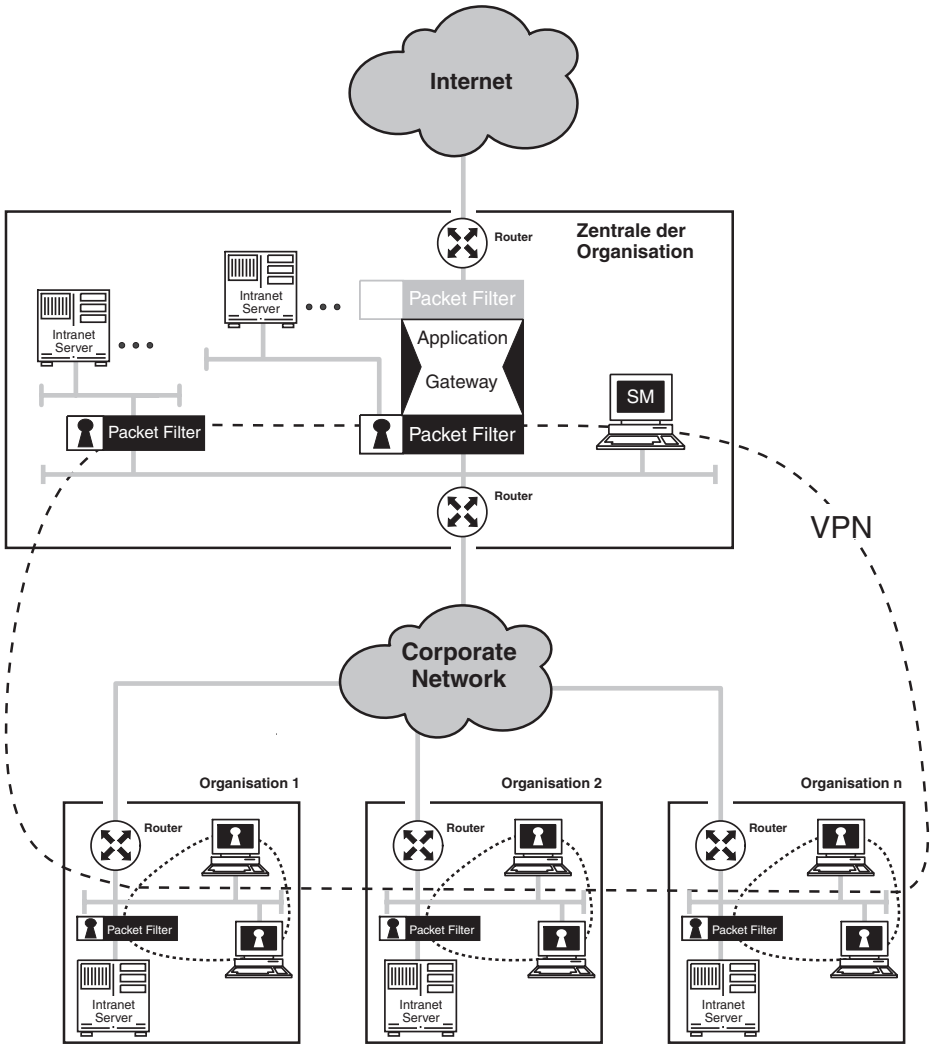


Abb. 10.5: Intranet Security mit PC Security Komponenten

neuKap10.fm Seite 306 Freitag, 18. Oktober 2002 3:52 15

10.3.2 Abschottung von Organisationseinheiten untereinander

Organisationseinheiten können sich auch gegeneinander abschotten: durch VPN-Gateways, durch Application Gateways oder ein High-level-Security-Firewall-System, je nach Schutzbedarf. Eine besondere Abschottung ist oft für Organisationseinheiten wie Vorstandsabteilung, Personalabteilung, arbeitsmedizinischer Bereich oder Forschungsabteilung notwendig, da der Schutzbedarf hier besonders hoch ist.

Wenn ein eigenes Application Gateway oder ein eigenes High-level-Security-Firewall-System eingesetzt wird, kann das Security Management in der Abteilung selbst realisiert werden (siehe Abb. 10.6).

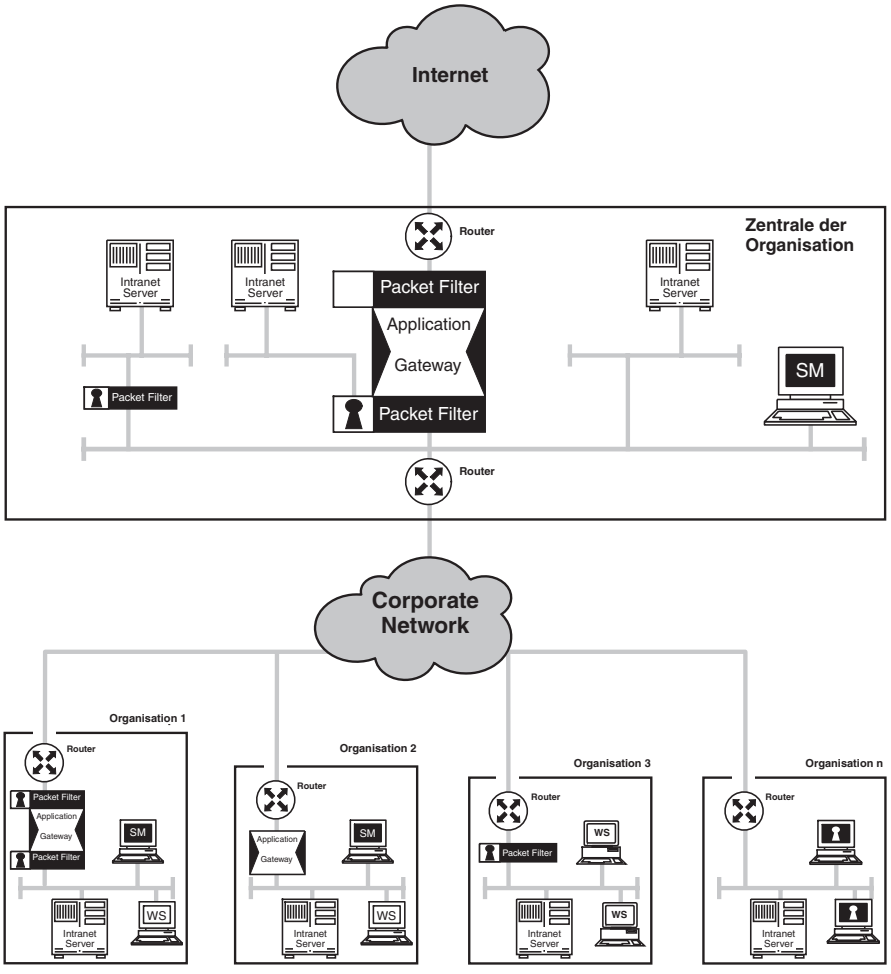


Abb. 10.6: Skalierbare Sicherheit

neuKap10.fm Seite 307 Freitag, 18. Oktober 2002 3:52 15

10.3.3 Skalierbare Sicherheit

Mit verfügbaren Sicherheitsmechanismen wie einem High-level-Security-Firewall-System, einem VPN-Gateway, einem Application Gateway oder/und einer PC-Security-Komponente kann dem Schutzbedarf der einzelnen Anwendungen entsprechend ein Sicherheitsmaß realisiert werden, das skalierbar ist:

- Informationen, die der ganzen Organisation zugänglich sein sollen, werden von Intranet Servern angeboten, in die keine Sicherheitsmechanismen integriert sind.
- Sicherheitsrelevante Daten werden durch das High-level-Security-Firewall-System, das Application Gateway oder separate VPN-Gateways effektiv geschützt.
- Hochsensible Bereiche in einzelnen Organisationseinheiten werden mit einem zusätzlichen separaten Application Gateway oder High-level-Security-Firewall-System abgeschottet.
- Die Organisationseinheiten werden ihrem Schutzbedarf entsprechend geschützt, einige mit VPN-Gateways, andere mit PC Security Komponenten, manche bleiben vielleicht ohne Sicherheitsmechanismen.

Das Security Management kann zentral oder dezentral (in den einzelnen Organisationseinheiten) durchgeführt werden, abhängig von den Verantwortungsbereichen und Erfordernissen in der jeweiligen Organisation.

10.4 Remote Access (Tele-Arbeit, Mobil-Arbeitsplätze)

Die Notwendigkeit, Rechnersysteme »remote« an das Intranet einer Organisation anzukoppeln, wird zunehmend größer.

Außendienstmitarbeiter benötigen direkten Zugriff auf Preislisten, Lieferzeiten und Bestellungen im Intranet, damit Arbeitsvorgänge effektiv und ohne Medienbruch durchgeführt werden können.

Im Hinblick auf die Veränderungen und Anforderungen der modernen Informationsgesellschaft wird es immer notwendiger, Heimarbeitsplätze anzubieten, die remote an das Intranet gekoppelt sind. Für Heimarbeitsplätze ist die Ankopplung über ISDN attraktiv, das sich zunehmend ausbreitet und eine hohe Geschwindigkeit bietet.

Notebooks können mit einem Modem über die Telefonleitung oder mit einem Mobiltelefon über das Mobilfunknetz (GSM-Netz) an das Intranet gekoppelt werden. Dabei ist zu beachten, dass in der Umgebung von Remote-Rechnern (z. B. Hotels) die Wahrscheinlichkeit eines Angriffs besonders hoch ist.

Im Sicherheitskonzept »Externe Anbindung« wird der geschützte Remote-Zugriff auf interne Intranet Server über das High-level-Security-Firewall-System oder spezielle Internet Server über VPN-Gateways ermöglicht. VPN-Gateway und PC-

neuKap10.fm Seite 308 Freitag, 18. Oktober 2002 3:52 15

Security-Komponenten machen es möglich, verschlüsselt über öffentliche Netze (analoges Netz, GSM, ISDN und überlagert das Internet) zu kommunizieren, wobei die Rechte der Zugreifenden durch das zentrale Security Management individuell definiert werden können.

Ein zentraler Übergang über ein High-level-Security-Firewall-System, der besonders gesichert ist, garantiert die vertrauliche und kontrollierte Ankopplung externer Benutzer, z.B. von Heimarbeitsplätzen, von mobilen Rechnersystemen von Außendienstmitarbeitern und von Kunden und Lieferanten (siehe Abb. 10.7).

Die Kombinationsmöglichkeit von VPN-Gateway und PC-Sicherheits-Komponenten bietet ein einfaches Konzept, mit dem das notwendige Maß an Sicherheit für die Kommunikation über unsichere Netze zur Verfügung gestellt wird: IP-Pakete werden in verschlüsselter Form über ISDN, das Fernsprechnetz oder das Mobilfunknetz gesendet und von Packet-Filtern mit Verschlüsselungsfunktion als zentraler Stelle wieder entschlüsselt.

Durch Verschlüsselung wird ein kryptographisches »Virtual Private Network (VPN)« im unsicheren Netz gebildet.

Falls der Remote-Zugriff über das High-level-Security-Firewall-System auf die Intranet Server zentral oder lokal bei den einzelnen Organisationseinheiten stattfindet, können alle hier vorhandenen Sicherheitsdienste genutzt werden. Neben der Verschlüsselung sind das z.B. Benutzerauthentikation, Rechteverwaltung der Anwendungen, Beweissicherung der Handlungen.

neuKap10.fm Seite 309 Freitag, 18. Oktober 2002 3:52 15

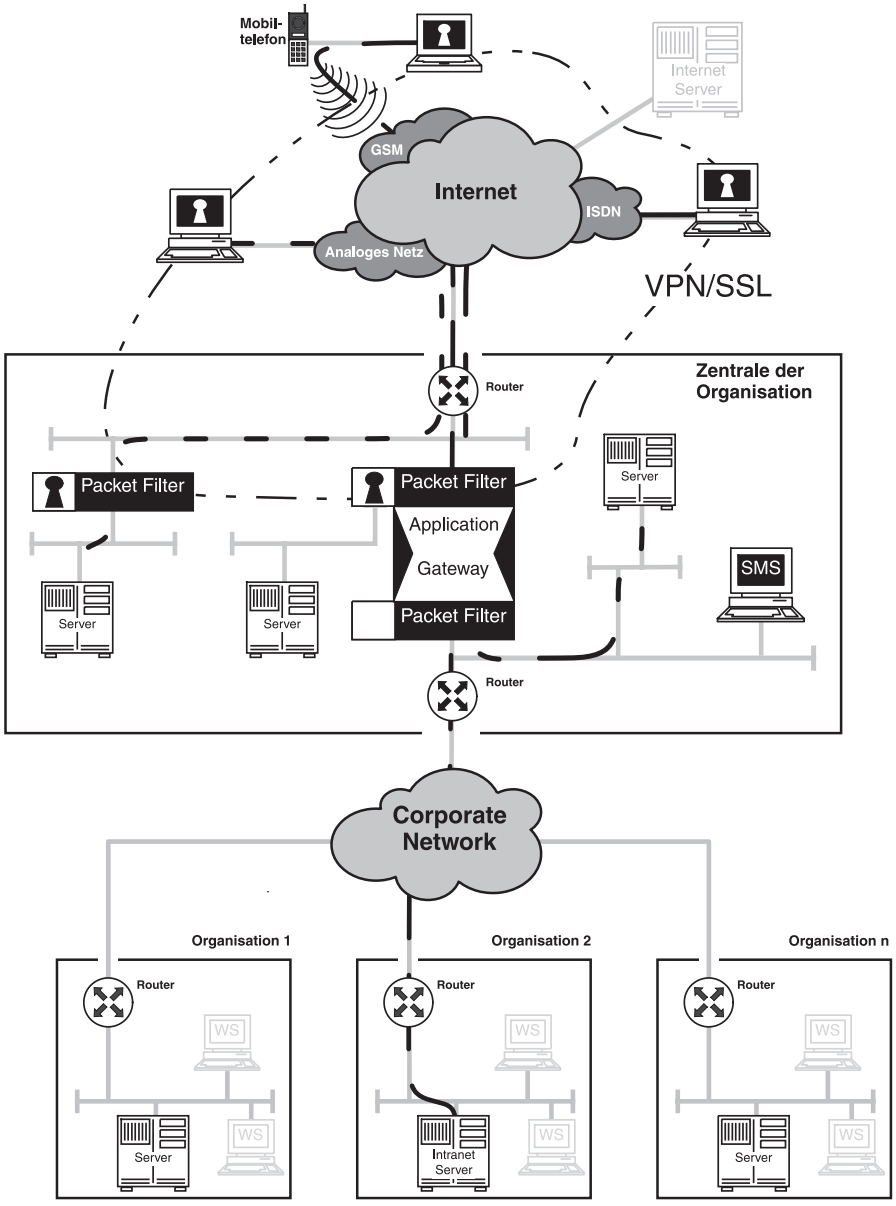


Abb. 10.7: Anbindung externer Anschlusspunkte

10.5 Ankopplung besonderer Organisationseinheiten

Es gibt sicherlich auch Organisationeinheiten, die über das High-level-Security-Firewall-System an das Intranet angekoppelt werden sollten, weil hierdurch ein höherer Schutz erreicht werden kann.

neuKap10.fm Seite 310 Freitag, 18. Oktober 2002 3:52 15

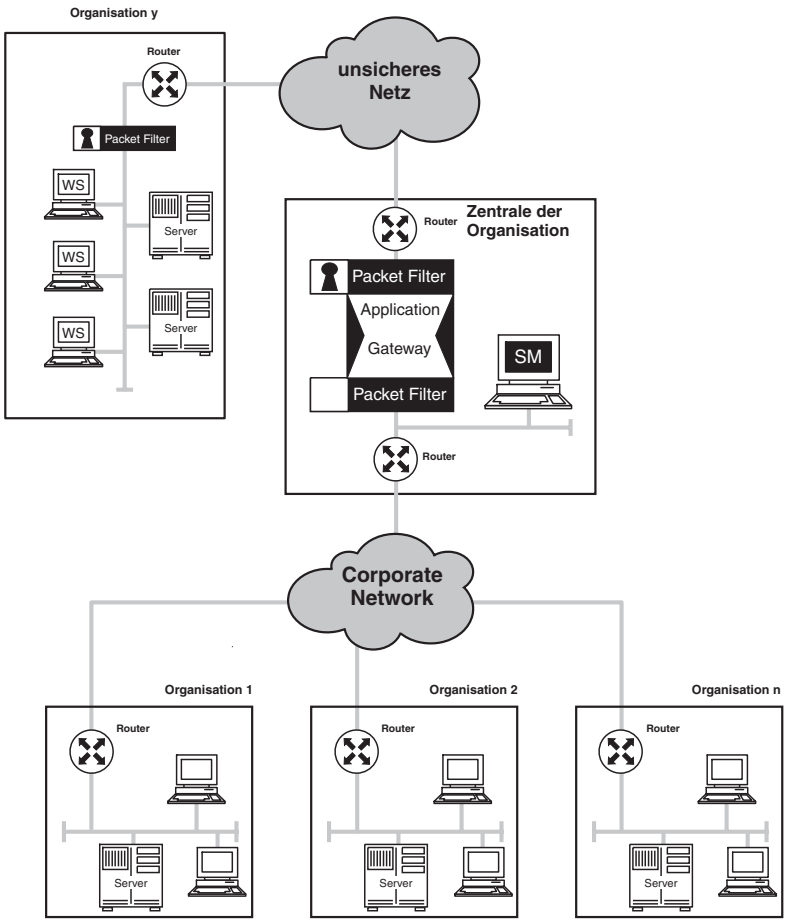


Abb. 10.8: Ankopplung besonderer Organisationseinheiten

Bei dieser Art der Ankopplung muss jeder Benutzer aus der Organisationseinheit Y eine Identifikation und Authentikation mit dem High-level-Security-Firewall-System durchführen. Außerdem können so bestimmte Dienste auf der Applikationsebene eingeschränkt und kontrolliert werden. Bestimmte Aktionen von Benutzern können durch die Protokollierung der Verbindungsdaten für eine Beweissicherung festgehalten werden. Durch die VPN-Gateways wird eine vertrauliche und kontrollierte Kommunikation über das unsichere Netz erreicht.

Organisationseinheiten, die einen geringeren Schutzbedarf haben und eventuell an andere unsichere Netze angeschlossen sind, können auf diese Weise an das Intranet angeschlossen werden. Die Steuerung und Verwaltung des Packet Filter in der Organisationseinheit Y kann vom zentralen Security Management aus realisiert werden. Diese Maßnahme sichert das Konzept des »Common Point of Trust«.

neuKap10.fm Seite 311 Freitag, 18. Oktober 2002 3:52 15

10.6 Externe Modem-Anschlüsse

Aus Gründen der Sicherheit sollten Modems für den Zugriff auf externe Rechnersysteme innerhalb einer Organisation nur zentral zur Verfügung gestellt werden. Zu diesem Zweck wird ein Modem Server vor dem Firewall-System im unsicheren Bereich positioniert. Wenn ein Mitarbeiter der Organisation ein Modem verwenden will, kann er nach einer Identifikation und Authentikation mit dem High-level-Security-Firewall-System auf den Modem Server zugreifen (z. B. über Telnet) und damit die Modem-Funktionalität von seinem Rechnersystem aus nutzen. Mit dem zentralen Modem-Pool, welches über das High-level-Security-Firewall-System erreichbar ist, kann das Konzept des »Common Point of Trust« beibehalten werden. Mithilfe des Security Management kann im Einzelnen festgelegt werden, welche Benutzer in welchen Zeiträumen und an welchen Wochentagen auf ein extern angebotenes Modem zugreifen dürfen. Die entsprechenden Aktionen können protokolliert und ausgewertet werden.

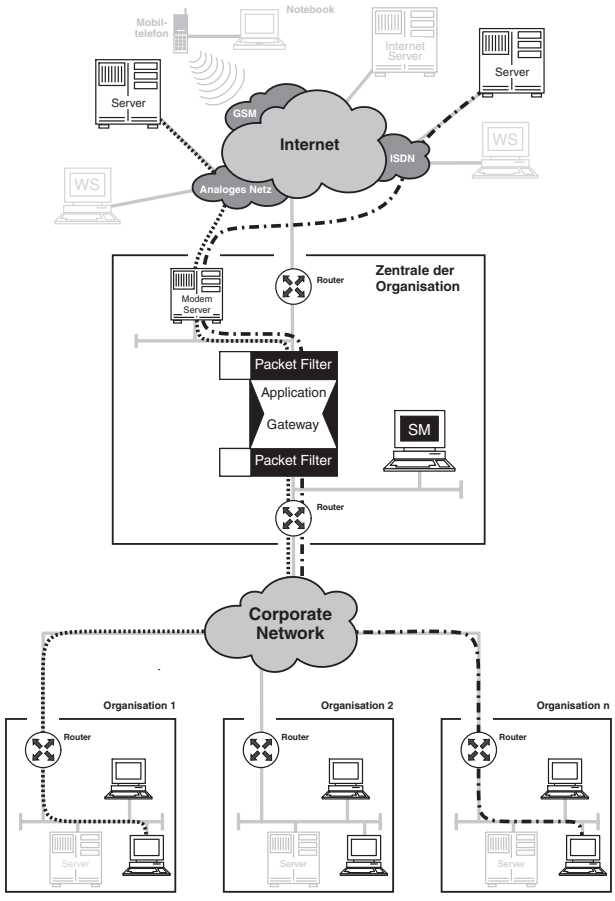


Abb. 10.9: Externe Modems

neuKap10.fm Seite 312 Freitag, 18. Oktober 2002 3:52 15

10.7 Modem-Verbindungen aus dem unsicheren Netz in das zu schützende Netz

Ein Modem Server im zu schützenden Netz kann in Verbindung mit dem High-level-Security-Firewall-System eine Wartungsfirma kontrollieren, die z. B. für ein UNIX-System die Wartung auf unterstem Level über die serielle Schnittstelle realisieren muss. Dieses Problem kann auf verschiedene Arten gelöst werden:

Variante a):

Vom Modem Server wird eine serielle Schnittstelle zum Rechnersystem, das gewartet werden soll, gelegt (siehe Abb. 10.10 *Organisationseinheit 1*)

Variante b):

In der Zentrale wird ein Modem Server installiert. Die dort angeschlossenen Modems bauen über die interne TK-Anlage eine Verbindung auf und können so ihr Ziel erreichen. Dem Server steht dann ein Modem für die interne Kommunikation zur Verfügung (siehe Abb. 10.10 *Organisationseinheit n*). Voraussetzung bei dieser Variante ist, dass nicht von außen auf die TK-Anlage zugegriffen werden kann. Zusätzliche nicht-technische Sicherheitsmaßnahmen müssen ergriffen werden, um diese Voraussetzung zu erfüllen.

Ablauf

Wenn die Wartungsfirma aus dem unsicheren Netz für Wartungszwecke auf das interne Rechnersystem zugreifen will, muss der jeweilige Mitarbeiter der Wartungsfirma eine Identifikation und Authentikation über das High-level-Security-Firewall-System durchführen und kann dann z. B. über eine Telnet-Session, die im High-level-Security-Firewall-System protokolliert wird, auf den Modem Server zugreifen und dort auf dem untersten Level die Wartungsarbeiten ausführen. Dieses Verfahren bietet ein Höchstmaß an Kontrollierbarkeit und Protokollierbarkeit und ermöglicht dennoch eine Fernwartung ohne Verwendung eines externen Modems am zu wartenden Rechnersystem. Im Logbuch werden die Handlungen des Mitarbeiters der Wartungsfirma für eine eventuelle Beweissicherung festgehalten.

neuKap10.fm Seite 313 Freitag, 18. Oktober 2002 3:52 15

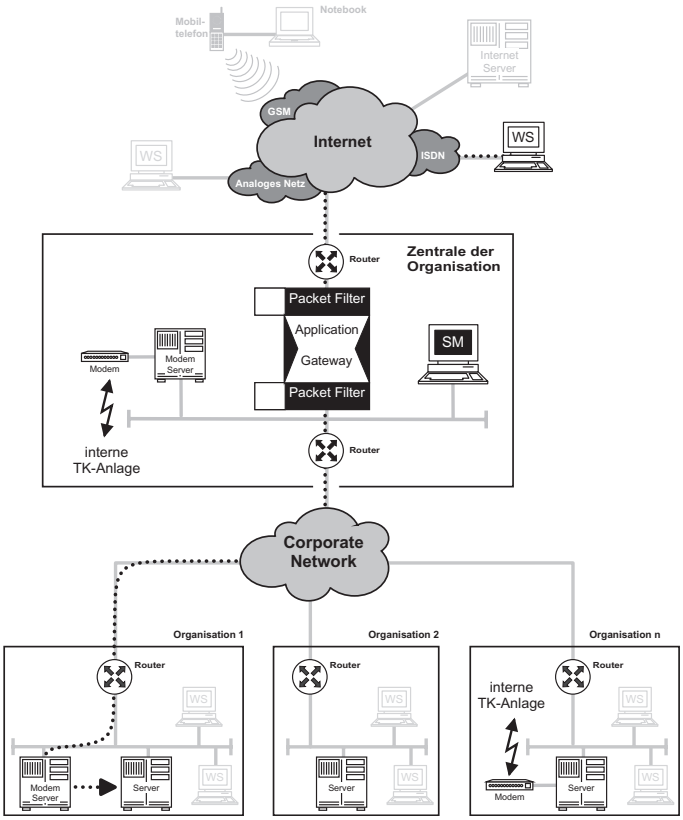


Abb. 10.10: Interne Modems

10.8 Virengefahr

Besonders zu beachten beim Austausch von Dateien als Anhänge von Mails oder WWW-Dokumenten ist die Gefahr, dass neben der eigentlichen Information (Daten, Programme) so genannte Malware (Viren, Würmer, Trojanische Pferde, ...) mitgesendet wird, die im Prinzip immer dem Empfänger schaden soll. Im Folgenden wird in diesem Kapitel immer von Viren gesprochen, obwohl dies in anderer Form auch Würmer, Trojanische Pferde usw. sein können.

Die Virengefahr ist nicht zu unterschätzen und wird durch die Ankopplung an unsichere Netze wie das Internet besonders brisant. Aus diesem Grund müssen wirkungsvolle Sicherheitsmechanismen eingeführt werden, um Risiken beherrschen und die Verletzbarkeit verringern zu können.

Zur Erkennung von Viren gibt es so genannte Viren-Scanner, die zentral oder auf einzelnen Rechnersystemen nach bekannten Viren suchen. Falls sie in einer Datei einen Virus gefunden haben, zeigen sie dies als sicherheitsrelevantes Ereignis an.

neuKap10.fm Seite 314 Freitag, 18. Oktober 2002 3:52 15

Generelles Problem bei der Erkennung von Viren:

Da es eine Vielzahl unterschiedlicher Viren gibt und jeden Tag neue hinzukommen, können Viren-Scanner nicht alle Viren erkennen. Das bedeutet, dass es auch mithilfe von Viren-Scannern keinen hundertprozentigen Schutz vor Viren geben kann. Bei der Übertragung von Dateien ist die Erkennungsrate von Viren noch weniger vorhersagbar.

Kompression von Dateien

Daten, die übertragen werden sollen, werden in der Regel mit Kompressionsverfahren reduziert (»gezipt«), damit eine geringere Menge an Bytes übertragen werden muss. Viren-Scanner suchen aber in einer Originaldatei nach Viren. Bei der Übertragung von komprimierten Dateien muss zuerst eine De-Kompression durchgeführt werden, bevor nach Viren gesucht werden kann. Viren-Scanner können diese Anforderung nur erfüllen, wenn standardisierte Kompressionsverfahren (wie z. B. ZIP) verwendet werden. Falls keine Standard-Kompressionsverfahren verwendet werden, haben die Viren-Suchprogramme keine Chance, Viren zu finden. Die Erkennungsrate für bekannte Viren wird hier schlechter.

Verschlüsselung der Dateien

Bei der Übertragung von objekt-verschlüsselten Dateien in Mails oder beim Filetransfer hat der Viren-Scanner überhaupt keine Möglichkeit, Viren zu erkennen, da in der Regel nur der Empfänger in der Lage ist, die Dateien zu entschlüsseln.

Da die Nutzung der Verschlüsselung von Dateien über unsichere Netze in Zukunft immer größer wird, wird hier die Erkennungsrate der Viren-Scanner immer kleiner.

Das bedeutet nicht, dass Viren-Scanner Viren in Dateien während der Übertragung nicht erkennen können. Aber es muss berücksichtigt werden, dass die Erkennungsrate unterschiedlich hoch sein wird.

10.8.1 Integration von Viren-Scannern am Common Point of Trust

Verschiedene Sicherheitsmaßnahmen können eingeführt werden, um die Ankopplung eines zu schützenden Netzes an ein unsicheres Netz virensicherer zu gestalten. Im Folgenden sollen einige Möglichkeiten diskutiert werden.

Integration eines Viren-Scanners im zentralen Mail Server

Der zentrale Mail Server wird um einen Viren-Scanner erweitert. Dadurch können alle Mail-Dateien überprüft werden, die über den zentralen Mail Server aus dem unsicheren Netz in das zu schützende Netz übertragen werden.

Vorteil: Da keine zusätzliche Hardware benötigt wird, ist diese Lösung kostengünstig. Mit entsprechender Konfiguration kann der Viren-Scanner zentral eingesetzt werden, sodass alle hereinkommenden Mails überprüft werden können.

Nachteil: Dienste wie HTTP und FTP werden nicht geschützt.

neuKap10.fm Seite 315 Freitag, 18. Oktober 2002 3:52 15

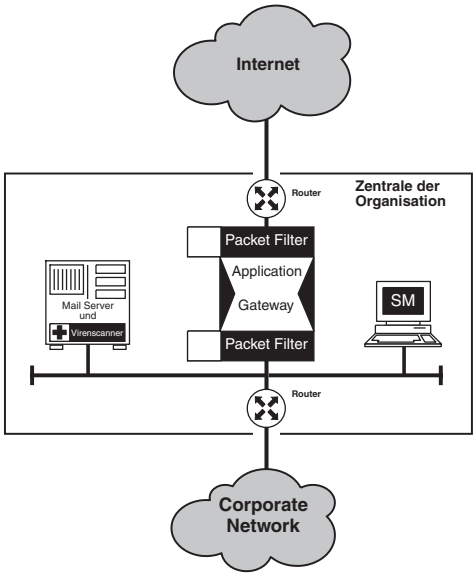


Abb. 10.11: Viren-Scanner im zentralen Mail Server

Zentraler Viren-Scanner im Intranet

Bei dieser Lösung wird ein Viren-Scanner im Intranet als Single-homed-Lösung zentral realisiert.

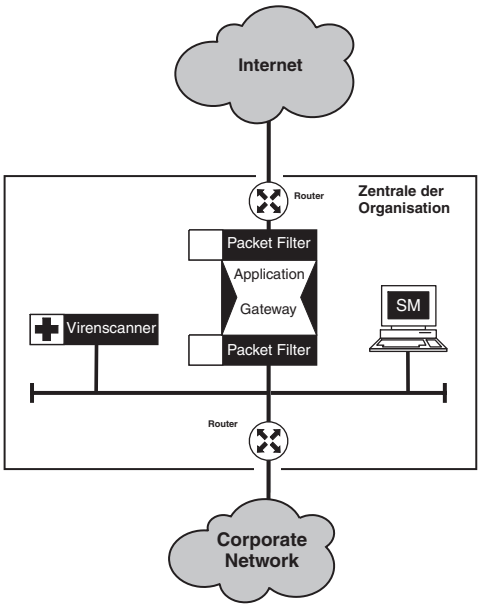


Abb. 10.12: Viren-Scanner im Intranet

neuKap10.fm Seite 316 Freitag, 18. Oktober 2002 3:52 15

Vorteil: Alle Dienste können genutzt werden, sofern der Viren-Scanner dafür gerüstet ist. Viren-Scanner dieser Art arbeiten im Transparentmodus, sodass die Benutzerfragen an das Firewall-System weitergegeben werden und die Benutzer keine neuen Verhaltensweisen lernen müssen.

Nachteil: Durch die Integration als Single-homed-Gateway sind die IP-Adressen der Rechnersysteme aus dem Intranet dem Firewall-System nicht mehr bekannt. Das Firewall-System sieht nur noch die IP-Adresse des Viren-Scanners.

Der Viren-Scanner arbeitet im Store-and-forward-Betrieb, d.h., er nimmt zunächst die ganze Datei auf, überprüft sie und sendet sie dann weiter. Diese Methode bedeutet ein anderes Zeitverhalten der Dateiübertragung für den Benutzer.

Viren-Scanner als Single-homed Gateway-Lösung im Inneren des Screened Subnet

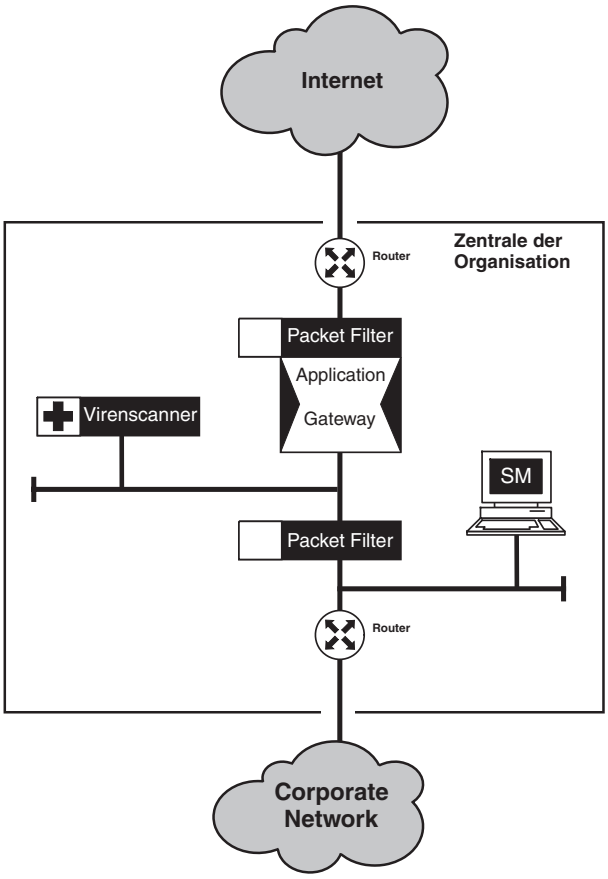


Abb. 10.13: Viren-Scanner im Inneren des Screened Subnet

neuKap10.fm Seite 317 Freitag, 18. Oktober 2002 3:52 15

Vorteil: Der innere Packet Filter schützt auch den Viren-Scanner und kontrolliert die IP-Adressen der Rechnersysteme im Intranet.

Nachteil: wie Viren-Scanner im Intranet

Viren-Scanner im äußeren Screened Subnet

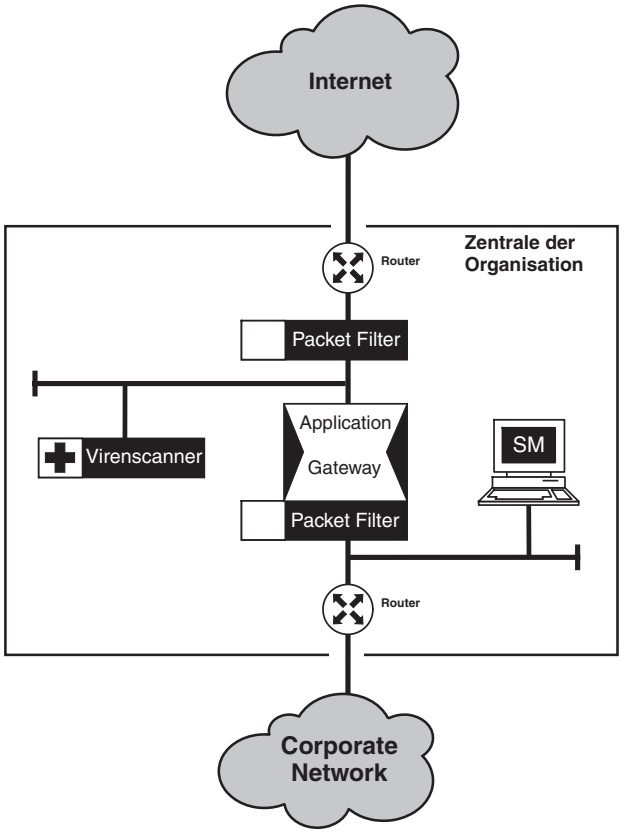


Abb. 10.14: Viren-Scanner im äußeren Screened Subnet

Vorteil: Das Application Gateway des Firewall-Systems kann die IP-Adressen im Intranet überprüfen. Der Viren-Scanner wird durch das äußere Packet Filter geschützt und tritt nach außen als single-homed-Lösung auf.

Nachteil: Das Application Gateway des Firewall-Systems kann die IP-Adressen aus dem unsicheren Netz nicht mehr erkennen und berücksichtigen. Die Identifikation und Authentikation muss daher auf die Benutzer reduziert werden.

neuKap10.fm Seite 318 Freitag, 18. Oktober 2002 3:52 15

Integration von verschiedenen Viren-Scannern

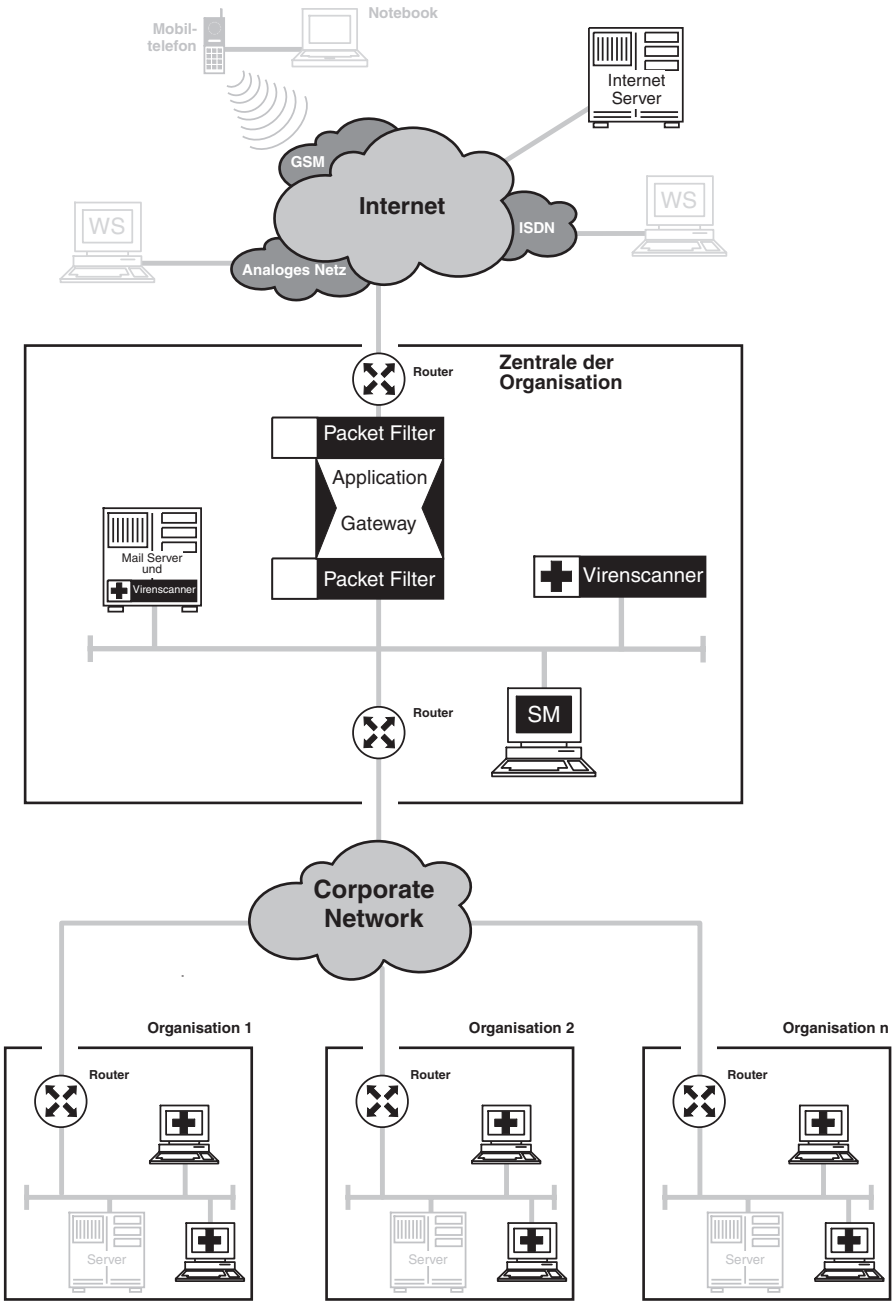


Abb. 10.15: Integration von verschiedenen Viren-Scannern

neuKap10.fm Seite 319 Freitag, 18. Oktober 2002 3:52 15

Abbildung 10.15 zeigt einen zentralen Viren-Scanner im inneren Screened Subnet als Single-homed-Lösung für die Dienste HTTP und FTP. Zusätzlich wird ein Viren-Scanner auf dem zentralen Mail Server für alle Mails sowie mehrere Viren-Scanner auf den Rechnersystemen aller Benutzer implementiert. Weitere Sicherheitsmaßnahmen (s. u.) werden ebenfalls berücksichtigt.

Vorteil: Der zentrale Viren-Scanner ist nicht mehr für alle Aufgaben zuständig, seine Aufgaben werden auf verschiedene Stellen verteilt.

10.8.2 Weitere technische, personelle und organisatorische Maßnahmen

Gegen die Virengefahr reicht eine zentrale Sicherheitskomponente nicht aus!

Risiken für die Rechnersysteme des zu schützenden Netzes, die bei der Ankopplung an unsichere Netze hinsichtlich der Virenproblematik auftreten, können nicht einzig und allein mit einem zentralen Virenscanner ausgeschlossen werden und auch nicht mit mehreren Virenscannern. Ein wirkungsvoller Schutz kann nur dann gegeben sein, wenn weitere technische, personelle und organisatorische Sicherheitsmaßnahmen ergriffen werden, mit denen die Risiken abschätzbar und damit beherrschbar gemacht werden können.

Weitere technische Sicherheitsmaßnahmen: Input-Subdirectory mit lokalen Viren-Scanner

Technisch sollte den Mitarbeitern der Organisation, die z. B. über FTP oder andere Dienste aus dem unsicheren Netz Dateien in das zu schützende Netz übertragen, auf ihren Rechnersystemen im zu schützenden Netz ein Input-Subdirectory eingerichtet werden. In diesem Input-Subdirectory werden alle Dateien geladen, die in das zu schützende Netz importiert werden. Hier muss die Möglichkeit geschaffen werden, durch einen einfachen Mausklick auf dem Rechnersystem (lokal) einen Viren-Scanner anzustoßen, der die Input-Dateien auf Viren untersucht. Diese Virenüberprüfung sollte vom Viren-Scanner in ein Logbuch protokolliert werden, damit mit dem Logbuch des lokalen Viren-Scanners auf dem Rechnersystem und dem zentralen Viren-Scanner des Firewall-Systems der richtige Umgang mit den Input-Dateien beweisbar dargestellt werden kann.

Personelle Sicherheitsmaßnahmen

Die Mitarbeiter müssen genaue Instruktionen erhalten, wie mit Input-Dateien umgegangen werden soll, und sich darüber hinaus verpflichten, das beschriebene Verfahren zur Virenerkennung einzuhalten. Die Mitarbeiter sind nur dann in der Lage, die Sicherheitspolitik einer Organisation zu unterstützen, wenn sie diese auch kennen und ihre Umsetzung mit den entsprechenden Hilfsmitteln bewerkstelligen können.

neuKap10.fm Seite 320 Freitag, 18. Oktober 2002 3:52 15

Organisatorische Sicherheitsmaßnahmen

Die Betreuung und Beratung von Benutzern, die Dateien aus unsicheren Netzen importieren, ist eine wichtige organisatorische Sicherheitsmaßnahme. Der Einsatz von Viren-Scannern erfordert eine Schulung der Benutzer. Neben der Schulung, die die Benutzer in die Lage versetzt, die Viren-Scanner sachgerecht zu nutzen, bedarf es einer Betreuung und Beratung der Benutzer für die im laufenden Betrieb auftretenden Probleme, insbesondere dann, wenn ein Viren-Scanner Viren gefunden hat.

10.9 Intrusion-Detection-Systeme

Der Einsatz von Intrusion-Detection-Systemen ermöglicht es, Sicherheitsverletzungen bereits im Vorfeld zu erkennen und somit noch bevor ein Schaden auftritt, Gegenmaßnahmen einzuleiten.

Intrusion-Detection-Systeme arbeiten grundsätzlich mit zwei Analysekonzepten:

1. Das Aufspüren bekannter Angriffe mithilfe von Signaturanalysen
2. Die Erkennung von Anomalien, die auf IT-Sicherheitsverletzungen hindeuten

Die Praxis zeigt, dass es sinnvoll ist, Analysekomponenten einerseits ins Internet zu stellen, um somit Angriffe von außen frühzeitig zu erkennen, aber gleichzeitig eine weitere Analysekomponente in das interne Netz zu stellen, um Angriffe von innen erkennen zu können.

Von besonderer Bedeutung beim Einsatz von Intrusion-Detection-Systemen ist die organisatorische Einbindung: Sie müssen so eingebunden werden, das immer auch definiert wird, welche Schritte einzuleiten sind, wenn ein Angriff erfolgt ist.

Hierbei sind z.B. die folgenden Punkte zu beachten:

- Abschaltung des Firewall-Systems oder Teile des Firewall-Systems
- Benachrichtigung des verantwortlichen Administrators
- Analyse, von wem der Angriffsversuch durchgeführt wurde, um weitere Angriffe verhindern zu können

Intrusion-Detection-Systeme werden im Kapitel 13.7 ausführlich besprochen.

neuKap10.fm Seite 321 Freitag, 18. Oktober 2002 3:52 15

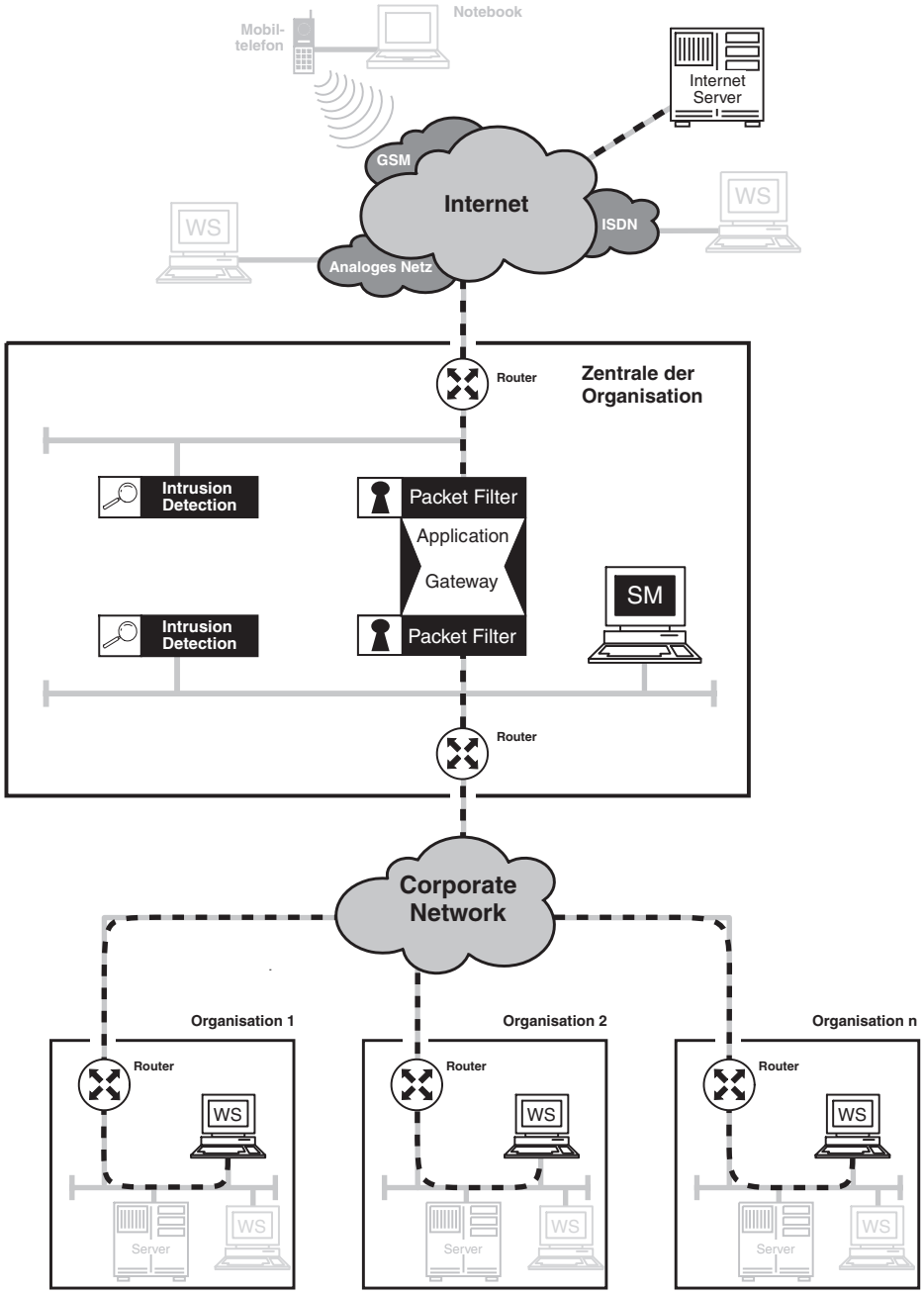


Abb. 10.16: Einbindung von Intrusion-Detection-Systemen

neuKap10.fm Seite 322 Freitag, 18. Oktober 2002 3:52 15

10.10 Personal Firewall

Eine Personal Firewall ist für den Einsatz von Desktop-PCs oder Notebooks gedacht, die z. B. über Internet-Provider per Wählverbindung (Analognetz, ISDN, GSM, ...) direkt auf das Internet zugreifen. Eine Personal Firewall arbeitet im Hintergrund, wird also vom Anwender bei der Arbeit nicht bemerkt.

Die Funktionalitäten dieser Software-Lösungen bestehen meistens aus

- Packet-Filter-Funktionalität,
- Ressourcen-Schutz (Dateien, Ports, ...) und
- Schutz vor Cookies, Applets, ActiveX-Controls /Alad99/.

Die einfachen Lösungen einer Personal Firewall (»light-Version«) werden durch den Benutzer selber verwaltet, die Enterprise-Lösungen werden von einem zentralen Security Management System verwaltet, um eine unternehmensweite Security Policy realisieren zu können.

Manche Hersteller haben angekündigt, die Personal Firewall mit VPN-Lösungen und/oder Anti-Virus-Lösungen zu kombinieren /Woel99/.

Praktische Realisierung

Um ein Höchstmaß an Sicherheit zu erreichen, ist es empfehlenswert, die Rechnersysteme zusätzlich zum Betrieb eines zentralen Firewall-Systems und anderen Sicherheitsmechanismen mit Personal Firewalls auszustatten, siehe Abbildung auf der nächsten Seite. So wird eine umfangreiche Sicherheit für die Ressourcen einer Organisation erreicht. Dies gilt sowohl für die Notebooks der mobilen Arbeitsplätze als auch für die Desktop-Telearbeitspätze und die Arbeitsplätze in der Organisation selber.

Zentrale Verwaltung

Mithilfe der zentralen Verwaltung der Personal Firewall sind Organisationen in der Lage, organisationsweit die eigene Sicherheitspolitik einfach, kostengünstig und sicher umzusetzen. Der Administrator kann anwendungs- und/oder benutzerorientiert die Rechte definieren, die mithilfe der Personal Firewall überwacht werden. Alle notwendigen Eintragungen zur Konfigurierung der Personal Firewall in der Organisation werden zentral durchgeführt und online auf die Rechnersysteme verteilt.

Mithilfe der Personal Firewall kann die durch die steigende Nutzung der Internet-Dienste zunehmende Verwundbarkeit der elektronischen Werte auf dem PC stark reduziert werden.

Die Einbindung von Personal Firewalls wird ausführlich im Kapitel 13.9 besprochen.

neuKap10.fm Seite 323 Freitag, 18. Oktober 2002 3:52 15

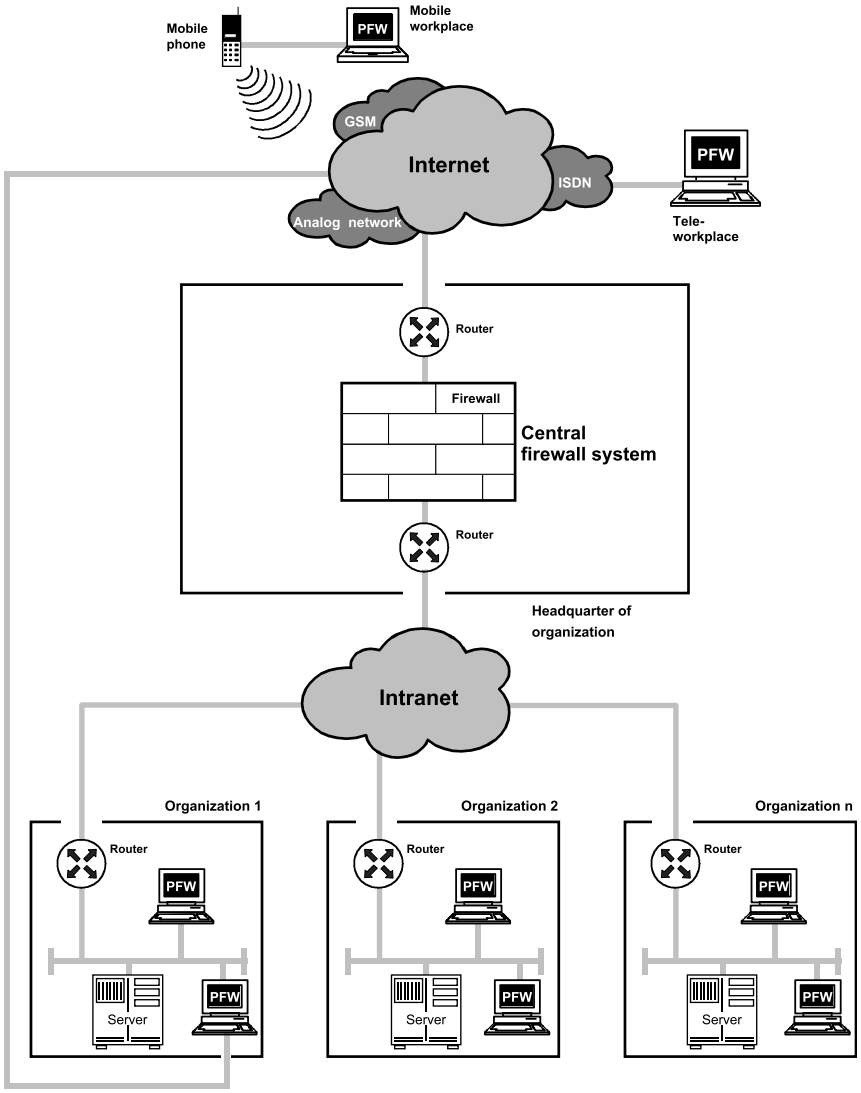


Abb. 10.17: Organisation mit Personal Firewalls

10.11 Security Gateway

In Unternehmen sind oft IT-Infrastrukturen vorhanden, die über Jahre »gewachsen« und entsprechend heterogen sind. Sollen in diese Strukturen neue Internetdienste integriert werden, wobei zugleich der Schutz der Unternehmenswerte gewährleistet bleiben soll, wirft dies erhebliche Probleme auf. Der Einsatz einer Vielzahl von Sicherheitsprodukten an verschiedenen Stellen des Netzwerks ist aufgrund des Umsetzungsaufwands sowohl auf technischer als auch auf organisatori-

neuKap10.fm Seite 324 Freitag, 18. Oktober 2002 3:52 15

scher Ebene als sehr bedenklich einzustufen. Eine große Anzahl von IT-Projekten scheitert nach wie vor an der organisatorischen Umsetzung.

Der Ansatz des zentralen Security Gateway bringt diesbezüglich entscheidende Vorteile. Gateways erlauben die konsequente Trennung von Netzen und die Überwachung der Verbindung. Zudem ermöglichen sie die Integration von Services wie beispielsweise Authentisierung und Verschlüsselung, ohne dass in den bestehenden Infrastrukturen tiefgreifende Änderungen vorgenommen werden müssen.

Im Folgenden werden drei auf diesem Konzept basierende Sicherheitslösungen vorgestellt:

- Mit dem **Authentication Gateway** steht eine zentrale Authentisierungs- und Identifikations-Komponente für vertrauliche Kommunikation (z. B. »secure remote access« via Mobiltelefon, PDA oder Browser) zur Verfügung.
- Das **Secure E-Mail Gateway** dient als »virtuelle Poststelle« für vertrauenswürdige E-Mails.
- Der **Signature Server** ist die zentrale Signatur-Komponente für sichere digitale Signaturen auch bei der Verarbeitung großer Datenmengen.

10.11.1 Das Authentication Gateway

Im Internet werden zunehmend Informationen bereitgestellt, die eindeutig einem Nutzer zugeordnet sind. Beispiele hierfür sind das persönliche Aktiendepot im Broker-Portal, das Bankkonto im Homebanking-Bereich, Dokumente auf den Servern des eigenen Unternehmens, der Internet Account, persönliche Versicherungsdaten und vieles mehr.

Im Alltag des E-Business steht ein Unternehmen nicht einer geschlossenen Benutzergruppe gegenüber, sondern vielen Gruppen mit unterschiedlichen Bedürfnissen, Zugriffsumgebungen und Zugriffsrechten: Mitarbeiter, Kunden, Lieferanten, Partner usw. Diese Benutzergruppen können in der Regel auf einen oder mehrere spezifische Internetdienste zugreifen.

neuKap10.fm Seite 325 Freitag, 18. Oktober 2002 3:52 15

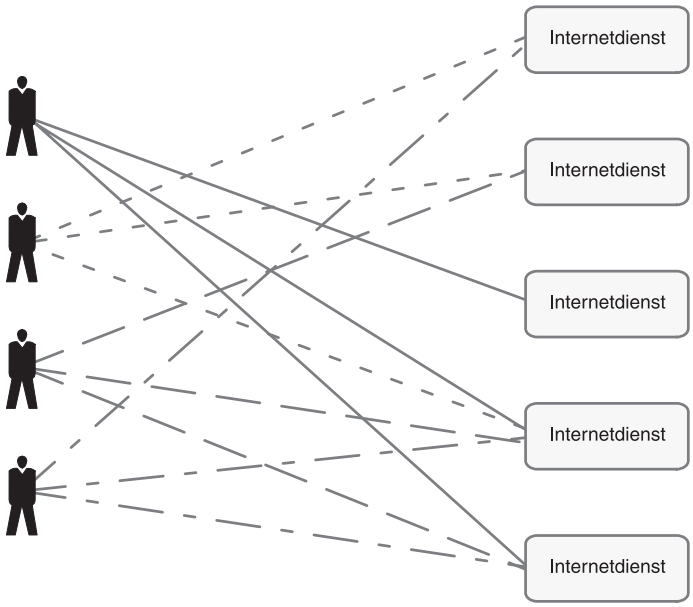


Abb. 10.18: Zugriffsmatrix

Die Personalisierung von Daten und Diensten für verschiedene Gruppen und der Zugriff über das Internet (World Wide Web) setzen Authentisierungsvorgänge bereits beim Zugriff auf das Webportal und nicht erst auf Präsentations- oder Applikationsebene voraus. So erhält der Nutzer auf kürzestem Weg den Zugriff auf die seiner Rolle und Zugriffsumgebung entsprechenden Daten oder Applikationen.

Der sichere Zugriff auf Daten soll dabei unabhängig vom Ort und von den Randbedingungen möglich sein, ohne dass besondere Anforderungen an die Zugangsrechner gestellt werden. Außerdem müssen die Verfahren zur Authentisierung besonders stark sein, damit die Internet-Dienste nicht von Unbefugten auf Kosten der rechtmäßigen Nutzer und/oder Unternehmen missbraucht werden können. In der Regel arbeiten Anwendungen, die auf diese Art über das Internet angeboten werden, mit einer Passwort-Authentisierung, die keine angemessene Sicherheit bietet.

neuKap10.fm Seite 326 Freitag, 18. Oktober 2002 3:52 15

Grundsätzliches Konzept des Authentication Gateway

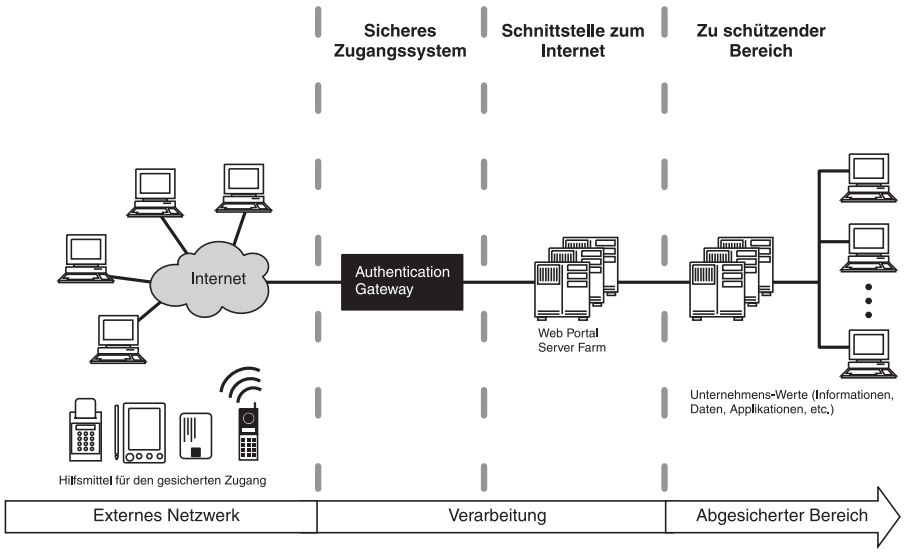


Abb. 10.19: Authentication Gateway

Das Authentication Gateway bündelt die notwendigen Sicherheitsmechanismen an zentraler Stelle und ermöglicht die Nutzung vorhandener Strukturen und Verfahren. Für Unternehmen, die mehrere Nutzergruppen mit unterschiedlichen Authentisierungsverfahren und Token ausstatten wollen, bietet es elegante Möglichkeiten, verschiedenste Verfahren bzw. Token parallel zu nutzen. Zum Beispiel kann ein Teil der Mitarbeiter oder Kunden das bereits vorhandene Verfahren weiter verwenden, ein anderer Kreis hingegen nutzt Alternativen wie das Mobiltelefon, PDAs oder Software-basierte Verfahren.

Von seinem Konzept her kann das Authentication Gateway an die technischen Randbedingungen und Anforderungen der jeweiligen Anwendungen angepasst werden, ohne eine bestimmte Struktur zwingend vorauszusetzen. Bezüglich der Plattformen, auf denen die angebotenen Internetdienste basieren (z. B. WebSphere, BEA, Apache etc.), ist es flexibel. Auch zukünftige Anforderungen sind einfach umzusetzen.

Das Authentication Gateway bietet die Dienste Authentisierung, Autorisierung und Administration (»3A«) an zentraler Stelle an. Es kann die entsprechenden (Basis-)Autorisierungen für die angebotenen Internetdienste durchführen und somit eine Entkoppelung der Dienste von der Client-Seite realisieren.

neuKap10.fm Seite 327 Freitag, 18. Oktober 2002 3:52 15

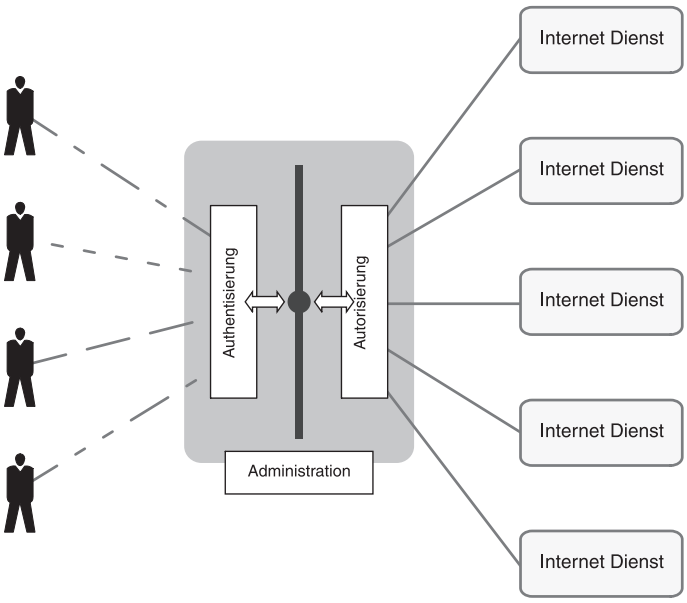


Abb. 10.20: Die virtuelle Schnittstelle

Das Konzept der Trennung von Authentisierung und Autorisierung bietet optimale Voraussetzungen für die Einführung neuer Verfahren und Systeme wie PKI-basierter Lösungen (mit SmartCards oder Software-Token). Durch die Möglichkeit der schrittweisen Integration und Freischaltung von Anwendergruppen räumt das Authentication Gateway einen Hauptgrund für die zögernde Haltung vieler Unternehmen zur Einführung von Public Key Infrastrukturen aus.

Integration von Authentication Gateways

Das Authentication Gateway wird an zentraler Stelle in die bestehende IT-Infrastruktur integriert und stellt folgende Funktionalitäten und Dienste bereit:

- Trennung der Netzwerke und Übernahme der Verbindungsanfrage
- verschlüsselte Kommunikation zwischen Client und Authentication Gateway
- Analyse der Verbindungsanfragen mit dem Ziel der Überprüfung, ob für diese Verbindungsanfrage eine Identifizierung notwendig ist
- Identifikation und Authentisierung des Anfragenden mit dem gewählten oder voreingestellten Verfahren
- Autorisierung in Abhängigkeit von der Plattform des Internetdienstes
- Administration

Systemübersicht

Das Authentication Gateway stellt eine gesicherte Plattform für die Integration unterschiedlicher Authentisierungs- und Autorisierungsdienste an einer zentralen

neuKap10.fm Seite 328 Freitag, 18. Oktober 2002 3:52 15

Stelle bereit. Die nachfolgende Systemübersicht zeigt die einzelnen Komponenten eines Authentication Gateway.

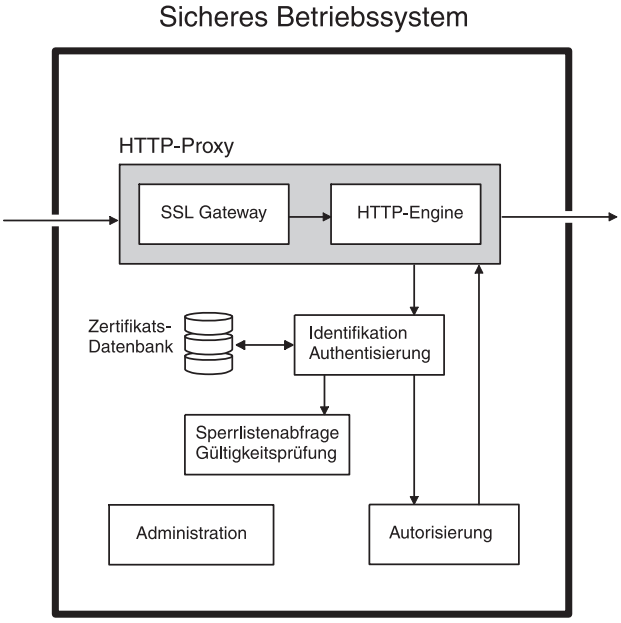


Abb. 10.21: Systemübersicht des Authentication Gateway

Zwei Kommunikationsschnittstellen regeln die Annahme der Verbindung und die Anmeldung an die dahinter geschalteten DV-Systeme. Weitere Schnittstellen sind entsprechend den zum Einsatz kommenden Authentisierungsmethoden zu ergänzen (z. B. Schnittstelle zu Verzeichnisdiensten, zu externen Kommunikationskanälen, für die Administration etc.).

HTTP-Proxy

Über das SSL-Gateway im HTTP-Proxy wird im ersten Schritt eine verschlüsselte Verbindung zwischen der anfragenden Anwendung (Client) und dem Authentication Gateway aufgebaut. Dadurch werden alle ausgetauschten Informationen zwischen Client (Browser) und Authentication Gateway verschlüsselt.

Der HTTP-Proxy überprüft die Verbindungsanfrage des Anwenders entsprechend dem eingestellen Regelwerk (z. B. nach IP-Adresse etc.) und leitet sie entweder zu den dahinter liegenden DV-Systemen weiter oder leitet die Identifikation und Authentisierung ein.

Identifikation und Authentisierung

Im ersten Schritt wird die Authentisierung des Anfragenden mit einem entsprechenden Verfahren durchgeführt. Im einfachsten Fall wird der Name des Benutzers und sein Passwort über einen verschlüsselten SSL-Kanal abgefragt. Die

neuKap10.fm Seite 329 Freitag, 18. Oktober 2002 3:52 15

Auswahl der Methode erfolgt in Abhängigkeit vom jeweiligen Anwender oder der Zugriffsumgebung. Die Bereitstellung aller relevanten Kommunikationsschnittstellen bildet die Grundlage für die Anwendung verschiedener Authentisierungsverfahren (Kommunikation mit SmartCard-Leser auf Client-Seite, Anfrage an Verzeichnisdienste zwecks Zertifikatsauskunft, Anfrage an RADIUS-Server zwecks Access-Listenabfrage etc.).

Beispielsweise können die folgenden gängigen Authentisierungsmethoden unterstützt werden:

- Username/Password (verschlüsselt)
- Hardware-Token (SecureID, DigiPass, OneTimePass o.ä.)
- Mobiltelefon (MAS)
- Software-Token (Zertifikats- oder PKI-orientiert)
- SmartCard/SmartCard-Reader (Zertifikats- oder PKI-orientiert)

Autorisierung

Um einem bestimmten Nutzer die entsprechende Rolle zuzuweisen, bereitet diese Systemkomponente korrespondierend zur angegebenen Identität und den angeschlossenen DV-Systemen (WebSphere, BEA, Apache, ...) die Daten zur Anmeldung auf und führt diese im entsprechenden plattformspezifischen Verfahren aus.

Administration

Mithilfe der Administration werden das Zugriffsmanagement, das Sperrlistenmanagement, die Protokollierungstiefe, das Alarmierungsverfahren usw. verwaltet. Außerdem können die Protokollierungsinformationen abgerufen werden.

Vorteile eines zentralen Authentication Gateways

Ein wesentlicher Vorteil eines Authentication Gateway liegt darin, dass er den wesentlichen Anforderungen aller Beteiligten gerecht werden kann:

- den Anwendern, die über das Authentication Gateway auf die für sie bereitgestellten Informationen zugreifen,
- den IT-System-Verantwortlichen, die das Authentication Gateway einsetzen und betreiben,
- den Security-Verantwortlichen der Organisation, die damit eine angemessene Sicherheit realisieren können,
- der Geschäftsleitung, die unter Berücksichtigung der kurz-, mittel- und langfristigen wirtschaftlichen Ziele und Strategien über den Einsatz bestimmter Technologien entscheidet.

Vorteile aus Sicht der Anwender

Der Anwender, der über das Authentication Gateway auf die speziell für ihn bereitgestellten Informationen, Applikationen oder Daten zugreift, möchte dies in der

neuKap10.fm Seite 330 Freitag, 18. Oktober 2002 3:52 15

Regel mit möglichst wenig Aufwand tun und erwartet die Verlässlichkeit und Vertrauenswürdigkeit der Operation.

Durch den zentralen Gateway-Ansatz erhält der Anwender die Option, aus einer breiten Palette von Hilfsmitteln für die Authentisierung zu wählen. Das Gateway bietet die Möglichkeit, alternativ oder parallel neue Verfahren und Methoden zu wählen. Grundsätzlich können sich Organisationen für die Weiterbenutzung einer bewährten Authentisierungsmethode (z. B. per SmartCard oder Software) entscheiden. Nicht nur die reinen Anschaffungskosten spielen bei der Entscheidung für oder gegen bestimmte Authentisierungsmethoden eine Rolle: Wird ein Token gewählt, das den Anwendern bereits bekannt ist, reduziert dies den organisatorischen Aufwand und sorgt für eine höhere Akzeptanz des Verfahrens.

Der zentrale Ansatz vereinfacht den Umgang mit Passworten und Zugangscodes. Eine einmalige Authentisierung erlaubt den Zugriff auf alle relevanten Server, Datenbanken und Applikationen gemäß der Rolle des Anwenders.

Vorteile aus Sicht der IT-Systemverantwortlichen

Mit der zentralen Authentisierung am Gateway wird ein »Common Point of Trust« realisiert. Dadurch verringert sich der Aufwand und letztlich auch die Kosten für Administration, Wartung und Pflege von Zugriffsregeln und Benutzerverwaltungen.

Durch die dem zentralen Authentication Gateway zugrunde liegende Firewall-Technologie verringert sich auch die Angriffsfläche der dahinter liegenden Web-Portale (Internetdienste). Die Angriffsfläche der zentralen Stelle wird reduziert und eine erweiterte Verbindungskontrolle wird ermöglicht.

Die Möglichkeiten zum Ausbau und zur Erweiterung der bestehenden Authentisierungsmethoden bieten ebenfalls Vorteile für die IT-Systemverantwortlichen: Bestehende Benutzerverwaltungen können problemlos integriert werden, da Standard-Schnittstellen bereitstehen (Radius Connectivity, LDAP Support etc.). Auch proprietäre Schnittstellen zu Informationssystemen wie Datenbanken oder Transaktionssystemen können an zentraler Stelle einfach integriert werden und bestehende oder noch in Planung befindliche PKIs können eingebunden werden.

Vorteile aus Sicht der Sicherheitsverantwortlichen

Die bestehende Sicherheitspolitik und die daran gebundenen Gruppen- oder Rollen-Konzepte müssen nur an einer zentralen Stelle abgebildet und auditiert werden. Eine Anpassung der Policy ist nicht erforderlich.

Die logische Trennung der Authentisierung und der (Basis-)Autorisierung lässt einen großen Spielraum für die Verwendung unterschiedlicher Authentisierungsverfahren. Abstufungen der Zugriffsrechte für die Anwender lassen sich auf diese Weise leicht realisieren.

neuKap10.fm Seite 331 Freitag, 18. Oktober 2002 3:52 15

Die problemlose Integration von PKI-Konzepten ist für die IT-Sicherheitsverantwortlichen von besonderer Bedeutung.

Vorteile aus Sicht der Entscheidungsträger in der Geschäftsleitung

Hier stehen weniger die technischen Features im Mittelpunkt als Investitionssicherheit und Ausbaufähigkeit. Durch seine hohe Flexibilität und die Erweiterungsmöglichkeiten bietet das Authentication Gateway Zukunftssicherheit. Versteckte Kostenstrukturen im Sinne der TCO können dadurch vermieden werden.

Darüber hinaus stellt das Authentication Gateway als ein zentrales System, das in die allgemeinen Unternehmensprozesse integriert werden kann, einen wesentlichen Schritt zur konsequenten Umsetzung der unternehmensweiten Security Policy dar.

10.11.2 Secure E-Mail Gateway

Der Austausch von E-Mails ist die meistgenutzte Anwendung im Internet. Der Informationsaustausch mittels elektronischer Briefe spiegelt jedoch nicht die unternehmensspezifischen Arbeitsabläufe wider. So können und müssen Prozesse, die unter Umständen weitreichende Konsequenzen haben, im Sinne einer Weisung durch einen zuständigen Sachbearbeiter in Form von verschlüsselten und/oder signierten E-Mails erfolgen. Die Abbildung dieser Vorgänge durch entsprechende Verfahren stellt eine Herausforderung an die beteiligten Systeme dar.

Beispiele für Organisationsabläufe, die in der IT-Struktur abgebildet werden sollten, sind Vertreter-Regelungen, die verteilte Bearbeitung innerhalb einer Gruppe, die Ausstellung von Empfangsquittungen u. Ä. oder die Archivierung des Schriftverkehrs. Bisher verfügbare Mail-Systeme beschränken sich auf den bloßen Transport von E-Mail, ohne die Abbildung der Arbeitsabläufe zu ermöglichen. Insbesondere der Workflow bei kryptographischen Operationen wird durch die Bindung an einzelne Personen bzw. Arbeitsplätze erschwert.

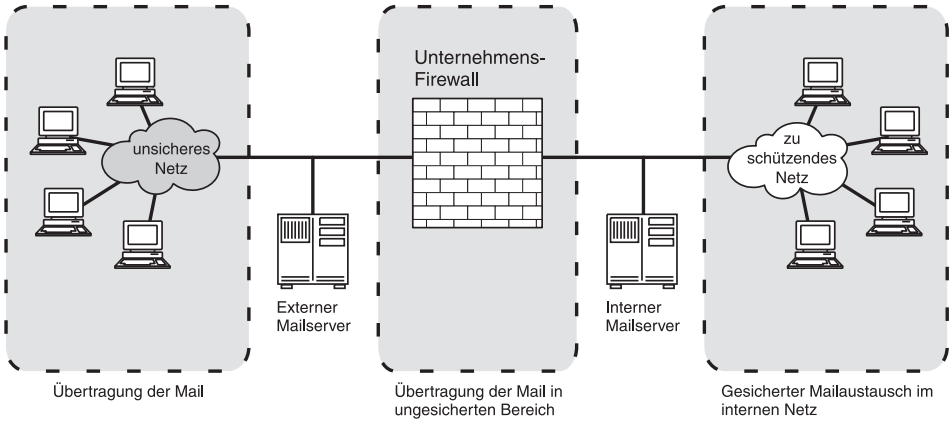


Abb. 10.22: Übersicht: Standard Mail Server System

neuKap10.fm Seite 332 Freitag, 18. Oktober 2002 3:52 15

An dieser Stelle setzt das Konzept des Secure E-Mail Gateway an. Die Aufstellung an zentraler Stelle im E-Mail-Verkehr erlaubt die Anwendung einer zentralen Unternehmens-Policy hinsichtlich der Verteilung der E-Mails sowie auch der Anwendung von kryptographischen Operationen. Unterstützt wir dies durch die Möglichkeit, kryptographische Schlüssel innerhalb des Secure E-Mail Gateways gesichert speichern zu können. Hierzu steht z. B. ein Hardware-Sicherheitsmodul (HSM) zur Verfügung.

Systemübersicht

Dem Gateway-Ansatz folgend, befindet sich das Secure E-Mail Gateway an zentraler Stelle im Netzwerk (»Common Point of Trust«). Es entschlüsselt und verifiziert eingehende E-Mails und ist in der Lage, ausgehenden Mail-Verkehr zu verschlüsseln und zu signieren. Durch seine Funktion als »zentrale Poststelle« bietet es Vertraulichkeit (Verschlüsselung), Integrität und Verbindlichkeit (Signatur) für den gesamten Mail-Verkehr. Auf der Gegenseite kann ein Secure E-Mail Gateway oder eine Client-Software die entsprechenden Sicherheitsfunktionen realisieren.

Funktionsweise

Das Secure E-Mail Gateway stellt eine Erweiterung der genutzten E-Mail Server dar. Definierte Benutzergruppen oder auch Einzelanwender können damit ihre E-Mail automatisch vor dem Versand signieren und/oder verschlüsseln lassen.

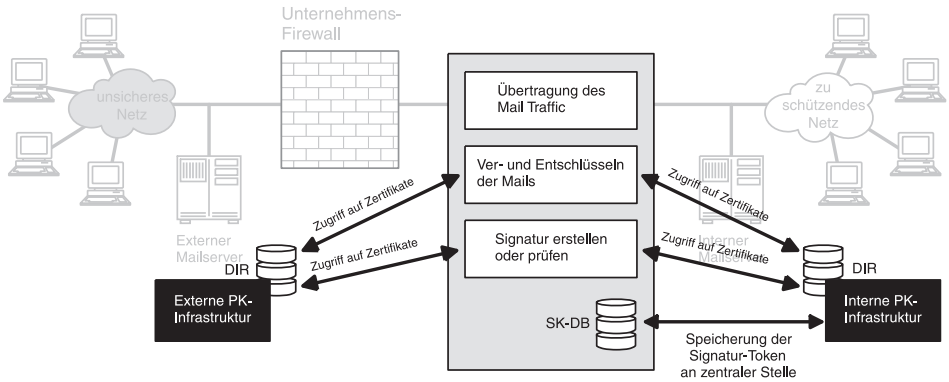


Abb. 10.23: Allgemeine Funktionsweise

Das Speichern der Übermittlungsbestätigung erlaubt den Nachweis der Kommunikation, wodurch eine weitere Anforderung des Signaturgesetzes erfüllt wird.

Ein Mitarbeiter des Unternehmens, der verschlüsselte Mails erhält, sieht diese aufgrund der automatisch ablaufenden Entschlüsselung im Klartext auf dem Bildschirm. Für den Anwender sind diese Vorgänge transparent, er selbst muss sie nicht aktiv ausführen. An die Client-Software (Mailprogramm) werden keine zusätzlichen Anforderungen gestellt.

neuKap10.fm Seite 333 Freitag, 18. Oktober 2002 3:52 15

Beim Versand von Mails kann für den Fall, dass bereits ein Zertifikat des Empfängers im Secure E-Mail Gateway vorliegt, die Mail automatisch verschlüsselt und verschickt werden. Falls das Zertifikat nicht vorliegt, kann das Secure E-Mail Gateway die notwendigen Zertifikate von externen oder internen Verzeichnis-Servern abrufen. Die Speicherung der empfangenen Zertifikate an zentraler Stelle ermöglicht Verschlüsselung auch dann, wenn ein Versender einer E-Mail bis zu diesem Zeitpunkt noch keine direkte Kommunikation mit dem Empfänger aufgenommen hat.

Die Verifikation der Zertifikate erfolgt an zentraler Stelle, ebenfalls die Festlegung der Regeln, nach denen das Secure E-Mail Gateway die ein- bzw. ausgehenden Mails für einzelne Empfänger oder Gruppen behandelt.

Neben den Standards wie S/MIME, ISIS-MTT oder PGP könnte ein Secure E-Mail Gateway auch nur die Anhänge von E-Mails mit einem symmetrischen Verschlüsselungsverfahren verschlüsseln, das eine selbstextrahierende verschlüsselte Datei produziert. Auf der Empfängerseite könnte dann eine einfache Software zur Verfügung gestellt werden, die in der Lage ist, diese Datei wieder zu entschlüsseln. Damit kann eine einfache Verschlüsselung von E-Mail-Anhängen realisiert werden, die auch dann funktioniert, wenn die auf der Empfängerseite genutzte Mail-Software Standards wie S/MIME, ISIS-MTT oder PGP nicht unterstützt.

Zeitstempeldienste

Digitale Signaturen sind durch die Einbindung von Zeitstempeldiensten erweiterbar. Die Zeitstempel-Funktionalität bedeutet jedoch mehr als nur einen elektronischen Post-Eingangsstempel: Ein Zeitstempel ist der eindeutige Beleg darüber, wann ein Dokument in einer bestimmten Form vorgelegen hat. Sobald an dem digital »zeitgestempelten« Dokument Veränderungen vorgenommen werden, ist dies nachprüfbar.

Zeitstempeldienste erlauben den Nachweis der Authentizität und Integrität von Daten zu einem bestimmten Zeitpunkt. Ereignisse wie z. B. der Eingang von Bestellungen, Online-Auktionsgeboten oder Online-Brokerage-Aktivitäten werden mittels des Zeitstempelsystems mit einer offiziellen Zeitangabe versehen. Vom Einsatz derartiger Funktionalitäten können neben der E-Mail-Korrespondenz auch Workflow- und Archivierungssysteme profitieren.

Vorteile der »zentralen Poststelle«

PKI-Lösungen als sehr zeit- und kostenaufwendige Infrastrukturen erfordern einen hohen Aufwand für Installation und Inbetriebnahme. Durch den zentralen Ansatz des Secure E-Mail Gateway sind PKI-Funktionalitäten schneller und einfacher einsetzbar.

neuKap10.fm Seite 334 Freitag, 18. Oktober 2002 3:52 15

Die Sicherstellung der Unveränderbarkeit von Daten erfolgt bisher nur über sehr aufwändige Archivierungsverfahren (CD-ROM- bzw. Bandlösungen etc.), die zudem keine vollständige Sicherheit bieten. Beim Secure E-Mail Gateway kann die Sicherung der Daten im Hintergrund mithilfe von Zeitsignaturen automatisch ablaufen.

Entscheidende Vorteile sind die deutlich reduzierte Komplexität durch die Realisierung an zentraler Stelle und die hohe Benutzerfreundlichkeit, weil keine zusätzliche Software auf der Anwenderseite bedient und geschult werden muss. Umständliche dezentrale Rollout-Planungen und hoher Wartungsaufwand entfallen. Gleichzeitig ist die »Key Recovery«-Problematik gelöst.

Im Unternehmen wird die Anzahl der benötigten Zertifikate deutlich reduziert und die Abbildung und Einhaltung der Security Policy konsequent umgesetzt. Sicherheit ist nicht länger Entscheidung des Anwenders. Die erhöhte Interoperabilität mit externen Systemen bringt dem Unternehmen entscheidende Impulse, eine wichtige Hemmschwelle entfällt.

10.11.3 Signature Server

Eine neue Aufgabenstellung im Zuge der Umsetzung von vertrauenswürdigen elektronischen Geschäftsprozessen ist die Verarbeitung von Massendaten. So ist z. B. die Einreichung von elektronischen Umsatzsteuer-Erklärungen an die Finanzbehörden, insbesondere bei großen Unternehmen, eine sinnvolle und Kosten sparende Anwendung.

In Großunternehmen ist die Menge der verarbeiteten Daten oftmals so groß, dass die elektronische Signatur nicht einfach umsetzbar ist. Der Signature Server stellt in Bereichen, in denen große Datenmengen signiert und verifiziert werden müssen, durch die Bereitstellung elektronischer Signaturen eine günstige Lösung dar.

Die bisherige Rechnungserstellung, geprägt durch den Mix von elektronischer Datenverarbeitung und dem üblichen Ausdruck und Postversand kostet unter Berücksichtigung der wiederholten Aufbereitung der Daten, Papierverbrauch, Kuvertierung, Portokosten und Unterhalt des Lettershops etwa 1,40 EUR pro Rechnung. Erfolgt die Rechnungsstellung ausschließlich elektronisch, sinken durch den Wegfall des Medienbruchs, der Portokosten etc. die Kosten auf 40 Cent /Goeb2002/.

Systemübersicht

Zu den Vorteilen eines zentralen Signature Servers gehören die auf eine zentrale Stelle konzentrierte Erstellung digitaler Signaturen, die einfache Integration in eine bestehende Infrastruktur und die zentrale Administrationsmöglichkeit.

neuKap10.fm Seite 335 Freitag, 18. Oktober 2002 3:52 15

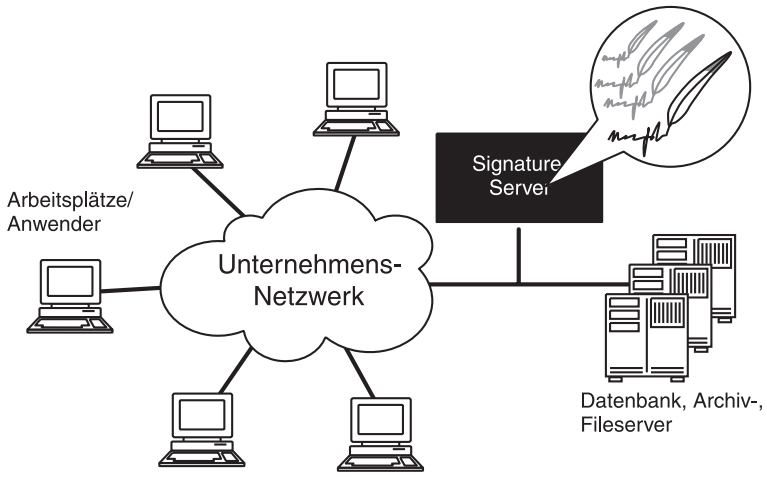


Abb. 10.24: Systemübersicht

Beispiel: Signature Server in einer ERP-Systemumgebung:

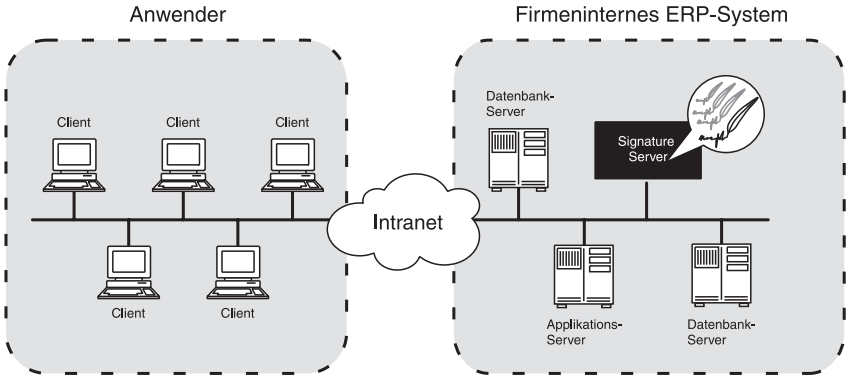


Abb. 10.25: Signature Server für ERP-Systemumgebungen

Innerhalb eines bestehenden firmeninternen ERP-Systems wird ein zentraler Signature Server integriert, der aus folgenden Komponenten besteht:

- **Kommunikationseinheit:**
  Integration der Signaturkomponente in das ERP-Netzwerk, dabei werden die Schnittstellen zum ERP-System unterstützt.
- **Signatur-Komponente:**
  Hardware-Sicherheitsmodul zur Speicherung und Anwendung der Signaturen oder vieler SmartCards parallel.
- **PKI-Schnittstelle:**
  Schnittstelle zur externen oder firmeninternen Public-Key-Infrastruktur (PKI).
- Gesicherte **Administrations-Schnittstelle**

neuKap10.fm Seite 336 Freitag, 18. Oktober 2002 3:52 15

Damit stellt der zentrale Signatur-Server folgende Dienste und Funktionen bereit:

- eine gesicherte Umgebung zur Speicherung der Signaturen
- eine gesicherte Umgebung zur Erstellung und Verifikation von Signaturen für Dokumente und Transaktionen
- einen gesicherten Zugriff auf die Signaturen durch die Anwender
  Erlaubt die Firmen-Sicherheitspolitik dies, können firmenweite Schlüssel durch die Applikations-Systeme zur Signaturerstellung herangezogen werden.

Bei der Konzeption eines Signature Server müssen verschiedene Fragestellungen berücksichtigt werden:

- Wird die Schlüsselerzeugung und Signaturzuordnung in einem Hardware-Sicherheitsmodul (HSM) vorgenommen, muss die Zertifikatseinbringung organisatorisch gelöst werden (im Gegensatz zur fertig personalisierten Chipkarte).
- Der Public Key des Unternehmens muss bei qualifizierten Signaturen durch ein signaturgesetzkonformes Trustcenter signiert sein.
- Es muss gewährleistet sein, dass die Signatur-Anwender an einer zentralen Stelle registriert sind. (Die Zuordnung von Anwendern zu Signaturschlüsseln erfolgt im Hardware-Sicherheitsmodul.)
- Die Anwender müssen für die Signaturanwendung am Signatur-Server freigeschaltet werden.
- Eine Regelung für die Sicherung der Verbindung zwischen Arbeitsplatz, ERP-System und Signatureinheit ist erforderlich. Diese kann jedoch problemlos realisiert werden.

Vorteile des Einsatzes eines Signature Server

Der Vorteil eines Signature Server liegt im Wesentlichen in der Performance. Mit einem Signatur-Server können große Datenmengen sehr schnell bearbeitet werden. Die Verwendung von SmartCards ist nicht nur langsamer, sondern auch aufgrund der Handhabung für große Datenmengen nicht geeignet. Außerdem zeichnet sich ein Signature Server durch eine hohe Migrationsfähigkeit aus. Eine Anpassung an erhöhte Performance-Anforderungen kann durch bereits implementierte Lastverteilungsverfahren durchgeführt werden.

Zentrale Signature Server sind einfach in bestehende Systeme zu integrieren. Bei der Nutzung eines Hardware-Sicherheitsmoduls erlauben sie die Anwendung unterschiedlicher kryptographischer Verfahren und großer Schlüssellängen. Sollten aktuelle Schlüsselstärken oder Algorithmen mit der Zeit als zu schwach angesehen werden, so können sie problemlos durch neue Verfahren oder höhere Schlüssellängen ersetzt werden. So ergibt sich eine hohe Investitionssicherheit.

neuKap10.fm Seite 337 Freitag, 18. Oktober 2002 3:52 15

Hardware-Sicherheitsmodule sind bereits seit Jahren bewährt und stellen den aktuellen Stand der Technik im Bereich für Hochsicherheits-Anwendungen und -Technologien dar. Die flexible Programmierbarkeit erlaubt die Realisierung verschiedenster Sicherheitsvorgaben. Jede organisatorische Anforderung (Vieraugenprinzip, Schlüsselgenerierung usw.) kann abgebildet werden. Darüber hinaus bietet ein Hardware-Sicherheitsmodul Platz für Zusatzanwendungen wie z. B. die Integration von Zeitstempel-Funktionalitäten oder Zahlungsverkehrs-Protokollen für eine transaktions-basierte Sicherheit. Die Signatur-Anwendung und der Signaturschlüssel (beides gesichert im Hardware-Sicherheitsmodul) sind nicht im Besitz einer Person, wodurch der Missbrauch von Signaturen deutlich erschwert wird.

Beim Einsatz eines Signature Server sind – anders als bei Verwendung von Smart-Cards – gesicherte Backup-Mechanismen nach Bedarf realisierbar.

10.11.4 Zusammenfassung

Security Gateways als Plattform zur Absicherung von Unternehmenswerten versetzen Organisationen in die Lage, flexibel und schnell bedarfsgerechte Sicherheit zu erzielen, ohne ein hohes Investment in die benötigte Infrastruktur zu tätigen. Sie bieten als modulare Plattform eine hohe Flexibilität, sind passgenau und zukunftssicher, da das Sicherheitssystem mit den Anforderungen wächst. Da die Schaffung und Umsetzung herstellerübergreifender Spezifikationen erfahrungsgemäß lange dauern kann und nicht immer erfolgreich ist, ist die einfache Integration unterschiedlicher Standards ebenfalls ein wichtiger Vorteil von Security Gateways. Daraus resultiert ein günstiges Kosten-Nutzen-Verhältnis, das zu einer Akzeptanz auf breiter Basis beitragen kann.

neuKap10.fm Seite 338 Freitag, 18. Oktober 2002 3:52 15

neuKap11.fm Seite 339 Freitag, 18. Oktober 2002 3:52 15

Ein Firewall-System ist mehr als ein Produkt

Ein Firewall-System ist kein Produkt, das nach dem Kauf automatisch Sicherheit gewährleistet. Unterschiedliche Aspekte müssen berücksichtigt werden, damit mithilfe eines Firewall-Systems das gewünschte Sicherheitsmaß erreicht werden kann. Das Firewall-System muss

- auf einer Firewall-Sicherheitspolitik aufbauen,
- im IT-Sicherheitskonzept der Organisation eingebettet sein,
- korrekt installiert und
- korrekt administriert werden.

In diesem Kapitel wird exemplarisch beschrieben, wie eine Firewall-Sicherheitspolitik auszusehen hat und welche Sicherheitsmaßnahmen für den Betrieb eines Firewall-Systems zusätzlich benötigt werden. Jedoch können Sicherheitsmaßnahmen für eine korrekte Installation oder Administration nicht berücksichtigt werden, weil sie vom jeweils eingesetzten Produkt abhängen. Auch die Einbettung der Firewall-Sicherheitspolitik in ein IT-Sicherheitskonzept wird nicht dargestellt, da sie organisationsspezifisch ist /BSI99/.

11.1 Firewall-Sicherheitspolitik

Eine Firewall-Sicherheitspolitik ist die Voraussetzung für den sicheren Betrieb eines Firewall-Systems. Ein Firewall-System macht nicht automatisch sicher, sondern mit einem Firewall-System kann der Übergang zwischen einem unsicheren und einem zu schützenden Netz sicher gemacht werden. Die Installation eines Firewall-Systems ohne vorausgehendes Sicherheitskonzept kann zu einem falschen Sicherheitsgefühl führen. Oft wird irrtümlicherweise davon ausgegangen, dass mit der Installation eines Firewall-Systems alles gesichert sei. Dieser Irrtum wiegt noch schwerer, wenn keine genaue Kenntnis über die vorhandene Netzwerktopologie vorhanden ist. Denn bei Unkenntnis der Netzwerktopologie kann man nicht davon ausgehen, dass nicht doch mehr als eine Verbindung zum Internet oder zu anderen unsicheren Netzen existiert.

Die Firewall-Sicherheitspolitik orientiert sich am Schutzbedarf der eingesetzten IT-Systeme und muss Teil einer vorhandenen organisationsweiten Sicherheitspolitik sein. Die Festlegung der Firewall-Sicherheitspolitik kann bestehende Richt-

neuKap11.fm Seite 340 Freitag, 18. Oktober 2002 3:52 15

linien und Vorschriften der allgemeinen Sicherheitspolitik mitbetreffen, die dementsprechend mitberücksichtigt werden müssen.

Die Firewall-Sicherheitspolitik definiert Sicherheitsziele, die durch den Einsatz eines Firewall-Systems erfüllt werden sollen, und stellt die zu schützenden Ressourcen dar. Die Kommunikationsanforderungen und die erlaubten Dienste für die Übertragung werden darin festgelegt. Die Firewall-Sicherheitspolitik ist wie eine organisationsweite Sicherheitspolitik auf die jeweilige Organisation und den Bereich abgestimmt, z. B. Medizin, Banken, Versicherungen, Energieversorger, Betriebs- u. Personalrat usw. /Pohl97a und Pohl97b/.

11.1.1 Sicherheitsziele

Im ersten Schritt müssen die Sicherheitsziele, die mit dem Einsatz eines Firewall-Systems erreicht werden sollen, definiert werden. Als Richtwerte können folgende Punkte betrachtet werden.

- *Zugangskontrolle auf der Netzwerkebene:* Nur Verbindungen mit definierten (Teil-) Netzen oder einzelnen Rechnersystemen kommen zustande. Zugriffe und somit auch Angriffe von nicht zugelassenen (Teil-)Netzen bzw. Rechnersystemen sind nicht möglich.
- *Zugangskontrolle auf Benutzerebene:* Auf Benutzerebene werden alle Benutzer, die über das Firewall-System kommunizieren wollen, identifiziert und authentisiert.
- *Rechteverwaltung:* In der Rechteverwaltung wird festgelegt, welche Dienste und Protokolle ein Benutzer zu welchen Zeiten nutzen darf.
- *Kontrolle auf der Anwendungsebene:* Auf der Anwendungsebene werden dem Benutzer für bestimmte Dienste, wie z. B. FTP oder HTTP, nur die Befehle zur Verfügung gestellt, die für seine Aufgabenstellung notwendig sind.
- *Entkopplung von Diensten:* Besonders risikobelastete Dienste (z. B. »sendmail«) werden dem unsicheren Netz nur über eigene Hilfsprogramme mit eingeschränkter Funktionalität zur Verfügung gestellt.
- *Beweissicherung und Protokollauswertung:* Verbindungsdaten und sicherheitsrelevante Ereignisse werden protokolliert und können für die Erkennung von Sicherheitsverletzungen und die Beweissicherung der Handlungen von Benutzern ausgewertet werden.
- *Alarmierung:* Besonders sicherheitsrelevante Ereignisse, die zur Beeinträchtigung der Sicherheit führen könnten, werden an ein Security Management gemeldet. Dort kann schnell reagiert werden, und geeignete Maßnahmen können eingeleitet werden.
- *Verbergen der internen Netzstruktur:* Ziel ist es, die Struktur des zu schützenden Netzes gegenüber dem unsicheren Netz zu verbergen. Es darf aus dem unsicheren Netz nicht erkennbar sein, welche Anzahl von Rechnersystemen im zu schützenden Netz vorhanden ist (10, 100, 1 000 oder 10 000) und um welche Art von Rechnersystemen es sich handelt (PCs oder Großrechner).

neuKap11.fm Seite 341 Freitag, 18. Oktober 2002 3:52 15

- *Vertraulichkeit der Nachrichten:* Nachrichten, die über verteilte Firewall-Systeme mit einem Kommunikationspartner ausgetauscht werden, sollen nicht im Klartext gelesen werden können. Durch Verschlüsselung wird die Vertraulichkeit der Nachrichten gewährleistet. Weitere Angriffe, z. B. von Trittbrettfahrern, können unterbunden werden.
- Weitere Ziele eines Firewall-Systems:
  - Das Firewall-System selbst muss gegen Angriffe resistent sein
  - Accounting (IP- und benutzerorientiert)
  - Network Adress Translation

11.1.2 Darstellung der zu schützenden Ressourcen

Die Darstellung der zu schützenden Ressourcen in der Firewall-Sicherheitspolitik dient dazu, alle schutzbedürftigen Rechnersysteme und Daten zu erfassen und in den weiteren Betrachtungen zu berücksichtigen. Schützenswerte Ressourcen sind beispielsweise:

- Rechnersysteme
- Kommunikationseinrichtungen
- Daten
- Drucker

11.1.3 Festlegung von Kommunikationsanforderungen

Die Kommunikationsanforderungen legen fest, auf welche Art die Kommunikation über das Firewall-System zwischen unsicherem und zu schützendem Netz erfolgen soll. Dabei sollten zunächst folgende Fragen beantwortet werden:

- Müssen Dateien übertragen werden? Wenn ja, in welche Richtung? Aus dem zu schützenden Netz in das unsichere Netz oder umgekehrt?
- Welche Informationen dürfen über das Firewall-System vom unsicheren in das zu schützende Netz und umgekehrt ausgetauscht werden?
- Welche Informationen soll das Firewall-System verdecken (z. B. die interne Netzstruktur und/oder die Benutzernamen des zu schützenden Netzes)?
- Welche Authentisierungsverfahren sollen innerhalb des zu schützenden Netzes bzw. für das Firewall-System benutzt werden (z. B. Einmal-Passworte oder Security Token)?
- Wie soll der Zugriff auf unsichere Netze erfolgen?
  - internes Netz → Firewall-System → Internet-Service-Provider → Internet
  - internes Netz → Firewall-System → Modem Server → Analog-/ISDN-Netz
- Wie erfolgen die Zugriffe auf das interne zu schützende Netz (z. B. Internet → Internet-Service-Provider → Firewall-System → internes Netz, oder Analog-/ISDN-Netz → Modem Server → Firewall-System → internes Netz)?

neuKap11.fm Seite 342 Freitag, 18. Oktober 2002 3:52 15

- Welcher Datendurchsatz ist zu erwarten (z. B. 64 kBit/s oder 2 MBit/s oder 34 MBit/s)?
- Wie sind die Verfügbarkeitsanforderungen (z. B. ständig [24 Stunden] oder zu bestimmten Zeiten [8–19 Uhr]; täglich [7 Tage] oder nur montags bis freitags)?

11.1.4 Festlegung von Diensten und Anwendungen

Aus den Kommunikationsanforderungen wird abgeleitet, welche Dienste oder Anwendungen durch das Firewall-System unterstützt werden sollen.

Dienste oder Anwendungen sind:

- SMTP (Simple Mail Transport Protocol) zum Versenden und Empfangen von E-Mail
- FTP (File Transfer Protocol) für den Dateitransfer zwischen Rechnersystemen
- HTTP (HyperText Transfer Protocol) zur Nutzung des World Wide Web (WWW)
- Telnet für den Zugriff auf entfernte Rechnersysteme mittels Terminalemulation
- NNTP (Network News Transport Protocol) zum Lesen und Posten von News in Newsgroups

Dienste sind z. B. auch Zugriffe auf Modems, über die vom Arbeitsplatz im zu schützenden Netz aus Fernwartungsarbeiten ausgeführt werden können oder externen Firmen der Wartungszugriff auf Systeme im internen Netz ermöglicht werden kann.

Mithilfe einer Dienste-Check-Liste wird z. B. definiert, in welche Richtung welche Dienste oder Anwendungen unterstützt werden sollen.

Dienst	OUT	IN
E-Mail	+	+
WWW	+	–
FTP	+	o
Telnet	+	o
News	+	+
Modem	+	o

Tabelle 11.1: Dienste-Check-Liste

Die jeweilige Kommunikationsrichtung wird durch die Definitionen OUT bzw. IN bestimmt:

OUT	Kommunikation vom zu schützenden Netz zum unsicheren gerichtet
IN	Kommunikation vom unsicheren Netz zum zu schützenden gerichtet
+	zugelassen
–	nicht zugelassen
o	nur mit Protokollierung und starker Authentikation zugelassen

neuKap11.fm Seite 343 Freitag, 18. Oktober 2002 3:52 15

Zusätzlich zu den erlaubten Diensten und Anwendungen kann die Sicherheitspolitik festlegen, zu welchen Zeiten ein Benutzer bestimmte Dienste oder eine bestimmte Anwendung nutzen darf. Bei der Definition solcher Filterregeln können die Arbeitszeiten berücksichtigt werden, damit ein unerlaubter Zugriff außerhalb der Arbeitszeiten ausgeschlossen werden kann.

Als Voreinstellung müssen alle Dienste und Anwendungen als nicht zugelassen festgelegt werden, die nicht benötigt werden.

Interne Benutzer

Nicht jedem Benutzer des internen zu schützenden Netzes sollen alle Dienste, die über das Firewall-System möglich sind, zur Verfügung gestellt werden, sondern nur die Dienste, die der Benutzer unbedingt für seine Aufgabenstellung benötigt. In Kommunikationsprofilen kann festgelegt werden, welche Dienste einem jeweiligen Benutzer zugewiesen werden. Dadurch wird der Aufwand, die Kommunikationsanforderungen einzelner Benutzer festzulegen, erheblich reduziert.

Dienst	Minimal	Standard	Service	Maximal
E-Mail	+	+	+	+
WWW	–	+	–	+
FTP	–	+	–	+
Telnet	–	–	–	+
News	–	+	–	+
Modem	–	–	+	+
Uhrzeit	7–19 Uhr	7–19 Uhr	0–24 Uhr	0–24 Uhr
Tage	Mo.–Fr.	Mo.–Fr.	Mo.–So.	Mo.–So.

Tabelle 11.2: Dienste-Check-Liste

In größeren Organisationen wird eine weitergehende Spezifikation der Kommunikationsprofile erforderlich sein.

Grundsätzlich gilt:

»Alles, was nicht explizit erlaubt ist, ist verboten!«

Externe Benutzer

Externe Benutzer sind Mitarbeiter der Organisation, die von unterwegs Zugriff auf aktuelle Daten benötigen oder ihre E-Mails lesen wollen, oder Servicefirmen, die auf die zu wartenden Rechnersysteme im zu schützenden Netz zugreifen müssen. Die Kommunikationsanforderungen aus dem unsicheren Netz müssen sorgfältig ausgewählt und festgelegt werden, weil jeder Zugriff auf das zu schützende Netz den Schutzbedarf erhöht.

neuKap11.fm Seite 344 Freitag, 18. Oktober 2002 3:52 15

Zum Beispiel kann es passieren, dass Servicearbeiten an Rechnersystemen im zu schützenden Netz aus Gründen hoher Verfügbarkeit sehr schnell stattfinden müssen. Mittels Telnet- oder FTP-Zugriff werden die notwendigen Arbeiten aus dem unsicheren Netz heraus durchgeführt und dabei gleichzeitig protokolliert.

Die Firewall-Sicherheitspolitik sollte weitere Kriterien festlegen:

- wer für die Festlegung der Kommunikationsprofile verantwortlich ist
- wer für die Vergabe der Kommunikationsprofile oder der einzelnen Dienste an die Benutzer verantwortlich ist
- wer für die Administration und damit auch für die Umsetzung der Filterregeln verantwortlich ist
- welche Informationen im Firewall-System protokolliert werden
- wer die Protokolldaten analysiert und in welchen Zeitabständen dies geschehen soll
- welche Protokolldaten analysiert werden sollen
- welche Alarme generiert werden und an wen sie gesendet werden sollen
- was passiert, wenn das Firewall-System einen Angriff meldet, z. B.:
  - Verbindung zwischen unsicherem und zu schützendem Netz unterbrechen
  - entscheiden, ob der Angreifer verfolgt werden soll
  - wer über den Angriff informiert wird (z. B. die Geschäftsführung, der Hersteller des Firewall-Systems, CERT usw.)
- wie erreicht werden kann, dass die Kommunikation zwischen dem unsicheren und dem zu schützenden Netz ausschließlich über das Firewall-System läuft, z. B. durch:
  - Organisationsanweisung an alle Benutzer
  - Festlegung eines Verantwortlichen, der überprüft, ob neue Zugänge geschaffen wurden
- wer die Einhaltung der Sicherheitspolitik regelmäßig/sporadisch überprüft

11.2 Zusätzliche Sicherheitsmaßnahmen

Das eigentliche Firewall-Produkt besteht aus Software und Hardware. Neben dieser technischen Sicherheitsmaßnahme müssen weitere Sicherheitsmaßnahmen beachtet werden, damit der sichere Betrieb des Firewall-Systems garantiert werden kann. Die im folgenden Abschnitt aufgeführten Sicherheitsmaßnahmen gelten auch allgemein für den Einsatz von IT-Systemen und sind in den meisten Organisationen vorhanden. Andere Sicherheitsmaßnahmen sind firewallspezifisch und müssen für den sicheren Betrieb eines Firewall-Systems umgesetzt werden, damit eine Sicherheit gewährleistet werden kann.

neuKap11.fm Seite 345 Freitag, 18. Oktober 2002 3:52 15

Diese zusätzlichen Sicherheitsmaßnahmen gliedern sich in die folgenden Unterpunkte:

- Infrastruktur
- Organisation
- Personal

11.2.1 Infrastruktur

Folgende infrastrukturelle Sicherheitsmaßnahmen tragen zur Erhöhung der Sicherheit des Firewallbetriebes bei:

- *Zugangsgesicherter Raum:* Sämtliche Komponenten des Firewall-Systems sollten in abgeschlossenen und zugangsgesicherten Räumen aufgestellt werden, um zu unterbinden, dass unberechtigte Personen die technischen Sicherheitsmechanismen ausschalten oder manipulieren.
- Eine *unterbrechungsfreie Stromversorgung (USV)* sollte installiert werden, um einen kurzzeitigen Stromausfall zu überbrücken, oder die Stromversorgung wenigstens solange aufrechtzuerhalten, dass ein geordnetes Herunterfahren angeschlossener Rechnersysteme möglich ist. Die Mehrzahl aller Stromausfälle ist innerhalb von 5 bis 10 Minuten behoben, sodass bei einer Überbrückungszeit von ca. 10 bis 15 Minuten noch 5 Minuten in Reserve bleiben, um das angeschlossene Firewall-System geordnet herunterfahren zu können, selbst wenn der Stromausfall länger andauert. Die meisten modernen USV-Geräte bieten Rechnerschnittstellen an, die ein automatisches Herunterfahren (Shut-down) nach einer vorher festgelegten Zeit einleiten können. Das Zeitintervall wird dem Zeitbedarf des Firewall-Systems und der Kapazität der USV entsprechend festgelegt. Alternativ zu einer lokalen USV kann die Stromversorgung unterbrechungsfrei aus einer vorhandenen Quelle bezogen werden, z. B. durch den Anschluss an eine zentrale USV.
- *Geschützte Leitungsführung:* Die Zuleitungen (zu schützendes und unsicheres Netz) sollen so eingerichtet werden, dass sie außerhalb des zugangsgeschützten Raumes nicht überbrückbar sind.
- Durch gute *Dokumentation und eindeutige Kennzeichnung* aller Leitungen des Firewall-Systems kann einer fehlerhaften Verkabelung vorgebeugt werden, die zu einer Überbrückung des Firewall-Systems führen könnte. Die Dokumentation ist ebenfalls für eine gute Wartung, eine erfolgreiche Fehlersuche und Instandsetzung erforderlich. Die Qualität dieser Dokumentation ist abhängig von der Vollständigkeit, der Aktualität und der Lesbarkeit.
- Durch Kopplung des Firewall-Systems an ein vorhandenes Netzwerkmanagementsystem können von diesem bestimmte Informationen über das Firewall-System abgefragt werden oder werden vom Firewall-System an das Netzwerkmanagementsystem gemeldet. Dazu gehören Statusmeldungen und Alarme, die durch das Auftreten sicherheitskritischer Ereignisse ausgelöst werden. Da

neuKap11.fm Seite 346 Freitag, 18. Oktober 2002 3:52 15

Netzwerkmanagementsysteme in der Regel lange Betriebszeiten erfüllen, z. B. 24 Stunden an 7 Tagen, erhöht die Kopplung des Firewall-Systems an das Netzwerkmanagementsystem die Verfügbarkeit des gesamten IT-Systems.

11.2.2 Organisation

Für den sicheren Betrieb eines Firewall-Systems müssen einige organisatorische Sicherheitsmaßnahmen berücksichtigt werden. Diese Maßnahmen betreffen die technische Realisierung, das Security Management, die Benutzer und die allgemeine Organisation.

Technische Realisierung

1. *Externe Zugänge:* Weitere externe Zugänge zum zu schützenden Netz, z. B. über einen Modem Server, sollten wie Zugänge aus dem unsicheren Netz behandelt werden. Dies lässt sich erreichen, indem z. B. ein Access Server mit angeschlossenen Modems auf die externe Seite des Firewall-Systems gestellt wird, sodass ein Zugang zu Rechnersystemen im zu schützenden Netz von dort aus z. B. nur über Telnet durchgeführt werden kann (siehe Kapitel 10.6 und 10.7).

   Klare Richtlinien, die allen Benutzern bekannt sind, müssen genau festlegen, dass keine externen Zugänge unter Umgehung des Firewall-Systems eingerichtet werden dürfen.

2. *Sichere Anordnung weiterer Komponenten im Bereich des Firewall-Systems:* Neben der Installation und dem Betrieb des Firewall-Systems müssen auch weitere Komponenten, die der Kommunikation zwischen zu schützendem und unsicherem Netz dienen, sicher angeordnet werden. Dazu gehören z. B. Internet und Intranet Server für die Bereitstellung von Informationen an interne oder externe Benutzer, Mail Server, DNS Server, Modem Server, zentrale Virenscanner usw.

Security Management

1. Festlegung der Verantwortlichkeiten für das Firewall-System

Die Verantwortlichkeiten für das Firewall-System müssen klar geregelt und getrennt sein. Für den Firewall-Einsatz müssen die Fachverantwortung und die Betriebsverantwortung festgelegt werden. Der Fachverantwortliche ist zuständig für die Erarbeitung der fachlichen Vorgaben für das Firewall-System. Die Fachverantwortung liegt i.d.R. beim IT-Sicherheitsmanagement, das ein Firewall-Sicherheitskonzept auf Grundlage der definierten Firewall-Sicherheitspolitik erstellt. Die Betriebsverantwortung hingegen umfasst den sicheren Betrieb und die Überwachung des Firewall-Systems. Diese Aufgabe wird vom Security-Administrator ausgeführt, der für die korrekte Einrichtung von weiteren Benutzern des Security Management verantwortlich ist.

neuKap11.fm Seite 347 Freitag, 18. Oktober 2002 3:52 15

2. Zugriffsrechte für das Security Management

Der Fachverantwortliche (IT-Sicherheitsmanagement) legt im Firewall-Sicherheitskonzept die Zugriffsrechte von Benutzern für das Security Management fest. Die Zugriffsrechte regeln, in welcher Funktion ein Administrator das Security Management nutzen darf. Der Betriebsverantwortliche (Security-Administrator) richtet die Funktionen ein, denen ein Administrator zugeordnet wird. Solche Funktionen sind z. B. Operator, Auditor (Revisor), Editor (Datenerfasser) usw. Dabei sollten immer nur so viele Zugriffsrechte vergeben werden, wie für die Wahrnehmung der spezifischen Aufgaben notwendig ist (»Need-to-know-Prinzip«). Der jeweils Verantwortliche veranlasst und dokumentiert die Veränderung von Zugriffsrechten. Aus der Dokumentation muss hervorgehen:

- welche Funktion unter Beachtung der Funktionstrennung mit welchen Zugriffsrechten ausgestattet wird,
- welcher Administrator welche Funktion wahrnimmt,
- welche Zugriffsrechte ein Administrator erhält und
- welche Konflikte bei der Vergabe von Zugriffsrechten aufgetreten sind. Konflikte können z. B. daraus resultieren, dass ein Administrator unvereinbare Funktionen wahrnimmt oder daraus, dass abhängig vom Firewall-System die Trennung bestimmter Zugriffsrechte nicht vorgenommen werden kann.

Der Security-Administrator aktiviert sinnvoll einsetzbare Protokollfunktionen zur Beweissicherung, falls das Security Management es zulässt. Dazu gehören erfolgreiche und erfolglose An- und Abmeldevorgänge, Fehlermeldungen des Systems und unerlaubte Zugriffsversuche.

In einem akuten Vertretungsfall muss der Security-Administrator kontrollieren, ob der Vertreter vom Fachverantwortlichen autorisiert ist, bevor er die erforderlichen Zugriffsrechte einrichtet.

3. Kontrolle der Protokolldaten

Die Protokollierung sicherheitsrelevanter Ereignisse ist als Sicherheitsmaßnahme nur wirksam, wenn die protokollierten Daten auch ausgewertet werden. Daher müssen die Protokolldaten in regelmäßigen Abständen durch einen Revisor ausgewertet werden. Wenn es technisch nicht möglich ist, die Rolle eines unabhängigen Revisors für Protokolldaten einzurichten, kann die Auswertung der Protokolldaten auch durch den Administrator erfolgen. In diesem Fall sind die Tätigkeiten des Administrators nur schwer zu kontrollieren. Das Ergebnis der Auswertung sollte daher dem IT-Sicherheitsbeauftragten, dem IT-Verantwortlichen oder einem anderen besonders zu bestimmenden Mitarbeiter vorgelegt werden.

Die regelmäßige Kontrolle und anschließende Löschung der Protokolldaten verhindert darüber hinaus ein übermäßiges Anwachsen der Protokolldaten. Da Protokolldaten in den meisten Fällen personenbezogene Daten beinhalten, ist

neuKap11.fm Seite 348 Freitag, 18. Oktober 2002 3:52 15

sicherzustellen, dass diese Daten nur zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes verwendet werden (vgl. §§ 14 Abs. 4 und 31 BDSG).

Die nachfolgenden Auswertungskriterien dienen als Beispiele, die Hinweise auf eventuelle Sicherheitslücken, Manipulationsversuche und Unregelmäßigkeiten erkennen lassen:

- Liegen die Zeiten des An- und Abmeldens außerhalb der Arbeitszeit (Hinweis auf Manipulationsversuche)?
- Häufen sich fehlerhafte Anmelde-Versuche (Hinweis auf den Versuch, Passworte zu erraten)?
- Häufen sich unzulässige Zugriffsversuche (Hinweis auf Manipulationsversuche)?
- Gibt es auffällig große Zeitintervalle, in denen keine Protokolldaten aufgezeichnet wurden (Hinweis auf eventuell gelöschte Protokollsätze)?
- Ist der Umfang der protokollierten Daten zu groß (eine umfangreiche Protokolldatei erschwert das Auffinden von Unregelmäßigkeiten)?
- Gibt es auffällig große Zeitintervalle, in denen anscheinend kein LogIn oder LogOut stattgefunden hat (Hinweis darauf, dass das konsequente Abmelden nach Arbeitsende nicht vollzogen wird)?

Wenn regelmäßig umfangreiche Protokolldateien ausgewertet werden müssen, ist es sinnvoll, ein Werkzeug zur Auswertung zu benutzen. Dieses Werkzeug sollte wählbare Auswertungskriterien zulassen und besonders kritische Einträge (z. B. mehrfache fehlerhafte Einlog-Versuche) hervorheben (siehe auch Kapitel 13.1 *Logbuch – Belastung oder Nutzen?*).

4. Informationsbeschaffung über Sicherheitslücken des Firewall-Systems

Wenn durch Veröffentlichungen neue Sicherheitslücken bekannt werden, müssen die erforderlichen organisatorischen und administrativen Maßnahmen ergriffen oder zusätzliche Sicherheits-Hardware bzw. -Software eingesetzt werden, um diese Lücken zu schließen.

Daher ist es sehr wichtig, sich über neu bekannt gewordene Schwachstellen zu informieren. Informationsquellen sind:

- Hersteller bzw. Vertreiber von Firewall-Systemen. Sie informieren registrierte Kunden über bekannt gewordene Sicherheitslücken ihrer Systeme und stellen korrigierte Varianten des Firewall-Systems oder Patches zur Behebung der Sicherheitslücken zur Verfügung. Dieser Service kann z. B. in einem Wartungsvertrag geregelt werden.
- Computer Emergency Response Teams (CERT)
- Bundesamt für Sicherheit in der Informationstechnik (BSI)

neuKap11.fm Seite 349 Freitag, 18. Oktober 2002 3:52 15

- hersteller- und systemspezifische sowie sicherheitsspezifische Newsgruppen im Internet
- IT-Fachzeitschriften

5. Reaktion auf Verletzungen der Sicherheitspolitik

Reaktionen auf Verletzungen der Sicherheitspolitik sollten vorab festgelegt werden, damit im Bedarfsfall schnell und wirksam reagiert werden kann.

Art und Herkunft der Verletzung müssen untersucht und angemessene schadensbehebende oder -mindernde Maßnahmen ergriffen werden sowie, falls erforderlich, zusätzlich schadensvorbeugende Konsequenzen gezogen werden. Welche Aktionen durchgeführt werden müssen, hängt sowohl von der Art der Verletzung als auch vom Verursacher ab.

Es muss vorab geklärt sein, wer dafür verantwortlich ist, Informationen über bekannte Sicherheitslücken einzuholen oder Informationen über aufgetretene Sicherheitslücken an andere Organisationen weiterzugeben. Auch muss dafür Sorge getragen werden, dass evtl. mitbetroffene Stellen schnellstens informiert werden (siehe auch Kapitel 13.1 *Logbuch – Belastung oder Nutzen?*).

6. Verpflichtung des Security-Administrators zur Datensicherung

Da die Datensicherung eine wichtige IT-Sicherheitsmaßnahme ist, sollte der betroffene Security Administrator zur Einhaltung des Datensicherungskonzeptes bzw. des Minimaldatensicherungskonzeptes für das Firewall-System verpflichtet werden. Eine regelmäßige Erinnerung und Motivation zur Datensicherung des Firewall-Systems sollte erfolgen.

Benutzer

1. Keine Weitergabe von Security Token und Passworten

Werden für die Authentisierung gegenüber dem Firewall-System Security Token verwendet, so ist die Sicherheit der Zugangs- und Zugriffsrechteverwaltung entscheidend von der sicheren Benutzung der Security Token abhängig. Dazu gehört auch, dass die Passworte geheim gehalten und die Security Token nicht weitergegeben werden. Den Benutzern muss bewusst sein, dass sie für ihre Passworte und Security Token verantwortlich sind. Sie können auch dafür verantwortlich gemacht werden, wenn Fremde damit Schaden anrichten.

2. Betreuung und Beratung der Benutzer, die über das Firewall-System kommunizieren

Der Einsatz eines Firewall-Systems erfordert eine Schulung der Benutzer, die sie in die Lage versetzt, das eingesetzte Firewall-System sachgerecht zu nutzen. Außer der Schulung muss den Benutzern für im laufenden Betrieb eventuell auftretende Probleme eine Betreuung und Beratung zur Verfügung stehen. Probleme können

neuKap11.fm Seite 350 Freitag, 18. Oktober 2002 3:52 15

aus unterschiedlichen Gründen auftreten, z. B. wegen Unzulänglichkeiten der Benutzer, die eventuell eine andere Art und Weise der Nutzung der Dienste über das Firewall-System erlernen müssen.

In größeren Organisationen kann es daher sinnvoll sein, eine zentrale Stelle mit der Betreuung der Benutzer, die über das Firewall-System kommunizieren, zu beauftragen, und diese allen Benutzern bekannt zu geben.

Allgemeine Sicherheitsmaßnahmen

1. Regelung für Wartungs- und Reparaturarbeiten am Firewall-System

Die ordnungsgemäße Durchführung von Wartungsarbeiten ist eine besonders wichtige vorbeugende Maßnahme, um das Firewall-System vor Störungen zu bewahren. Die Wartungsarbeiten sollten von vertrauenswürdigem Personal oder externen Firmen durchgeführt werden.

Wenn Wartungs- und Reparaturarbeiten durch Externe durchgeführt werden, sind Regelungen über deren Beaufsichtigung zu treffen: Während der Arbeiten sollte eine fachkundige Kraft die Arbeiten soweit beaufsichtigen, dass sie beurteilen kann, ob während der Arbeit nicht-autorisierte Handlungen, z. B. unerlaubte Zugriffsrechte aus dem externen Netz, vollzogen werden.

Vor und nach Wartungs- und Reparaturarbeiten sind folgende Maßnahmen einzuplanen:

- Ankündigung der Maßnahme gegenüber den betroffenen Benutzern
- Wartungstechniker müssen sich auf Verlangen ausweisen.
- Die dem Wartungstechniker eingeräumten Zutritts-, Zugangs- und Zugriffsrechte sind auf das notwendige Minimum zu beschränken und nach den Arbeiten zu widerrufen bzw. zu löschen.
- Nach der Durchführung von Wartungs- oder Reparaturarbeiten sind – je nach »Eindringtiefe« des Wartungspersonals – Passwortänderungen erforderlich.
- Die durchgeführten Wartungsarbeiten sind zu dokumentieren (Umfang, Ergebnisse, Zeitpunkt, evtl. Name des Wartungstechnikers).

2. Rechtzeitige Beteiligung des Personal-/Betriebsrates

Die Protokollierung ist eine Maßnahme, die geeignet ist, eine Verhaltens- oder Leistungsüberwachung von Benutzern zu ermöglichen, und bedarf daher der Mitbestimmung der Personalvertretung. Grundlage sind die Betriebsverfassungs- und Personalvertretungsgesetze von Bund und Ländern. Die rechtzeitige und umfassende Information des Betriebs- oder Personalrates kann eine Zeitverzögerung bei der Einführung eines Firewall-Systems verhindern.

neuKap11.fm Seite 351 Freitag, 18. Oktober 2002 3:52 15

11.2.3 Personal

Personelle Sicherheitsmaßnahmen können das Security Management und die Benutzer betreffen.

Security Management

1. Profil des Security Administrators

Der Security Administrator muss grundlegende Kenntnisse im Bereich IT-Sicherheit und speziell über Firewall-Systeme besitzen und diese Kenntnisse kontinuierlich aktualisieren und erweitern. Die Teilnahme an Schulungen über die Konfiguration und sichere Verwaltung des Firewall-Systems, die vom jeweiligen Hersteller oder Vertreiber angeboten werden, ist zu empfehlen. Der Security Administrator muss in der Lage sein, Fehlermeldungen und Alarme richtig einzuschätzen, um geeignete Gegenmaßnahmen ergreifen zu können. Bei Eingriffen von externem Personal ins Firewall-System muss der Administrator die durchgeführten Arbeiten nachvollziehen können.

2. Auswahl eines vertrauenswürdigen Administrators und Vertreters

Den Administratoren und Vertretern des Firewall-Systems muss großes Vertrauen entgegengebracht werden, da sie sehr weitgehende Befugnisse haben. Administrator und Vertreter sind in der Lage, auf alle gespeicherten Daten zuzugreifen, sie zu verändern und Berechtigungen zu vergeben, sodass erheblicher Missbrauch entstehen könnte.

Das hierzu eingesetzte Personal muss sorgfältig ausgewählt und regelmäßig darüber belehrt werden, dass seine Befugnisse nur für die erforderlichen Administrationsaufgaben verwendet werden dürfen.

3. Vertretungsregelungen

Vertretungsregelungen haben den Sinn, in vorhersehbaren (Urlaub, Dienstreise) und auch in unvorhersehbaren Fällen (Krankheit, Unfall, Kündigung) des Personenausfalls die Fortführung der Aufgabenwahrnehmung zu ermöglichen. Daher muss vor Eintritt eines solchen Falles geregelt sein, wer wen in welchen Angelegenheiten mit welchen Kompetenzen vertritt. Dies ist beim Firewall-System von besonderer Bedeutung, da dafür meist Spezialwissen erforderlich ist und eine zeitgerechte Einarbeitung unkundiger Mitarbeiter für den Vertretungsfall nicht möglich ist.

Für die Vertretungsregelungen sind folgende Randbedingungen einzuhalten:

- Der Verfahrens- oder Projektstand muss hinreichend dokumentiert sein.
- Der Vertreter muss geschult werden. Der Ausfall von Personen, die aufgrund ihres Spezialwissens nicht kurzfristig ersetzbar sind, bedeutet eine gravierende

neuKap11.fm Seite 352 Freitag, 18. Oktober 2002 3:52 15

Gefährdung des Normalbetriebes. In diesem Fall ist die Schulung eines Vertreters von besonders großer Bedeutung.

- Es muss festgelegt sein, welcher Aufgabenumfang im Vertretungsfall von wem wahrgenommen werden soll.
- Der Vertreter darf die erforderlichen Zugangs- und Zutrittsberechtigungen nur im Vertretungsfall erhalten.
- Ist es in Ausnahmefällen nicht möglich, für Personen einen kompetenten Vertreter zu benennen oder zu schulen, sollte frühzeitig überlegt werden, welche externen Kräfte für den Vertretungsfall eingesetzt werden können.

4. Geregelte Verfahrensweise beim Ausscheiden von Benutzern

Scheidet ein Benutzer aus, so ist zu beachten, dass sämtliche für den Ausscheidenden eingerichteten Berechtigungen in das Firewall-System entzogen bzw. gelöscht werden müssen. Dies betrifft auch die externen Zugangsberechtigungen via Datenübertragungseinrichtungen.

Benutzer

1. Anweisungen an die Benutzer bzgl. der Nutzung von Internetdiensten (Download, Foren)

Für Benutzer, die die angebotenen Internetdienste nutzen, müssen Organisationsanweisungen erstellt werden. Diese Organisationsanweisungen enthalten Anweisungen über das Verhalten von Benutzern, die an Diskussionsforen bzw. an Newsgroups teilnehmen, und über die Behandlung empfangener Dateien vor der Verwendung im eigenen System.

Die persönliche Meinung eines Benutzers innerhalb eines Diskussionsforums kann anhand seiner Mailadresse (z. B. nachname@firma-xyz.com) auch als Aussage der Firma xyz interpretiert und unter Umständen als solche verwendet werden. Hierdurch können große Probleme auftreten, die allen Beteiligten aufgezeigt werden müssen.

Nach dem Download einer Datei sind entsprechende Maßnahmen gegen Viren durchzuführen.

Bei Benutzung von WWW-Browsern müssen evtl. die Optionen für Java, Java Script und ActiveX von den Benutzern abgeschaltet werden.

2. Aufklärung der Benutzer über die Protokollierung von Firewall-Daten

Die Benutzer müssen darüber aufgeklärt werden, dass ihre Verbindungen über das Firewall-System protokolliert werden können. Gleichzeitig sollte der Grund der Protokollierung erklärt werden, damit er von den Benutzern verstanden und akzeptiert wird. Eine Aufklärung der Benutzer hat auch einen Warneffekt, der vor einem potenziellen Missbrauch schützen kann.

neuKap11.fm Seite 353 Freitag, 18. Oktober 2002 3:52 15

3. Sensibilisierung der Benutzer für mögliche Gefahren bei der Nutzung des Internet

Benutzer müssen darauf hingewiesen werden, welche Gefahren durch die Anbindung an das Internet entstehen können. Durch Aufklärung und Sensibilisierung der Benutzer kann verhindert werden, dass das Firewall-System z. B. aus Bequemlichkeit umgangen wird und dadurch eine ungeschützte Verbindung zum Internet mit all ihren Gefahren entsteht.

4. Schulung zum Thema Sicherheit

Die überwiegende Zahl von Schäden entsteht durch Nachlässigkeit. Um dem entgegenzuwirken, muss jeder einzelne Benutzer zum sorgfältigen Umgang mit der Informationstechnologie motiviert werden. Zusätzlich sind Verhaltensregeln zu vermitteln, die ein Verständnis für die Sicherheitsmaßnahmen wecken. Die Schulung zu Sicherheitsmaßnahmen soll insbesondere folgende Themen vermitteln:

- *Sensibilisierung für IT-Sicherheit:* Jeder Benutzer ist auf die Notwendigkeit der IT-Sicherheit hinzuweisen. Das Aufzeigen der Abhängigkeit der Organisation und damit der Arbeitsplätze reibungslosen Funktionieren der IT-Systeme ist ein geeigneter Einstieg in die Sensibilisierung. Darüber hinaus ist der Wert von Informationen herauszuarbeiten, insbesondere unter den Gesichtspunkten Vertraulichkeit, Integrität und Verfügbarkeit. Diese Sensibilisierungsmaßnahmen sind in regelmäßigen Zeitabständen zu wiederholen, evtl. auch durch praktische Hinweise z. B. in der Hauspost.
- *Benutzerbezogene IT-Sicherheitsmaßnahmen:* Dieses Thema soll die IT-Sicherheitsmaßnahmen vermitteln, die in einem Firewall-Sicherheitskonzept erarbeitet wurden und von den einzelnen Benutzern umzusetzen sind. Dieser Teil der Schulungsmaßnahmen hat eine große Bedeutung, da viele IT-Sicherheitsmaßnahmen erst nach entsprechender Schulung und Motivation effektiv umgesetzt werden können (z. B. zentraler Modem-Pool).
- *Vorbeugung gegen Social Engineering:* Die Benutzer sollen auf die Gefahren des Social Engineering hingewiesen werden. Die typischen Muster solcher Versuche, über gezieltes Aushorchen an vertrauliche Informationen zu gelangen, ebenso wie die Methoden, sich dagegen zu schützen, sollten bekannt gegeben werden. Da Social Engineering oft mit der Vorspiegelung einer falschen Identität einhergeht, sollten Benutzer regelmäßig darauf hingewiesen werden, die Identität von Gesprächspartnern zu überprüfen und insbesondere am Telefon keine vertraulichen Informationen weiterzugeben.

neuKap11.fm Seite 354 Freitag, 18. Oktober 2002 3:52 15

11.2.4 Notfall

1. Festlegung von Verfügbarkeitsanforderungen

Verfügbarkeitsanforderungen an das Firewall-System und die Dienste, die darüber zur Verfügung gestellt werden, müssen festgelegt werden. Bei Ausfall des Firewall-Systems ermöglicht ein Übersichtsplan über die Verfügbarkeitsanforderungen eine schnelle Aussage, ab wann ein Notfall vorliegt. Dies bildet die Grundlage für eine Untersuchung und Einrichtung von Backup-Möglichkeiten.

2. Backup-Möglichkeiten

Sind die Verfügbarkeitsanforderungen an bestimmte Dienste besonders hoch, müssen Backup-Möglichkeiten geschaffen werden, die diesen Anforderungen genügen. Zum Beispiel kann im zu schützenden Netz ein Rechnersystem im Bedarfsfall einen unmittelbaren Telnet-Zugriff einer Servicefirma benötigen. Dies kann bedeuten, dass bei Ausfall des Firewall-Systems ein zweites Firewall-System bereitstehen muss, das nur den Dienst Telnet bietet, oder die Servicefirma kann per Modem direkt auf das zu wartende Rechnersystem zugreifen. Im zweiten Fall stehen die Sicherheitsmechanismen eines Firewall-Systems nicht zur Verfügung.

11.3 Konzeptionelle Grenzen eines zentralen Firewall-Systems

Die Firewall-Systeme, die Sicherheitsdienste für die Kommunikation im Internet und Intranet bieten, sind sehr komplexe Sicherheitskomponenten.

Aber auch Firewall-Systeme können keine hundertprozentige Sicherheit durch technische Sicherheitsmaßnahmen gewährleisten. Im Folgenden sollen einige Aspekte betrachtet werden, die beim Einsatz von Firewall-Systemen zu beachten sind.

11.3.1 Hintertüren

Ein Firewall-System schützt genau die Kommunikationsverbindungen, die darüber laufen. Gibt es Kommunikationsübergänge am Firewall-System vorbei (backdoors), hat das System keinen Einfluss mehr. Aus diesem Grund ist es absolut wichtig, dass keine weitere Verbindung zwischen dem unsicheren Netz und dem zu schützenden Netz besteht, damit das »Common Point of Trust«-Konzept realisiert werden kann. Eine hohe Gesamtsicherheit des Firewall-Systems kann nur durch personelle und organisatorische Sicherheitsmaßnahmen erreicht werden.

neuKap11.fm Seite 355 Freitag, 18. Oktober 2002 3:52 15

11.3.2 Interne Angriffe

Ein Firewall-System bietet Sicherheitsdienste zur Abschottung gegen das unsichere Netz oder zur Kontrolle der Kommunikation zwischen dem unsicheren Netz und dem zu schützenden Netz. Ein Firewall-System hat nur sehr geringen Einfluss auf interne Angriffe.

Um internen Angriffen entgegenzuwirken, müssen weitere, ergänzende Sicherheitsmechanismen (z. B. Personal Firewall und/oder Intrusion-Detection-Systeme) eingeführt werden.

11.3.3 Angriffe auf Datenebene

Ein Firewall-System ist ursprünglich nicht in der Lage, im Bereich der erlaubten Kommunikation Angriffe auf der Datenebene zu erkennen. Dazu gehören: Angriffe durch das Senden von Malware wie E-Mail-Attachments, Downloads aus dem Web, Java Applets und Active-X-Controls. Angriffe, die über den Inhalt der Anwendungsdaten realisiert werden, können nicht alleine mit den Sicherheitsfunktionen eines Firewall-Systems abgewehrt werden. Die Komplexität der Anwendungen wie z. B. WWW-Server ist so groß, dass mit Kommunikationssicherheitseinrichtungen wie Firewall-Systemen keine hundertprozentige Sicherheit bei anwendungsdatenorientierten Angriffen erreicht werden kann (siehe auch Kapitel 10.8 *Virengefahr*).

11.3.4 Trittbrettfahrer

Ein potenzieller Angriffspunkt liegt darin, dass ein Angreifer aus dem unsicheren Netz eine Verbindung übernimmt, über die ein berechtigter Nutzer vom unsicheren Netz aus auf Rechnersysteme im zu schützenden Netz zugreift.

Schutz vor diesem Angiffstyp bietet eine Verschlüsselung der Kommunikation zwischen dem Firewall-System und der Workstation des Nutzers im unsicheren Netz, siehe Kapitel 7.5 *Virtual Private Networks, Secure Layer und Firewall-Systeme*.

11.3.5 Richtige Sicherheitspolitik und richtige Umsetzung der Sicherheitpolitik

Ein Firewall-System kann nur die Sicherheitsdienste erbringen, die entsprechend eingerichtet sind. Aus diesem Grund ist es von besonderer Bedeutung, dass eine Sicherheitspolitik erarbeitet wird, die darstellt, welche Ressourcen (Rechnersysteme, Kommunikationseinrichtungen, Daten usw.) im zu schützenden Netz einen hohen Schutzbedarf haben und wie sie geschützt werden sollen. Außerdem muss definiert werden, wie die Sicherheitsmechanismen für die Aufrechterhaltung des sicheren Betriebs eines Firewall-Systems regelmäßig/sporadisch überprüft werden.

neuKap11.fm Seite 356 Freitag, 18. Oktober 2002 3:52 15

Weitere Beispiele für Aspekte, die bei einer Sicherheitspolitik wichtig sind: Wer ist für die Festlegung der Kommunikationsprofile verantwortlich, wer ist für die Vergabe der Kommunikationsprofile oder der einzelnen Dienste an die Benutzer verantwortlich; wer ist für die Administration und damit auch für die Umsetzung der Filterregeln verantwortlich, welche Informationen werden im Firewall-System protokolliert; wer analysiert wann die Protokolldaten, was soll passieren, wenn ein Angriff über das Firewall-System erkannt wird?

11.3.6 Wissen und Hypothese

Mit einem Firewall-System können durch theoretisches Wissen und praktische Erfahrungen Fehlerursachen verhindert werden. Gerade bei innovativen Anwendungen und Technologien wie dem Internet wird mit einer Vielzahl von Hypothesen gearbeitet. Daher gibt es einen Bereich des Neuen, Unbekannten und auch Unerwünschten und Unvorhersehbaren, was wir mithilfe eines Firewall-Systems nicht beherrschen können, weil dieses nur auf Ereignisse reagieren kann, die wir bereits eindeutig kennen. Hier liegt eine Grenze von Firewall-Systemen. Diesem können wir nur mit weiteren, modular ergänzten Sicherheitsmechanismen entgegenwirken. Zum Beispiel vermag Intrusion Detection auch neuartige Angriffsversuche zu erkennen.

11.3.7 Security versus Connectivity – Risiko versus Chance

Je kleiner die Menge erlaubter Aktionen ist, um so geringer ist das Risiko, dass ein Schaden auftreten kann. Jeder Teilnehmer, jeder Rechner, der über ein Firewall-System kommunizieren darf, stellt ein zusätzliches Risiko dar. So stellen z.B. auch die erlaubten Kommunikationspartner ein Risiko dar, falls sie unberechtigte Kommunikationsverbindungen nutzen. Aus diesem Grund ist zu beachten: So wenig wie möglich/nötig über das Firewall-System zulassen, damit ein Höchstmaß an Sicherheit erreicht werden kann.

Je mehr erlaubt ist, um so größer ist das Risiko der Verwundbarkeit. Wenn nichts erlaubt ist, kann über das Netz auch kein Schaden auftreten. Hier wird das Spannungsfeld zwischen »security und connectivity« deutlich. Mithilfe eines Firewall-Systems sollen die Vorteile der Kommunikation nach außen genutzt werden, aber der mögliche Schaden durch diese Handlungen begrenzt werden.

Die Teilnehmer, die zur Erfüllung ihrer Aufgabenstellung kommunizieren müssen, sollen mit den Kommunikationsprotokollen und -diensten, die sie für ihre speziellen Aufgaben benötigen, zu den entsprechenden Zeiten dies tun dürfen – aber nur so weit, wie dafür nötig ist.

neuKap11.fm Seite 357 Freitag, 18. Oktober 2002 3:52 15

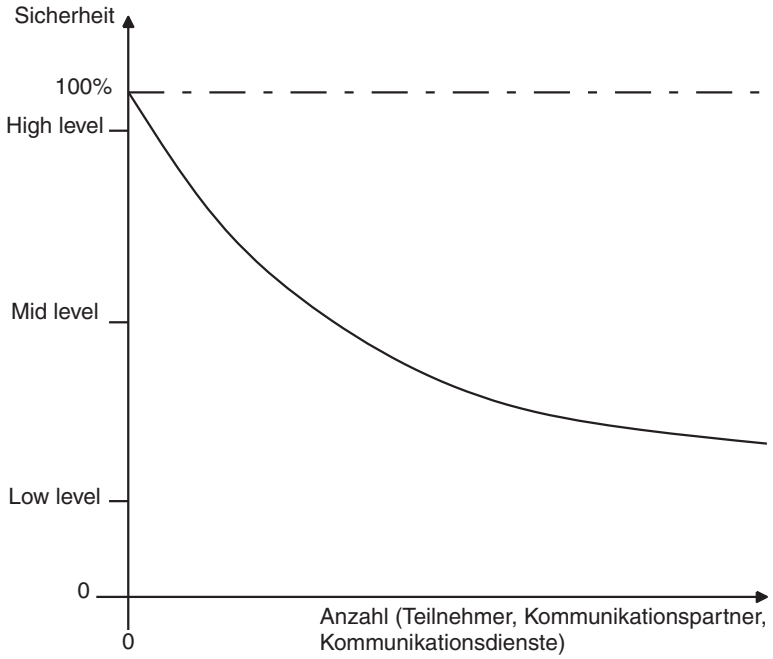


Abb. 11.1: Sicherheit versus Connectivity

11.3.8 Vertrauenswürdigkeit des Kommunikationspartners und der empfangenen Daten

Für die Entscheidungen, die eine Firewall-System durchführt, ist die Vertrauenswürdigkeit des Kommunikationspartners und der empfangenen Daten notwendig. Da diese Eigenschaften nicht durch Sicherheitsmechanismen des Firewall-Systems vollständig erbracht werden können, müssen hier weitere, ergänzende Sicherheitsmechanismen wie z. B. Verschlüsselung (VPN) oder digitale Signatur eingesetzt werden.

11.3.9 Zusammenfassung

Aus den konzeptionellen Grenzen eines zentralen Firewall-Systems folgt, dass bei einer praktischen Realisierung von Firewall-Systemen weitere ergänzende Sicherheitsmechanismen hinzugefügt werden müssen, damit die Verwundbarkeit minimiert wird und die Chancen der Ankopplung an das Internet risikoärmer genutzt werden können.

neuKap11.fm Seite 358 Freitag, 18. Oktober 2002 3:52 15

11.4 Praktische Sicherheit

In der Diskussion über die konzeptionellen Grenzen von Firewall-Systemen ist deutlich geworden, dass es keine hundertprozentige Sicherheit gibt.

Es gibt aber definierte Sicherheitsmechanismen und Sicherheitskriterien, um das Maß an Sicherheit zu erhöhen oder die Unsicherheiten zu verringern. Dabei muss für die konkrete Anwendung ein praxisgerechter Sicherheitsansatz realisiert werden.

Praxisgerechte Sicherheit von Firewall-Systemen ist dann gegeben, wenn

- mit den verfügbaren Ressourcen
- durch die bekannten Angriffe
- mit vertretbarem Aufwand

das Firewall-System nicht überwunden werden kann.

Die folgende Grafik verdeutlicht, wie in Abhängigkeit der Sicherheit – low, mid und high – und Aufwand betrachtet werden kann:

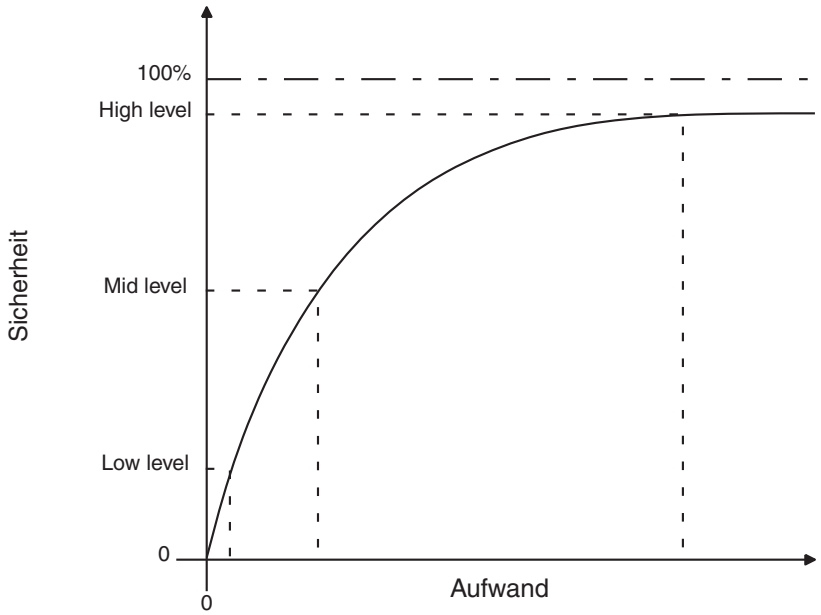


Abb. 11.2: Sicherheit versus Aufwand

Für Netze mit hohem Schutzbedarf kann mit sehr hohem Aufwand High-Level-Sicherheit erreicht werden. Um noch mehr Sicherheit zu erreichen, müssen zusätzlich weitere Sicherheitsmechanismen genutzt werden.

neuKap11.fm Seite 359 Freitag, 18. Oktober 2002 3:52 15

Sicherheitsziele bei der Umsetzung eines Firewall-Systems sind:

1. alle Unsicherheiten mit großer Wahrscheinlichkeit vollständig zu eliminieren
2. möglichst vielen Unsicherheiten mit passenden Sicherheitsmechanismen entgegenzuwirken und damit die Wahrscheinlichkeit eines Schadens durch einen erfolgreichen Angriff auf eine praktisch nicht vorkommende Größe zu minimieren
3. Unsicherheiten, die nicht verhindert werden können, zu erkennen, um im Angriffsfall im Nachhinein angemessen reagieren zu können, mit dem Ziel, den Schaden zu minimieren.
4. Angriffe im Vorfeld zu erkennen, damit erst gar kein Schaden auftreten kann.

neuKap11.fm Seite 360 Freitag, 18. Oktober 2002 3:52 15

neuKap12.fm Seite 361 Freitag, 18. Oktober 2002 3:52 15

Kapitel 12

Besondere Aufgabenstellungen bei Firewall-Systemen

Bei der Integration von Firewall-Systemen müssen in der Regel einige besondere Aufgabenstellungen bewerkstelligt werden. Solche Aufgaben sind die Umsetzung der Netzwerkadressen, die Verwaltung mehrerer Firewall-Systeme mithilfe eines Security Management, die Kommunikation über mehrere Firewall-Systeme und die Ausfallsicherheit.

12.1 Network Address Translation

Im Internet hat jeder eine eindeutige offizielle IP-Adresse, die zentral vom Network Information Center (NIC) und seinen Unterorganisationen vergeben und verwaltet wird. Da die Anzahl dieser offiziellen IP-Adressen aber begrenzt ist, gibt es den Mechanismus der Network Address Translation. Hier haben die Organisationen, die sich an das Internet anschließen, die Möglichkeit, mit für private Zwecke reservierten IP-Adressen im eigenen Bereich zu arbeiten. Durch den Mechanismus des Network Address Translation werden diese reservierten Adressen für das Intranet in die offiziellen IP-Adressen des Internets umgewandelt und umgekehrt.

Im zu schützenden Netz sollen die Rechnersysteme mit für private Zwecke reservierten IP-Adressen versehen werden. Damit diese eindeutig sind, sollten hier nur IP-Adressen stehen, die im Internet nicht vorkommen. Dazu gibt es so genannte reservierte IP-Adressen, die für das zu schützende Netz verwendet werden können. Die zur Verfügung stehenden reservierten IP-Adressen sind:

eine Class A Adresse:	10.0.0.0	– 10.255.255.255
16 Class B Adressen:	172.16.0.0	– 172.31.255.255
256 Class C Adressen:	192.168.0.0	– 192.168.255.255

Tabelle 12.1: Für private Zwecke reservierte IP-Adressen

Die Adressräume sind jeweils zusammenhängend. Diese IP-Adressen sind für private Zwecke reserviert und werden im Internet niemals vergeben. Da diese IP-Adressen nur im zu schützenden Netz verwendet werden, können alle Netze die gleichen reservierten Adressräume verwenden.

neuKap12.fm Seite 362 Freitag, 18. Oktober 2002 3:52 15

Je nach Bedarf kann der Adressraum ausgesucht werden. In großen zu schützenden Netzen, bei denen Subnetzmasken kein Problem darstellen, wird man z. B. die Class A Adresse 10.0.0.0 verwenden, bei einem kleinen zu schützenden Netz kann eine der Class C Adressen, z. B. 192.168.1.0, verwendet werden.

Entsprechende Hinweise sind im RFC 1918 zu finden. Hier sind auch die entsprechenden IP-Adressräume reserviert.

Für externe IP-Adressen ist die Vergabe bei der Registrierungsstelle zu berücksichtigen.

Beispiele für die Aufteilung der reservierten Adressen im zu schützenden Netz:

1. Kleine Organisation mit drei Abteilungen, keine Abteilung hat mehr als 250 Rechnersysteme, eher deutlich weniger
   - Abteilung 1: IP-Adressen 192.168.1.0 - 192.168.1.255
   - Abteilung 2: IP-Adressen 192.168.2.0 - 192.168.2.255
   - Abteilung 3: IP-Adressen 192.168.3.0 - 192.168.3.255

   Vorteile dieser Adressaufteilung sind die überschaubare Netzgröße, eine klare Trennung der einzelnen Abteilungen und dass die Standard-Netzmaske in den einzelnen Subnetzen anwendbar ist.

2. Große Organisation, viele Abteilungen mit nochmaliger Unterteilung in Unterabteilungen oder Abteilungen mit sehr großer Zahl von Rechnersystemen:
   - Wahl des Netzes 10.0.0.0
   - Abteilungen bekommen jeweils ein eigenes Class B Netz, das nach eigenem Bedarf weiter unterteilt werden kann, z. B. in Class C Subnetze oder kleinere.
   - Zu beachten ist, dass die Subnetze mit der Adresse 0 und 255 nicht verwendet werden sollten, da es ansonsten mit den Netzadressen und mit Broadcasts zu Uneindeutigkeiten kommen kann.

   Beispiel: Die Subnetze 10.0.xxx.yyy (Problem mit Netzadressen 10.0.0.0) oder 10.255.xxx.yyy (Problem beim Broadcast 10.255.255.255) oder 10.1.255.xxx (wie letztes Beispiel) sollten nicht vergeben werden.

3. Die Class B Adressen können bei Organisationen mit mittlerem Bedarf eingesetzt werden. Im Allgemeinen wird man aber gleich zur einfachen Lösung mit den 192.168.xxx.yyy oder zur großen Lösung mit dem Netz 10.0.0.0 greifen.

12.1.1 Firewall-System und Network Address Translation

Firewall-Systeme bzw. Firewall-Elemente wie Application Gateways führen zwar keine Network Address Translation in der »reinen Lehre« durch, erreichen aber den gleichen Zweck, indem sie zum unsicheren Netz offizielle Internet IP-Adressen und zum Intranet in der Regel reservierte IP-Adressen haben.

neuKap12.fm Seite 363 Freitag, 18. Oktober 2002 3:52 15

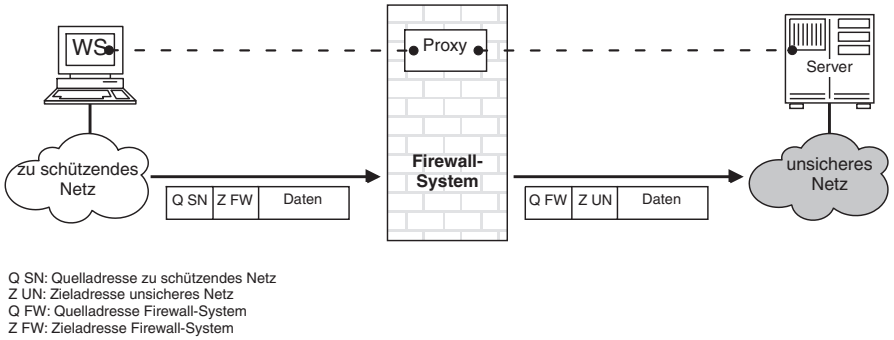


Abb. 12.1: Firewall-System und Network Address Translation

Bei einer Kommunikation über ein Firewall-System hat ein Application Gateway eine Kommunikationsverbindung mit dem Rechnersystem im zu schützenden Netz (Workstation) und eine Kommunikationsverbindung mit dem Rechnersystem im unsicheren Netz (Server), d.h., das Firewall-System ist der jeweilige Kommunikationspartner. Das Firewall-System kommuniziert im unsicheren Netz mit der offiziellen Internet-IP-Adresse und im zu schützenden Netz (Intranet) mit der reservierten IP-Adresse. Dieses Verhalten ist wie das von Network Address Translation, nur wird es hier mit anderen Mechanismen erreicht.

Als Kommunikationspartner im zu schützenden Netz ist immer die IP-Adresse, eine IP-Adresse aus dem reservierten IP-Adressbereich des Intranets, des Firewall-Systems angegeben (Abb. 12.1 *Ziel-Adresse*).

Als Kommunikationspartner im unsicheren Netz ist immer die offizielle Internet IP-Adresse des Firewall-Systems angegeben (Abb. 12.1 *Quell-Adresse*). Dadurch ist nicht erkennbar, welches Rechnersystem sich hinter der Kommunikation über das Firewall-System im zu schützenden Netz verbirgt.

12.1.2 Probleme für Netze, die mit illegalen IP-Adressen arbeiten

Einige Netze haben in der Vergangenheit das Konzept der reservierten IP-Adressen nicht genutzt, was bei der Ankopplung an das Internet zu Problemen führen kann. Werden im zu schützenden Netz illegalerweise IP-Adressen verwendet, die anderen Organisationen offiziell zugewiesen wurden, gibt es beim Übergang Probleme, weil die IP-Adressen im unsicheren und im zu schützenden Netz vorkommen.

Hier gibt es im Prinzip zwei Lösungsansätze:

1. Vergabe von reservierten IP-Adressen im Intranet

   Die illegal genutzten IP-Adressen werden nicht mehr verwendet, sondern mit reservierten IP-Adressen, mit denen es keine Probleme gibt, vertauscht. Bei diesem Lösungsansatz haben einige große Organisationen Probleme, weil dies bei einer großen Anzahl von Rechnersystemen sehr aufwendig sein kann.

neuKap12.fm Seite 364 Freitag, 18. Oktober 2002 3:52 15

2. Mapping der IP-Adressen

   Die illegalen IP-Adressen werden auf reservierte Adressen gemapped, damit keine Probleme mehr auftreten. Dies wird z. B. durch eine Substitutionstabelle oder mithilfe einer einfachen Mappingregel abhängig von den verwendeten illegalen Adressen realisiert. Einige Firewall-Produkte bieten das Mapping der IP-Adressen als zusätzliche Funktionalität an.

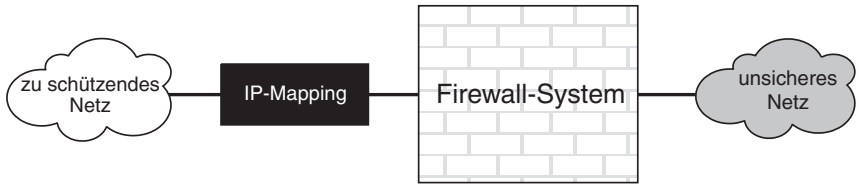


Abb. 12.2: Mapping der IP-Adressen

12.2 Domänen-Namen (Domain-Namen)

Im Allgemeinen gibt es einen Primary DNS Server im Internet und einen Primary DNS Server im Intranet. Namen und IP-Adressen des Intranets sollen nur dem DNS Server im Intranet bekannt sein. Dies ist nötig, damit die Adressenvergabe im Internet eindeutig bleibt.

Wegen der Eindeutigkeit der Namen im gesamten Internet (einschließlich des eigenen Intranet) sollten die Domain-Namen für das Intranet auch an das Namenschema des Internets angepasst sein. Dazu kann der Domain-Name im Intranet (Subdomain-Name) vor den Domain-Namen im Internet gestellt werden.

Beispiel:

Internet-Domain : `firma.de`

Intranet-Domain : `intra.firma.de`

Durch dieses Konzept kann bei großen Intranets ein vereinfachtes Verfahren für die DNS-Server- und Firewall-Konfiguration realisiert werden.

12.3 Verwaltung mehrerer Firewall-Systeme mithilfe eines Security Managements

In großen Organisationen kann die Anforderung bestehen, dass mehrere Übergänge zu unsicheren Netzen realisiert werden müssen. Dann ist es sinnvoll, mit einem Security Management eine Vielzahl von Firewall-Systemen zentral verwalten und steuern zu können.

neuKap12.fm Seite 365 Freitag, 18. Oktober 2002 3:52 15

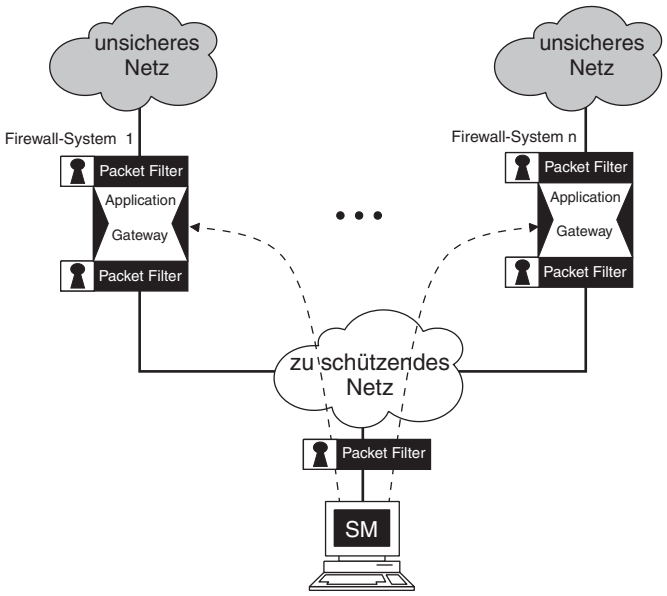


Abb. 12.3: Verwaltung mehrerer Firewall-Systeme

Mithilfe des zentralen Security Managements ist es möglich, mehrere Firewall-Systeme zu verwalten (siehe Abb. 12.3). Dadurch kann die Sicherheitspolitik einer Organisation bei mehreren Übergängen zu unsicheren Netzen sehr einfach realisiert werden. Zwischen dem Security Management und den Firewall-Systemen werden die Informationen in gesicherter Form ausgetauscht. Im Intranet können mit dem zentralen Security Management auch noch weitere Firewall-Elemente wie Packet Filter und Application Gateway verwaltet werden (siehe auch Kapitel 10 *Praktischer Einsatz von Firewall-Systemen*).

12.4 Geschachtelte Firewall-Konstellationen

Es gibt auch Anwendungen in einer Organisation, in denen eine geschachtelte Firewall-Konstellation auftreten kann. Die folgende Abbildung 12.4 zeigt exemplarisch und vereinfacht eine solche Konstellation.

Zwischen dem unsicheren und dem zu schützenden Netz ist ein Firewall-System eingerichtet. Außerdem ist noch ein weiteres Firewall-System im zu schützenden Netz selber installiert, um eine besonders zu schützende Organsationseinheit (z. B. den Vorstand) zu separieren. Möchte nun ein Benutzer von der Workstation 1 oder 2 Dienste eines Servers im unsicheren Netz nutzen, muss dies entsprechend im Firewall-System 1 berücksichtigt werden. Möchte aber ein Benutzer von der Workstation 3 diesen Server nutzen, muss dies im Firewall-System 1 und 2 berücksichtigt werden.

neuKap12.fm Seite 366 Freitag, 18. Oktober 2002 3:52 15

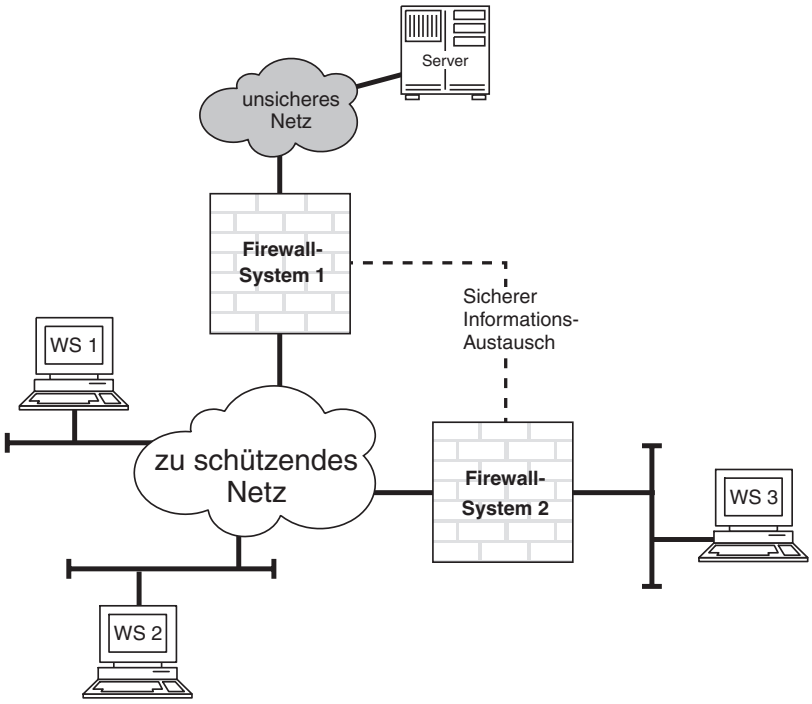


Abb. 12.4: Geschachtelte Firewall-Konstellationen

Dieser Fall kann entweder mit zwei unabhängigen Security Managements oder mit einem Security Management realisiert werden. Falls nur ein Security Management verwendet wird, werden an dieses besondere Anforderungen gestellt. Zwischen den beiden Firewall-Systemen müssen Informationen über die Authentikation und das Ziel der Daten in gesicherter Form ausgetauscht werden.

12.5 Verfügbarkeit

Im Internet-Zeitalter besteht für einige Organisationen, z. B. Application Service Provider (ASPs) die Anforderung, mit Rechnersystemen 24 Stunden verfügbar zu sein. Der Anwender muss sich darauf verlassen können, dass die Services, die er für die Erledigung seiner Aufgaben benötigt, »immer« verfügbar sind. Dies betrifft alle Komponenten, die ein Firewall-System ausmachen, aber auch die Verfügbarkeit des Netzes, insbesondere die Verfügbarkeit über das Internet. Inwieweit Organisationen in der Lage sind, Quality of Service im Internet zu garantieren, hängt wesentlich davon ab, ob die Internet Provider (ISPs) dies zukünftig global garantieren können.

neuKap12.fm Seite 367 Freitag, 18. Oktober 2002 3:52 15

Aus der Sicht des Anwenders müssen Mindestanforderungen im Bereich »Quality of Service« garantiert werden, damit das Risiko der Nichtverfügbarkeit sinnvoll abgeschätzt werden kann. Deshalb müssen für die Firewall-Systeme Redundanzlösungen zur Verfügung gestellt werden, die eine hohe Verfügbarkeit gewährleisten.

Bezüglich der Verfügbarkeit der Komponenten eines Firewall-Systems muss ein Verfügbarkeitskonzept erarbeitet werden. Die wichtigsten Komponenten müssen dementsprechend redundant ausgelegt werden. Außerdem ist Loadbalancing notwendig, damit eine passende Verfügbarkeit realisiert werden kann, um den Grad an »Quality of Service« zu erreichen, der für die Anwendung notwendig ist /Harl2000/. Dies kann z.B. durch Firewall-Konstellationen realisiert werden, die einen Hot-stand-by-Modus haben und innerhalb weniger Minuten in der Lage sind, die Arbeit von ausgefallenen Firewall-Elementen zu übernehmen oder im Cold-stand-by zu arbeiten und z.B. innerhalb von zwei Stunden als Ersatz für ein ausgefallenes Firewall-Element verwendet werden zu können. Dazu müsste dann der Security Administrator verfügbar sein.

Wichtig ist, dass Verfügbarkeitsüberlegungen durchgeführt werden, bevor ein Verfügbarkeitsproblem auftritt (siehe auch die Kapitel 5 *Elemente eines Firewall-Systems* und 6 *Konzepte für Firewall-Systeme*).

neuKap12.fm Seite 368 Freitag, 18. Oktober 2002 3:52 15

neuKap13.fm Seite 369 Freitag, 18. Oktober 2002 3:52 15

Kapitel 13

Weiterführende Aufgabenstellungen bei Firewall-Systemen

In diesem Kapitel werden einige weiterführende Aufgabenstellungen behandelt, die mit dem Betrieb von Firewall-Systemen verbunden sind. Dazu gehören die Protokollierung der sicherheitsrelevanten Daten in Logbüchern, die Frage der Sicherheit von Java und ActiveX, die notwendigen Aufwendungen für Beschaffung und Betrieb eines Firewall-Systems, die Evaluierung und Zertifizierung einer Firewall-Lösung und die Weiterentwicklung von Firewall-Systemen.

13.1 Logbuch – Belastung oder Nutzen?

Die meisten Firewall-Lösungen generieren Protokolldaten, die in Logbüchern festgehalten und verarbeitet werden müssen. In diesem Kapitel soll diskutiert werden, ob die Protokollierung eine Belastung darstellt, die überflüssig ist, oder ob sie für den Betrieb einer Firewall-Lösung einen verwertbaren Nutzen erbringt. Außerdem werden hier die Aspekte Alarmierung, Beweissicherung, Schutz der Protokolldaten, Aktionen nach Erkennen einer Sicherheitsverletzung sowie der Datenschutz behandelt.

13.1.1 Ziele der Protokollierung

Mithilfe der Protokollierung können unterschiedliche Ziele erreicht werden, je nachdem, welche Informationen protokolliert und wie sie ausgewertet werden.

Erkennung von Sicherheitsverletzungen

Im Logbuch eines Firewall-Systems werden sowohl Informationen über gewöhnliche (nicht-sicherheitsrelevante) als auch solche über außergewöhnliche (sicherheitsrelevante) Ereignisse gespeichert.

Die Auswertung dieser Ereignisse dient der Feststellung, ob tatsächlich eine Sicherheitsverletzung vorgelegen hat und welche Informationen und Rechnersysteme davon betroffen waren.

Hierdurch können Angriffe auf das Firewall-System selbst und auf Rechnersysteme im zu schützenden Netz, die über das Firewall-System stattgefunden haben, erkannt und Reaktionen auf Sicherheitsverletzungen eingeleitet werden.

neuKap13.fm Seite 370 Freitag, 18. Oktober 2002 3:52 15

Beweissicherung der Handlungen von Benutzern

Die Speicherung von Ereignissen stellt sicher, dass über Handlungen von Benutzern bzw. über Prozesse, die im Namen dieser Benutzer ausgeführt werden, Informationen gespeichert werden, damit die Folgen solcher Handlungen dem betreffenden Benutzer zugeordnet werden können und der Benutzer für seine Handlungen verantwortlich gemacht werden kann.

Dieser Aspekt der Protokollierung hat eine starke Abschreckungswirkung gegenüber solchen Benutzern, die sicherheitsgefährdende Aktionen in Erwägung ziehen (z. B. Mitarbeiter von Firmen, die Servicearbeiten auf Rechnersystemen im zu schützenden Netz durchführen).

13.1.2 Protokollierung von Ereignissen

Firewall-Elemente müssen die Möglichkeit bieten, Ereignisse wie Handlungen von Benutzern mit den dazugehörigen Informationen festzuhalten, damit mit ihrer Hilfe Sicherheitsverletzungen erkannt werden können. Die Protokolldaten zu möglichen Ereignissen können auf verschiedenen Ebenen erzeugt werden.

Fehlerhafter Authentikationsprozess

Hier werden fehlgeschlagene Versuche von Benutzern oder Angreifern festgehalten, sich mit dem Firewall-System zu authentifizieren.

Mögliche Ursachen:

- Verwendung einer nicht erlaubten Identifikation (Benutzername)
- fehlerhaftes kryptographisches Authentikationsprotokoll

Verstoß gegen das Regelwerk, bezogen auf die Analyse der Kommunikationsdaten

Hier wird festgehalten, ob bei der Analyse der Kommunikationsdaten über das Firewall-System ein Verstoß gegen das Regelwerk (Sicherheitspolitik) festgestellt worden ist.

Beispiele:

- versuchte Nutzung eines unerlaubten Kommandos (z. B. »del«) bei einer FTP-Verbindung
- versuchte Nutzung eines nicht erlaubten Dienstes (z. B. Telnet)
- versuchte Nutzung des Firewall-Systems zu einer nichterlaubten Zeit (z. B. sonntags um 5.00 Uhr)

Erkennung von Angriffsversuchen auf das Firewall-System selbst

Das Firewall-System selbst erkennt, ob ein Angriffsversuch stattgefunden hat.

neuKap13.fm Seite 371 Freitag, 18. Oktober 2002 3:52 15

Beispiele:

- Fehlerhafte Authentikation mit dem Security Management (z. B. Angreifer)
- Überschreitung des Füllstandes eines Logbuches

Identifizierung eines Fehlverhaltens der Firewall-Software und -Hardware

Das Firewall-Element erkennt selbst, dass ein Fehlverhalten aufgetreten ist, das für den normalen Betrieb der Firewall nicht vorgesehen ist.

Beispiele:

- Die Software befindet sich in einem nicht definierten Zustand (z. B. Automat des Analysemoduls).
- Ein Defekt des Speichermediums wurde identifiziert (z. B. Festplatte).

Speicherung der Aktionen, die über das Firewall-System durchgeführt worden sind

Das Firewall-System speichert alle Aktionen, die bei der Kommunikation über das Firewall-System durchgeführt worden sind.

Beispiele:

- Informationen über eine Telnet- oder FTP-Verbindung
- Informationen über Aktionen mit dem Security Management

Ein weiterer Aspekt, der für den sicheren Betrieb eines Firewall-Systems zu beachten ist, ist die Protokollierung aller Aktivitäten, die mit dem Security Management durchgeführt werden. Dieser Bereich ist besonders gefährdet, weil mithilfe des Security Management ein direkter Einfluss auf das Regelwerk genommen werden kann (siehe Kapitel 5 *Elemente eines Firewall-Systems*).

Beispiel:

Welcher Administrator des Firewall-Systems hat zu welchem Zeitpunkt welche Aktionen mit dem Security Management durchgeführt, z. B.

- Rechte an Benutzer vergeben
- Logbücher gelöscht.

13.1.3 Alarmierung

Eine Alarmierung über sicherheitsrelevante Ereignisse kann auf unterschiedlichen Ebenen erfolgen. Typischerweise werden sicherheitsrelevante Ereignisse in einem Firewall-Element identifiziert und abhängig von der Definition im Regelwerk entweder in ein Logbuch geschrieben oder als Spontane Meldung an eine höhere Instanz, das Security Management, gesendet. Nach einem bestimmten vorgegebenen Verfahren werden dann die Logbücher zu einem späteren Zeitpunkt dem Security Management ebenfalls zur Verfügung gestellt.

neuKap13.fm Seite 372 Freitag, 18. Oktober 2002 3:52 15

Dazu muss in den Firewall-Elementen mithilfe des Regelwerkes definiert werden, welches Ereignis besonders sicherheitsrelevant ist und sofort gemeldet, und welches Ereignis erst in ein Logbuch eingetragen und später dem Security Management zur Verfügung gestellt wird.

Im Security Management selbst kann dann wiederum auf verschiedene Weisen mit den Spontanen Meldungen verfahren werden: Sie können dem Administrator direkt mithilfe von visuellen und akustischen Signalen angezeigt werden, oder sie werden zuerst durch einen Auswertungsmechanismus analysiert, dessen Ergebnis, z. B. die Identifizierung eines Angriffes, entsprechend angezeigt wird.

Es ist auch möglich, dass der Auswertungsmechanismus erst alle Logbücher aus den unterschiedlichen Firewall-Elementen ausliest und das Ergebnis dieser Analyse in die Entscheidung mit einbezieht, ob sich hinter einer Spontanen Meldung ein Angriff verbirgt.

Mit dem Mittel der Spontanen Meldungen ist eine aktuelle Erkennung von sicherheitsrelevanten Ereignissen und von Sicherheitsverletzungen möglich. Es sollte auch einen Weg geben, eine Alarmierung von einem Security Management zu einem Netzwerkmanagement über standardisierte Netzwerkmanagementprotokolle wie z. B. SNMP zu senden. Vom Netzwerkmanagement aus könnten dann definierte Reaktionen eingeleitet werden.

13.1.4 Beweissicherung

Die Beweissicherung hat das Ziel, Handlungen zu protokollieren, die über das oder mit dem Firewall-System durchgeführt werden, damit sie zu einem späteren Zeitpunkt als Beweismittel verwendet werden können. Damit dies möglich ist, müssen die gespeicherten Protokolldaten in den Logbüchern gegen Manipulationen geschützt werden.

Die Protokollierung folgender Vorkommnisse ist für eine Beweissicherung sinnvoll:

Servicearbeiten

Servicearbeiten, die remote aus dem unsicheren Netz auf Rechnersysteme im zu schützenden Netz durchgeführt werden, werden im Firewall-System protokolliert, damit die Protokolldaten als Beweissicherung für das Handeln der Mitarbeiter der Service-Firma verwendet werden können.

Beispiel:

Eine Service-Firma wartet mithilfe von Telnet ein Rechnersystem im zu schützenden Netz. Auf dem Firewall-System wird festgehalten, welcher Mitarbeiter der Service-Firma zu welcher Zeit und wie lange auf einem bestimmten Rechnersystem gearbeitet hat. Im Bedarfsfall wird sogar die ganze Telnet-Session mitprotokolliert.

neuKap13.fm Seite 373 Freitag, 18. Oktober 2002 3:52 15

Falls nun das Rechnersystem nach Abschluss der Servicearbeiten nicht mehr funktionsfähig ist, kann mit den Protokolldaten aus den Logbüchern festgestellt werden, ob ein Mitarbeiter der Service-Firma dafür verantwortlich ist oder nicht.

13.1.5 Schutz der Protokolldaten

Protokolldaten kommen als Beweismittel bei straf- bzw. arbeitsrechtlichen Ermittlungen in Frage. Aus diesem Grund sind die ordnungsgemäß erfolgte Speicherung sowie die zweifelsfreie Echtheit bzw. Unversehrtheit der Protokolldaten in den Logbüchern für ihre Verwertbarkeit von besonderer Bedeutung.

Dazu muss verhindert werden, dass Angreifer in der Lage sind, die Protokollierung auszuschalten, die Protokolldaten in den Logbüchern zu löschen oder sie inhaltlich zu manipulieren. Dies kann durch folgende Schutzmechanismen erreicht werden:

- Im Security Management muss durch Zugangskontrolle und Rechteverwaltung dafür gesorgt werden, dass nur Berechtigte in der Lage sind, auf die Protokolldaten zuzugreifen.
- Die Protokolldaten aller Firewall-Elemente sollten über einen vertrauenswürdigen Pfad an das Security Management geschickt werden, damit sie vor ihrer Auswertung und endgültigen Speicherung nicht verändert werden können.

13.1.6 Reaktionen auf eine Sicherheitsverletzung

Falls eine Sicherheitsverletzung durch die Sicherheitsmechanismen im Firewall-System erkannt wird, müssen Aktionen eingeleitet werden. Im Folgenden soll beschrieben werden, in welcher Reihenfolge und mit welchen Aktionen reagiert werden kann.

Es muss entschieden werden, ob das Firewall-System oder Teile des Firewall-Systems sofort abgeschaltet werden sollen.

Wer diese Entscheidung treffen und durchführen darf, muss genau festgelegt sein.

Eine automatische Abschaltung des Firewall-Systems kann eingerichtet werden, wenn sichergestellt ist, dass keine Verfügbarkeitsaspekte verletzt werden.

Je nach Angriff kann die Abschaltung auf verschiedenen Ebenen erfolgen:

- Es können z. B. nur bestimmte Benutzer, bestimmte Dienste, bestimmte Rechnersysteme usw. gesperrt oder die Zeiten reduziert werden, zu denen eine Kommunikation über das Firewall-Sytem stattfinden darf.
- Es kann aber auch das ganze Firewall-System abgeschaltet werden, wenn das Risiko eines möglichen Schadens zu groß wird.

neuKap13.fm Seite 374 Freitag, 18. Oktober 2002 3:52 15

Der Angriff muss analysiert werden.

Falls eine Sicherheitsverletzung erkannt wird, werden die dazu gespeicherten Protokolldaten in den Logbüchern dahingehend analysiert, von welcher Person und von welchem Rechnersystem dieser Angriff aus dem unsicheren Netz durchgeführt wurde.

Außerdem wird analysiert, auf welches Rechnersystem im zu schützenden Netz und auf welche Informationen dort der Angriff gezielt hat. Für diese Analyse können auch die Logbücher der Rechnersysteme hinzugezogen werden.

Grundsätzlich muss entschieden werden, ob der Angreifer verfolgt werden soll. Zumindest kann festgestellt werden, welche IP-Adresse, d.h. welche Firma oder Person sich hinter dem betreffenden Angriff verbirgt.

Auch wenn die rechtlichen Möglichkeiten einer Verfolgung beschränkt sein sollten, da ja jeder Benutzer jede IP-Adresse annehmen kann, sollte eine Verfolgung in Erwägung gezogen werden, weil hierdurch der Angreifer erkennt, dass die Protokolldaten analysiert wurden und er bei einem erneuten Angriffsversuch erkannt werden kann.

Die Möglichkeit besteht, dass ein Angreifer eine andere Organisation als Sprungbrett nutzt, um seine Angriffsversuche durchzuführen. Wenn diese Organisation darüber informiert wird, kann sie zukünftig verhindern, dass der Angreifer sie als Sprungbrett verwendet.

Eine erneute Sicherheitsverletzung muss verhindert werden.

Nach der genauen Analyse des Angriffes muss eine Strategie entwickelt werden, wie eine solche Sicherheitsverletzung in Zukunft verhindert werden kann. Dabei gibt es verschiedene Möglichkeiten, mit dem Firewall-System zu reagieren:

- Der Angriff wird in die Wissensbasis der Protokollauswertung aufgenommen, damit ein erneuter Angriffsversuch schneller erkannt wird und entsprechend reagiert werden kann.
- Es muss überprüft werden, ob ein solcher Angriff zukünftig mit neuen und weiteren Sicherheitsmechanismen verhindern werden kann. Dazu kann das Angriffsszenarium mit dem Hersteller des Firewall-Systems diskutiert werden. Der Hersteller sollte auf jeden Fall über den Angriff informiert werden, damit er darauf reagieren und auch die anderen Anwender seiner Firewall-Systeme informieren kann. Unter diesem Aspekt ist die Information für alle Beteiligten von Nutzen.
- Weiterhin ist es mithilfe eines Firewall-Systems möglich, die Rechte einzuschränken, damit ein solcher Angriff nicht mehr stattfinden kann. Folgende Einschränkungen kommen in Betracht:
  - Benutzer
  - Rechnersysteme

neuKap13.fm Seite 375 Freitag, 18. Oktober 2002 3:52 15

- Dienste
- Zeiten, zu denen die Kommunikation über das Firewall-System möglich ist
- Kommandos der Anwendungen
- Authentikationsversuche

Außerdem besteht die Möglichkeit, mehr Protokolldaten produzieren zu lassen, die bei einem erneuten Angriff mehr Informationen zur Verfügung stellen, die für die Verfolgung bzw. Abwehr des Angriffes genutzt werden können.

13.1.7 Datenschutzaspekte

Protokolldaten von Firewall-Systemen haben grundsätzlich Datenschutzrelevanz. Die aufgezeichneten Daten über die Aktivitäten von Benutzern dürfen dabei nur zum Nachweis der fehlerfreien und ordnungsgemäßen Datenverarbeitung und nicht zur Verhaltens- und Leistungskontrolle verwendet oder ausgewertet werden. Es muss also genau festgelegt werden, wer diese Daten wie, mit welchen Hilfsmitteln, in welchen Abständen und zu welchen Zwecken auswerten darf. Es empfiehlt sich, die Personalvertretung bei der Festlegung der zulässigen Auswertungen der Protokolldateien sowie der Art ihrer Nutzungen einzubinden.

Die aufgezeichneten Protokolldaten müssen aus Sicht des Datenschutzes vollständig sein, d.h., die Aktivitäten der Administratoren müssen ebenfalls aufgezeichnet werden. Für priviligierte Administratoren, wie z.B. den Operator, dürfen keine Möglichkeiten zur Manipulation der Protokolldaten existieren. Es muss immer nachweisbar sein, wann auf die Protokolldaten zugegriffen wurde. Dies ist im Hinblick auf den weiter unten zitierten § 31 des Bundesdatenschutzgesetzes (BDSG) besonders wichtig.

Neben den allgemeinen Bestimmungen des BDSG müssen die folgenden Paragraphen von Mitarbeitern, die mit der Auswertung der Protokolldaten eines Firewall-Systems beauftragt sind, berücksichtigt werden:

§ 5 Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

§ 31 Besondere Zweckbindung

Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

neuKap13.fm Seite 376 Freitag, 18. Oktober 2002 3:52 15

Die Verpflichtung auf das Datengeheimnis trifft auf jeden zu, der im Anwendungsbereich des BDSG zu tun hat, und ist in der Informationstechnik eine Selbstverständlichkeit. In der Literatur wird auch von einer »leeren Förmlichkeit« gesprochen.

Dennoch kann es in der Praxis sinnvoll sein, den mit der Protokollauswertung beschäftigten Mitarbeitern die Bedeutung des Datenschutzes durch ausdrückliche Verpflichtung auf ein »Datengeheimnis« vor Augen zu halten. Insofern sollte von den entsprechenden Mitarbeitern die Unterzeichnung einer Verpflichtungserklärung verlangt werden, wenn sie nicht schon ausdrücklich im Arbeitsvertrag enthalten ist.

Es ist zu empfehlen, mit dem Personal- oder Betriebsrat eine Betriebsvereinbarung über die Auswertung der Protokolldaten des Firewall-Systems auszuarbeiten, sofern nicht schon eine für die allgemeinen Protokolldaten existiert. Durch eine Betriebsvereinbarung wird sichergestellt, dass das Instrument der Protokollierung nicht zweckentfremdet wird, etwa für die Durchführung einer Verhaltens- oder Leistungskontrolle der Mitarbeiter. In dieser Vereinbarung sollten die zulässigen Auswertungen der Protokolldateien (wer darf diese wie, mit welchen Hilfsmitteln und zu welchem Zweck auswerten) sowie die Art ihrer Nutzung festgelegt werden.

13.2 Aktive WWW-Inhalte – Java und seine Verwandten

Bei der Kommunikation über Firewall-Systeme sind einige weitere innovative IT-Client-Konzepte relevant. In diesem Kapitel werden Java, Javascript und ActiveX diskutiert. Die Unterschiede in den Konzepten und die Sicherheitsproblematik werden allerdings vereinfacht dargestellt.

Grundlage

Als vor wenigen Jahren das World Wide Web eingeführt wurde, bot es erstmals die Gelegenheit, Texte, Grafiken und Verweise zu verwandten Themen in der Form von HTML-Dokumenten darzustellen. Durch die rasante Entwicklung des Internets waren der Umsetzung von kreativen Ideen durch die textorientierten HTML-Dokumente sehr bald Grenzen gesetzt. Zunächst entwickelte man unterschiedliche Zusatzmodule, so genannte PlugIns. Diese sind für jeden Browsertyp speziell angepasst und ermöglichen unter anderem die Übertragung von Audio- und Videosequenzen oder die Darstellung von virtuellen, dreidimensionalen Welten (VRML oder Virtual Reality Modelling Language) im Internet. Diese Lösungen sind wegen der Vielzahl von Hard- und Software-Systemen auf Dauer aber unbefriedigend. Es fehlte eine Möglichkeit, individuelle Inhalte oder Programme auf dem Rechnersystem des Anwenders zu transportieren, ohne seine jeweilige Hard- oder Software-Konfiguration berücksichtigen zu müssen.

neuKap13.fm Seite 377 Freitag, 18. Oktober 2002 3:52 15

Abb. 13.1: Beispiel eines HTML-Dokuments

Das Common Gateway Interface (CGI)

Das CGI oder Common Gateway Interface ist ein erster Schritt bei der Umsetzung interaktiver Funktionen. Dieses Verfahren bildet eine Schnittstelle, auf deren Funktionen beliebige Programme in den unterschiedlichsten Programmiersprachen zugreifen können. Diese Programme werden durch das Aufrufen einer URL oder von Hyperlinks vom Anwender auf dem eigenen Rechnersystem aktiviert und laufen auf dem jeweiligen WWW-Server ab. Dieses Verfahren wird vor allem bei Durchsuchen umfangreicher Datenbanken, der Abspeicherung von Kundeninformationen oder der Auswertung von grafischen Menüs benutzt. Die Anwenderinformationen werden z. B. durch spezielle Eingabefelder innerhalb eines HTML-Dokumentes erfasst, die vom Anwender ausgefüllt werden müssen, oder die Koordinaten eines Mausklicks werden vom Rechnersystem des Anwenders an das CGI-Programm übertragen. Die Ergebnisse werden nach der Verarbeitung wieder zum Anwender übertragen.

neuKap13.fm Seite 378 Freitag, 18. Oktober 2002 3:52 15

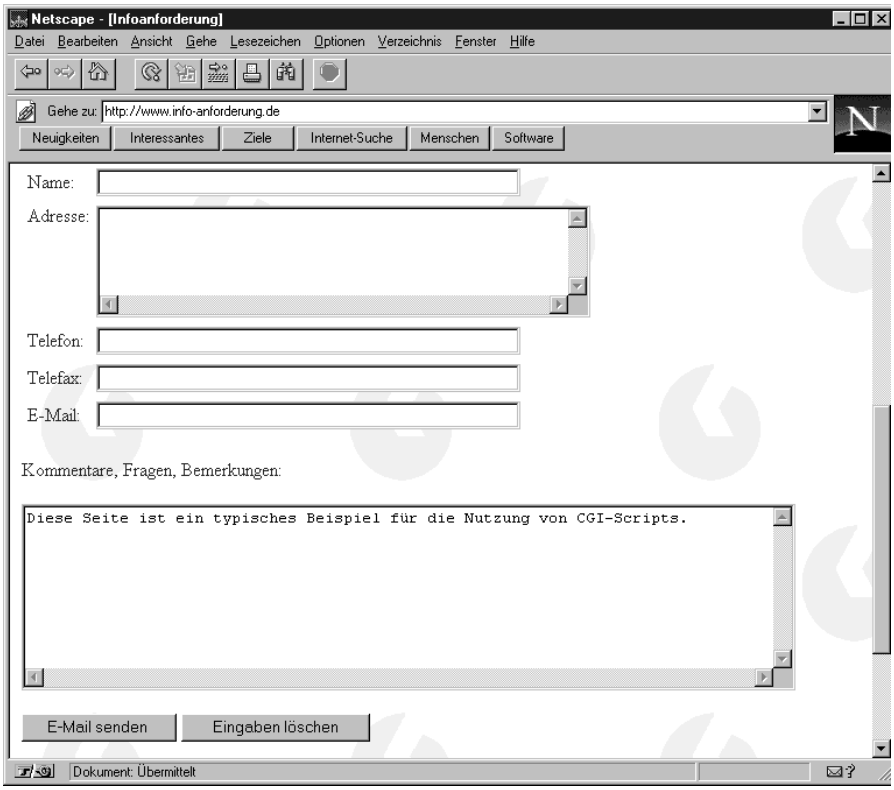


Abb. 13.2: Eingabefelder zur Erfassung von Benutzerdaten

Die Nachteile dieses Verfahrens sind offensichtlich:

- Sämtliche Daten werden vom Rechnersystem des Anwenders zum Server übertragen, dort verarbeitet, und die Ergebnisse werden anschließend wieder zum Anwender zurückgeschickt. Damit wird einem Angreifer die Möglichkeit angeboten, die Informationen auf dem Weg durch das Netz abzuhören oder zu manipulieren.
- CGI-Anwendungen werden auf dem jeweiligen Server ausgeführt und benötigen für ihre Ausführung Systemressourcen. Dies stellt ein potenzielles Sicherheitsrisiko dar und verlangt vom Betreiber des Servers einen entsprechenden Aufwand an Sicherungsmaßnahmen.
- Die Datenübertragung sämtlicher Informationen zwischen Rechnersystem und Server beansprucht die Infrastruktur des Netzwerks. Die Folgen bei intensiver Nutzung sind Netzüberlastungen und Wartezeiten, die den Server zum informationstechnischen »Flaschenhals« machen. Dies macht sich vor allem bei der Programmierung grafischer Applikationen oder Animationen bemerkbar, deren Datenmengen sich regelrecht durch das Netz quälen müssen.

neuKap13.fm Seite 379 Freitag, 18. Oktober 2002 3:52 15

- Bei komplexen Rechenvorgängen werden die Rechnersysteme der Anwender gar nicht oder nur in geringem Maße genutzt. Dieses System erinnert an ehemalige Großrechenanlagen, die über »dumme« Terminals, also Rechnersysteme mit geringer oder gar keiner Rechenleistung, bedient wurden. Da heutige Rechnersysteme aber über eigene »Intelligenz« verfügen, deren Leistung durch die technische Entwicklung ständig steigt, bedeuten CGI-Anwendungen im Grunde genommen einen technologischen Rückschritt.

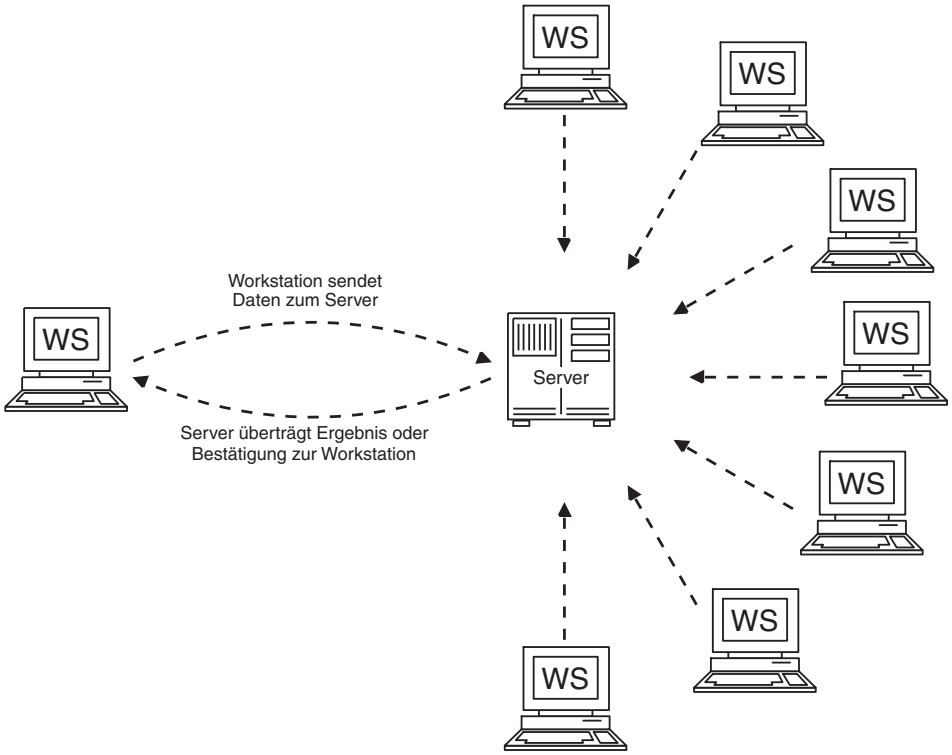


Abb. 13.3: Der Nachteil von CGI, die hohe Serverbelastung

Active Server Pages (ASP)

Um einen Teil der Probleme mit CGI zu beheben, ist Microsoft den Weg hin zu einem proprietären Standard gegangen, den Active Server Pages. ASP-Seiten sind nach wie vor server-basiert, d.h., es müssen dort die entsprechenden Ressourcen zur Verfügung stehen.

ASP hat aber gegenüber CGI einige Vorteile. So wird nicht für jeden Aufruf eines Skipts durch den Client ein eigener Prozess gestartet. Der Start eines Prozesses verschlingt durch die Anmeldung am Betriebssystem, die Erstellung eines Ein-

neuKap13.fm Seite 380 Freitag, 18. Oktober 2002 3:52 15

trages in der Prozessliste, die Zuweisung von Speicher etc. viele Ressourcen. Diese stehen bei den meisten CGI-Anwendungen im krassen Gegensatz zu den wenigen Befehlen, mit denen die Benutzeranfrage abgehandelt wird. ASP handelt die Client-Anfragen im normalen Prozesskontext des Servers ab, beispielsweise durch Threads.

Zusätzliche Funktionen zum Session-Management gleichen die Nachteile des HTTP-Protokolls (und auch von CGI) aus, die beide zustandslos sind. Komplexe Zugriffs auf Datenbanken lassen sich aber nur mit einer Zustandsmaschine effizient durchführen.

Die Programmierschnittstelle von ASP ist recht flexibel, es werden die Sprachen Perl, VBScript, JavaScript und ActiveX-Script unterstützt.

Trotz dieser Vorteile ist der Einsatz von ASP zurzeit im Wesentlichen auf eine reine Microsoft-Umgebung mit dem Internet Information Server beschränkt, einzig der Web-Server WebSite Pro von O'Reilly erweitert das Produktspektrum auf einen unabhängigen Anbieter. Trotzdem ist ASP im Internet recht verbreitet, die ASP-Seiten sind im Browser an der Dateiendung *.asp zu erkennen (im Gegensatz zu dem gewöhnlichen HTML-Seiten mit den Endungen *.html oder *.htm).

13.2.1 Java

Als Lösung aller Probleme bot sich die von der Firma Sun entwickelte Programmiersprache Java an. Ursprünglich wurde Java entwickelt, um eine einfache Programmierung von elektronischen Haushaltsgeräten, wie z. B. Videogeräten, Stereoanlagen, Mikrowellen usw., zu ermöglichen. Doch man erkannte sehr schnell, dass dieses Prinzip weitaus zukunftsträchtiger war. Java ermöglicht es, Programme und Daten über das Internet zu jedem angeschlossenen Rechnersystem zu transportieren und dort unabhängig von der verwendeten Hardware-Plattform lokal ablaufen zu lassen. Damit wird die Arbeit im Gegensatz zu CGI oder ASP vom Rechnersystem des Anwenders durchgeführt.

Java besteht aus drei Komponenten: der eigentlichen Programmiersprache, einem Compiler und dem Laufzeitsystem. Diese Aufteilung hat sich bereits bei vielen anderen Computersprachen bewährt, und so ist es kein Wunder, dass sich auch Java eng an bereits vorhandene Konzepte angelehnt hat. Im Gegensatz zu C++, an deren Sprachsyntax sich Java orientiert, ist es weniger komplex und einfacher aufgebaut. Durch den objektorientierten Aufbau und die Verwendung von Klassen oder Objekttypen ist Java ein leistungsstarkes Programmierwerkzeug, das auf den modernen Grundlagen der Software-Entwicklung aufbaut.

Ein Java-Programm, auch Applet genannt, wird ähnlich einem CGI-Programm durch einen URL oder Hyperlink innerhalb eines HTML-Dokumentes aktiviert. Doch im Gegensatz zu CGI werden die Daten nicht zum Server übertragen und dort ausgewertet, sondern das Programm, das die Berechnungen ausführen soll,

neuKap13.fm Seite 381 Freitag, 18. Oktober 2002 3:52 15

wird als Bytecode vom WWW-Server auf das Rechnersystem des Anwenders übertragen. Der Browser, der über die entsprechende Laufzeitumgebung verfügen muss, führt dieses Programm anschließend auf dem lokalen Rechnersystem aus. Dadurch können aufwendige Programmierungen realisiert werden, die dann spontan und dynamisch genutzt werden können. Die Software-Verteilung ist in der Anwendung realisiert, Updates werden nur noch zentral auf den WWW-Servern notwendig, usw.

Um Java-Programme auf jeder beliebigen Plattform abarbeiten zu können, wurde die so genannte Java Virtual Machine (JVM oder auch VM) definiert. Diese kann man sich wie einen virtuellen Prozessor vorstellen, der Maschinenbefehle in einer eigens für ihn definierten Sprache ausführt. In der Praxis wird die VM durch einen an die jeweilige Rechnerarchitektur angepassten Interpreter realisiert.

Trotz aller Euphorie haben sich im Laufe der Entwicklung immer wieder Sicherheitsmängel im Konzept und den verschiedenen Implementierungen der VM herausgestellt. Das Sicherheitskonzept von Java beruht auf der Annahme, dass ein Applet in einer geschlossenen Umgebung ohne Verbindung zu den Ressourcen des Rechnersystems abläuft. Die Sicherheitsmechanismen bestehen aus vier Bestandteilen, die ein so genanntes Sandbox-Modell bilden.

- Die eigentliche Sprache der VM sollte von Anfang an sicher und robust gestaltet sein. Codemodifikationen und Direktzugriffe auf Speicherinhalte bzw. ein direktes Ansprechen der Ressourcen eines Rechnersystems (z. B. Lesen und Schreiben auf Festplatte) sind per Definition nicht erlaubt.
- Bevor das Laufzeitsystem ein Java-Programm auf einem Rechnersystem ausführt, überprüft ein so genannter Byte Code Verifyer den empfangenen Code auf die Gültigkeit von Zuweisungen, korrekte Parameter innerhalb der Bytecode-Instruktionen, die Zulässigkeit von Registerzugriffen und die Konsistenz der Speicher (Stacks).

Java unterscheidet streng zwischen lokalem und externem Code. Ein lokaler Code, dazu gehören bei der Einrichtung installierte Klassen oder vom Anwender erstellte Applikationen, wird vom Laufzeitsystem als vertrauenswürdig angesehen und ohne Zugriffsbeschränkung ausgeführt. Ein externer Code, also ein vom Netz empfangener und durch den Byte Code Verifyer überprüfter Code, wird als solcher markiert und durch den so genannten Class Loader installiert. Dieser sorgt dafür, dass sich ein externer Code nicht mit einem lokalen oder bereits vorher installiertem externem Code verbinden kann. Zur Unterscheidung und Speicherung der Klassen benutzt Java die so genannten Name Spaces. Jeder externe Code wird in einem eigenen Name Space aufbewahrt und isoliert. Damit wird verhindert, dass ein neu empfangener, externer Code einem bereits existierenden Code überschreibt bzw. ergänzt.

neuKap13.fm Seite 382 Freitag, 18. Oktober 2002 3:52 15

- Der Security Manager ist ein Teil des Laufzeitsystems und kontrolliert alle externen Zugriffe von Codes auf die Systemressourcen und verhindert unzulässige Zugriffe.

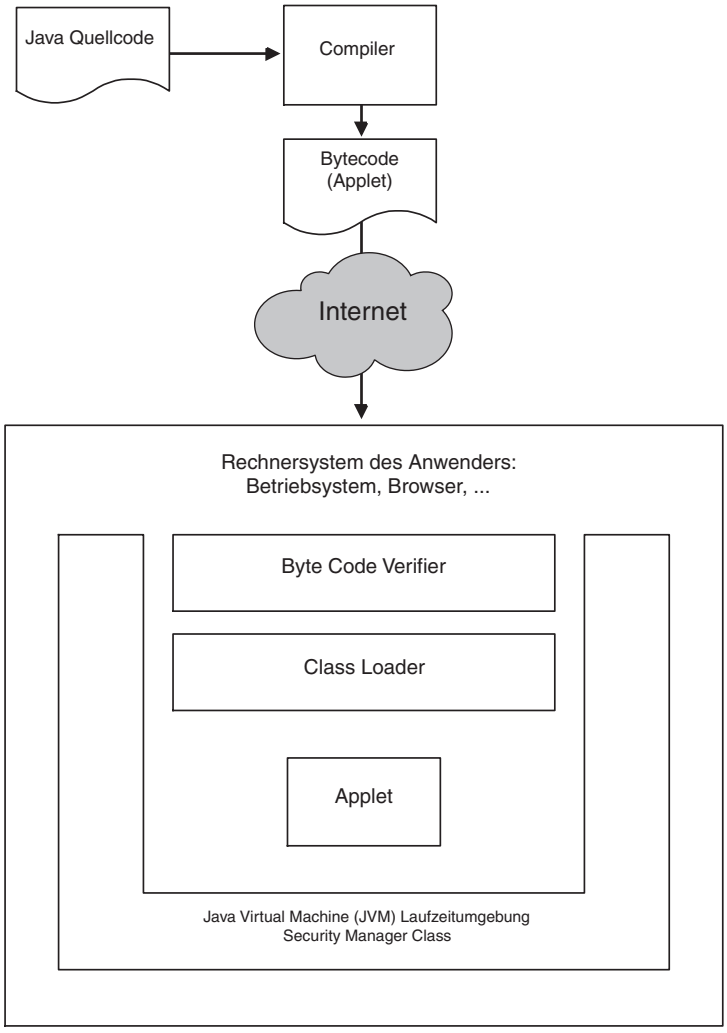


Abb. 13.4: Das Sandbox-Modell der Java Sicherheitsstrukturen

Im Prinzip hört sich das Konzept gut durchdacht an, doch bei näherer Betrachtung fallen einem mehrere Schwachpunkte auf:

- Der übertragene Bytecode ist während der Übertragung im Netz der Gefahr von Angriffen ausgesetzt und damit nicht vor Modifikationen oder Manipulationen geschützt.

neuKap13.fm Seite 383 Freitag, 18. Oktober 2002 3:52 15

- Die logische Trennung der unterschiedlichen Sicherheitsmechanismen stellt für einen Angreifer keine unabhängigen Hürden dar, die er erst nach und nach überwinden muss, sondern bauen aufeinander auf. Nur wenn alle vier Mechanismen ineinander greifen und fehlerfrei arbeiten, ist ein gewisses Maß an Sicherheit gewährleistet.
- Die Verantwortung für die einzelnen Sicherheitsmechanismen liegt bei unterschiedlichen Herstellern. Dadurch hängt es von der einzelnen firmenpolitischen Entscheidung ab, wie die Implementierungen der Sicherheitsmechanismen durchgesetzt werden.
- In Java fehlt jede Möglichkeit der Beweissicherung.
- Der Security Manager muss vom Laufzeitsystem gestartet werden. Falls durch einen Installationsfehler oder eine Manipulation dieses nicht erfolgt, werden alle Zugriffe erlaubt, und einem Angreifer stehen alle Möglichkeiten zur Verfügung.

Über die Umsetzung der Sicherheitsmechanismen wurde bereits viel diskutiert. Weltweit beschäftigen sich unzählige Institutionen und Einzelpersonen mit der Analyse dieser Mechanismen. Im Internet werden regelmäßig neue Fehlerlisten und Sicherheitslücken veröffentlicht. Meistens beruhen diese Sicherheitslücken auf fehlerhafter Implementierung durch den Hersteller. Eine Reihe dieser Lücken wurde zwar bereits durch neue Versionen oder Reparaturen (Patches) der Software ersetzt, doch es besteht eine hohe Wahrscheinlichkeit, dass noch weitere Sicherheitslücken existieren, die erst nach und nach auftauchen werden.

Eine Weiterentwicklung der Java-Applets sind die so genannten Java-Beans, neuenglisch auch JavaBeans genannt. Im Gegensatz zu einem Java-Applet, das oft ein recht großes Gebilde ist und zudem immer aus einem Browser heraus gestartet wird, sind die JavaBeans kompakte, wiederverwendbare Minimodule, die von einem oder mehreren Java-Applets, aber auch von Applikationen genutzt werden können. Trotz der stärkeren Modularisierung bleiben den JavaBeans alle Vorteile der virtuellen Maschine und der Sandbox erhalten.

Bewertung

Aus heutiger Sicht erscheint es sinnvoll, die Vorteile von Java bei solchen Intranet-Anwendungen zu nutzen, bei denen auf die Java Applets Einfluss genommen werden kann. Bei der Kommunikation mit Rechner-Systemen aus dem unsicheren Netz (z. B. Internet) ist immer die Gefahr eines Schadens gegeben. Java sollte daher bei diesen Anwendungen nicht leichtfertig genutzt werden. Da bei Recherchen im Internet auf das mittlerweile weit verbreitete Java kaum noch komplett verzichtet werden kann, dürfen diese Arbeiten keinesfalls von einem Rechner durchgeführt werden, der sensible Daten enthält oder der sich in einem sicherheitsrelevanten Netz befindet. Darüber hinaus ist der Einsatz eines Filters für Java-Applets am Zugang zum Internet unerlässlich.

neuKap13.fm Seite 384 Freitag, 18. Oktober 2002 3:52 15

Die zukünftige Entwicklung bei Java sollte dahingehend beobachtet werden, ob die aufgezeigten Sicherheitsmängel behoben werden und einem uneingeschränkten Einsatz von Java damit nichts mehr im Wege steht.

13.2.2 JavaScript

JavaScript ist eine von Netscape entwickelte Scriptsprache, die zunächst nur für die von Netscape vertriebenen Produkte verfügbar war. Mittlerweile hat JavaScript allerdings eine sehr große Verbreitung erfahren, sodass es auch von Microsoft in dessen Internet Explorer integriert wurde (dort allerdings unter der Bezeichnung Active Scripting).

JavaScript ist in zwei Varianten erhältlich, als server- und als client-basierte Version. Die server-basierte Version entspricht in ihrer Funktionalität den ASP-Seiten von Microsoft, die gesamte Verarbeitung findet auf dem Server statt. Die client-basierte Version jedoch ist unter Sicherheitsaspekten sehr problematisch, da hier immer wieder Sicherheitslücken entdeckt werden.

Javascript in der Client-Version ist eine klassische Scriptsprache, die von einem Interpreter auf dem Client ausgeführt wird, und zwar ohne die schützende Sandbox von Java. Die Javascript-Statements werden ganz zwanglos in die HTML-Seiten auf dem Web-Server eingestreut und beim Ansehen der Seite automatisch auf den Client geladen und dort ausgeführt.

Da die gesamte Sicherheit nur aus einer einzigen Stufe besteht (dem Interpreter), ist bei JavaScript besondere Vorsicht angebracht. Jeder Fehler im Interpreter kann von Hackern durch entsprechend ausgestaltete Webseiten ohne Umwege zu einem Angriff missbraucht werden. Viele JavaScript-Angriffe wurden bisher bekannt. Sie reichen vom Lesen bestimmter Dateien auf der Festplatte bis hin zur Ausführung beliebigen Programmcodes auf dem Client.

Deshalb gilt ganz allgemein: Finger weg von JavaScript! Die Defaulteinstellung in jedem Browser sollte die Deaktivierung von JavaScript bzw. Active Scripting sein.

Leider hat JavaScript eine Verbreitung erreicht, die die aller vergleichbaren Produkte wie Java oder ActiveX bei weitem übertrifft. Das liegt vor allem an der einfachen Art der Programmierung, die selbst den ungeübten Laien in die Lage versetzt, effektvolle bunte Fenster zu programmieren. Allerdings gibt es auch durchaus ernsthafte Webseiten (wie Telefonverzeichnisse und andere Nachschlagewerke), die auf JavaScript basieren. Hier gibt es nur zwei Alternativen. Entweder wird JavaScript punktuell beim Zugriff auf solche Webangebote aktiviert und danach sofort wieder deaktiviert, oder ein Filter im Zugang zum Internet sorgt für die Freigabe einiger weniger JavaScript-Programme.

neuKap13.fm Seite 385 Freitag, 18. Oktober 2002 3:52 15

13.2.3 ActiveX

Neben Java und JavaScript hat sich noch das von Microsoft propagierte ActiveX auf dem Markt etabliert. Dieses Konzept ist im Gegensatz zu Java kein abgegrenztes System, sondern ein integraler Bestandteil des Betriebssystems und der verwendeten Programme.

Ein Programm, oder ActiveX-Control genannt, lässt sich in jeder beliebigen Programmiersprache schreiben, solange es den Spezifikationen der ActiveX-Schnittstelle genügt. Die Aktivierung des jeweiligen Programms erfolgt wie bei Java durch den Aufruf einer URL oder von Hyperlinks aus dem Browser des Anwenders. Zwar war anfangs nur der Microsoft Internet Explorer in der Lage, diese Controls zu verarbeiten, doch sind mittlerweile unterschiedliche Versionen oder Zusätze (PlugIns) für eine Vielzahl anderer Produkte erschienen.

Die Firmenpolitik von Microsoft möchte einem Programmierer von ActiveX-Controls den Zugriff auf sämtliche Systemressourcen ermöglichen. Deshalb besitzt er die gleichen Rechte wie der gerade angemeldete Anwender. Kurz gesagt, es existiert keinerlei Sicherheitsarchitektur für ein Rechnersystem mit ActiveX-Anwendungen.

Als Ersatz für das Fehlen jeglicher Sicherheitsstruktur gibt Microsoft seine eigens entwickelte »Authenticode«-Technologie ein. Dabei handelt es sich um ein Verfahren, um die Herkunft der verwendeten ActiveX-Controls nachvollziehen zu können, ähnlich der digitalen Signatur (siehe Kapitel 7 *Firewall-Systeme und Verschlüsselung*). Dabei wird allerdings stillschweigend vorausgesetzt, dass der Anwender ohne weiteres zwischen seriösen und unredlichen Anbietern unterscheiden kann.

Um sein Control signieren zu können, beantragt ein Anbieter gegen eine geringe Gebühr ein Zertifikat und bekommt dieses und einen privaten Schlüssel zugewiesen. Der Anbieter muss dafür lediglich erklären, dass er nicht wissentlich oder fahrlässig bösartige Codes oder Viren herzustellen beabsichtigt.

Gegen ActiveX ist eine Fülle von Angriffen bekannt, die meist versuchen, das »Authenticode«-Verfahren auszuhebeln. So wurde beispielsweise auf einer präparierten Webseite ein Excel-Sheet versteckt, das dann seinerseits das »todbringende« ActiveX-Programm startete. Da Excel ein lokales Programm mit der höchsten Sicherheitsstufe ist, wurde die Sicherheitsüberprüfung von Microsoft anstandslos passiert.

Das Gefahrenpotenzial bei ActiveX ist bedeutend höher anzusetzen als bei Java oder auch JavaScript. Das zeigt sich an der großen Zahl von Angriffen, die nahezu wöchentlich entdeckt werden und jeweils einen oder mehrere Hotfixes von Microsoft zur Folge haben. Leider setzt Microsoft voll auf ActiveX, sodass z. B. Software-Updates über das Internet ohne ActiveX unmöglich sind.

neuKap13.fm Seite 386 Freitag, 18. Oktober 2002 3:52 15

Abb. 13.5: Das »Authenticode«-Zertifikat von Microsoft

Der Einsatz von Active-X-Technologien ist auf wirtschaftlich genutzten Systemen in öffentlichen Netzen wie dem Internet nicht anzuraten. Beim Aufbau eines Intranet sollte dieses System aber auch nur dann verwendet werden, wenn es durch zusätzliche Sicherheitsmaßnahmen geschützt wird.

Es wird sich in der Zukunft zeigen, inwiefern die »Authenticode«-Technologie im Rahmen des Signatur-Gesetzes verwendet werden kann, um den Firmen, die über ActiveX ihre Software verteilen, eine verbindliche Aussage über die Qualität der zur Verfügung gestellten Software zu ermöglichen. Dabei spielen vor allem Haftungsfragen eine Rolle. Wenn dieses Problem für alle Seiten zufriedenstellend gelöst werden kann, wäre es durchaus denkbar, ActiveX in Verbindung mit »Authenticode«-Technologie zu nutzen, da dann für den Anwender die Möglichkeit besteht, bei fehlerhafter oder virenverseuchter Software auf Schadensersatz zu klagen.

13.3 Firewall-Systeme zur Risikominimierung

Ein Firewall-System ist kein Selbstzweck. Mithilfe eines Firewall-Systems kann das Risiko bei der Ankopplung an unsichere Netze wie das Internet reduziert werden. In diesem Kapitel werden die Kosten eines Firewall-Systems aus unterschiedlichen Blickwinkeln betrachtet. Da ein Firewall-System eine Investition für die Zukunft ist, sollten die Kosten-Nutzen-Aspekte schon bei der Planung besonders berücksichtigt werden.

neuKap13.fm Seite 387 Freitag, 18. Oktober 2002 3:52 15

13.3.1 Total Cost of Ownership

Im Folgenden soll abgeschätzt werden, wie groß der Aufwand ist, ein Firewall-System anzuschaffen und zu betreiben.

Der Aufwand für ein Firewall-System kann unter dem Gesichtspunkt des Aufwandes in drei Phasen unterteilt werden.

- Beschaffungsphase eines Firewall-Systems
- Installationsphase eines Firewall-Systems
- Aufrechterhaltung des Betriebs eines Firewall-Systems

Die Aufwendungen, die in diesem Abschnitt benannt werden, sind reale Aufwendungen, die unabhängig vom jeweiligen Zeitpunkt erbracht werden müssen. Aufwand wird auf Tage gerundet, wobei davon ausgegangen wird, dass sechs Stunden Aufwand einen Arbeitstag ausmachen. Bei den angegebenen Aufwendungen wird davon ausgegangen, dass über das Firewall-System potenziell 1000 Mitarbeiter der Organisation kommunizieren dürfen.

Die Personalkosten werden mit EUR 750,- pro Tag veranschlagt. Falls die angegebenen Leistungen von Fachfirmen durchgeführt werden, muss wahrscheinlich mit einem höheren Kostenbetrag gerechnet werden.

13.3.2 Beschaffungsphase eines Firewall-Systems

In der Beschaffungsphase muss von der Organisation eine Firewall-Sicherheitspolitik festgelegt werden, die als Grundlage für den Betrieb des Firewall-Systems dient. Hier ist besonders wichtig, den Schutzbedarf des zu schützenden Netzes mit den Rechnersystemen zu analysieren, damit eine richtige Sicherheitsanforderung festgelegt werden kann.

Mit den definierten Randbedingungen der Sicherheitspolitik der Organisation kann dann die Produktauswahl eines Firewall-Systems beginnen, z. B. durch Einholen von Angeboten, Testinstallationen, Referenzbewertung etc. Dabei muss im Vorfeld festgelegt werden, nach welchen Kriterien ein Produkt bewertet werden soll.

Wichtig in dieser Phase ist, dass auch infrastrukturelle, personelle und organisatorische Sicherheitsmaßnahmen vorbereitet werden, damit die nächste Phase eingeleitet werden kann (siehe Kapitel 11 *Ein Firewall-System ist mehr als ein Produkt*).

Aufwand für die Beschaffungsphase

Falls die Organisation noch keine generelle Sicherheitspolitik erarbeitet hat und diese im Rahmen der Firewall-Beschaffung erstellt werden muss, ist der Aufwand in der Beschaffungsphase zu berücksichtigen. Die Erstellung einer Sicherheitspolitik kann je nach Größe der Organisation und je nach Schutzbedarfs zwischen zwei Wochen und drei Monaten liegen.

neuKap13.fm Seite 388 Freitag, 18. Oktober 2002 3:52 15

Für die Auswahl eines Firewall-Produktes ist der Aufwand abhängig vom Produktauswahlverfahren sehr unterschiedlich, je nachdem, ob z. B. nur mithilfe von Prospekten ausgewählt wird oder Testinstallationen mehrerer Firewall-Systeme mit Aufbau eines Testsystems stattfinden sollen. Der Aufwand liegt in der Regel zwischen zwei Wochen und drei Monaten.

Die Definition und Vorbereitung der infrastrukturellen, personellen und organisatorischen Sicherheitsmaßnahmen kann zwischen einer Woche und vier Wochen liegen.

Die Anschaffungskosten für ein Firewall-Produkt liegen zwischen 5 000 EUR und 75 000 EUR, abhängig vom Maß an Sicherheit/Vertrauenswürdigkeit, das es erbringen kann, und seiner Leistungsfähigkeit.

Installationsphase eines Firewall-Systems

In der Installationsphase gliedern sich die Aufwendungen für ein Firewall-System in mehrere Unterpunkte.

- *Installation des Firewall-Systems:* Diese Phase umfasst alle infrastrukturellen Sicherheitsmaßnahmen, die zum sicheren Betrieb eines Firewall-Systems notwendig sind (siehe Kapitel 11 *Ein Firewall-System ist mehr als ein Produkt*).
- *Inbetriebnahme des Firewall-Systems:* In dieser Phase ist es sinnvoll, entsprechend den Vorgaben der Sicherheitspolitik Benutzerprofile für bestimmte Mitarbeitergruppen zu definieren, damit die Eingaben des Regelwerkes später mithilfe dieser Benutzerprofile schneller erfolgen können. Nach Formulierung dieser Profile werden die Benutzer, die über das Firewall-System kommunizieren dürfen, mit ihren Rechten in das Security Management eingetragen.
- *Sonstige Sicherheitsmaßnahmen:* In der Installationsphase ist es wichtig, dass weitere Sicherheitsmaßnahmen wie z. B. die Schulung der Benutzer durchgeführt werden, damit diese den richtigen Umgang mit dem Firewall-System lernen und dadurch unnötige Schwierigkeiten beim Betrieb vermieden werden, Organisationsanweisungen schreiben, usw. (siehe Kapitel 11 *Ein Firewall-System ist mehr als ein Produkt*).

Die folgenden Tabellen sollen zeigen, welche zeitlichen und finanziellen Aufwendungen für die Beschaffungs- und Installationsphase einzuplanen sind.

Beschaffungsphase	Zeitaufwand	minimale Kosten	maximale Kosten
Sicherheitspolitik	zwei Wochen bis drei Monate	EUR 7 500	EUR 45 000
Auswahl eines Produktes	zwei Wochen bis drei Monate	EUR 7 500	EUR 45 000

Tabelle 13.1: Aufwand und Kosten für die Beschaffungsphase

neuKap13.fm Seite 389 Freitag, 18. Oktober 2002 3:52 15

Beschaffungsphase	Zeitaufwand	minimale Kosten	maximale Kosten
weitere Sicherheitsmaßnahmen	eine bis vier Wochen	EUR 3 750	EUR 15 000
Produktkosten		EUR 5 000	EUR 75 000

Tabelle 13.1: Aufwand und Kosten für die Beschaffungsphase (Forts.)

Installationsphase	Zeitaufwand	minimale Kosten	maximale Kosten
Installation des Firewall-Systems	2 bis 5 Tage	EUR 1 500	EUR 3 750
Inbetriebnahme des Firewall-Systems	3 bis 10 Tage	EUR 2 250	EUR 7 500
Sonstige Sicherheitsmaßnahmen	3 Wochen bis 3 Monate	EUR 11 250	EUR 45 000

Tabelle 13.2: Aufwand und Kosten während der Installationsphase

Anschaffungskosten	minimale Kosten	maximale Kosten
Summe	EUR 38 750	EUR 236 250

Tabelle 13.3: Kosten der Beschaffungsphase und Installationsphase

13.3.3 Aufrechterhaltung des Betriebs eines Firewall-Systems

Der Aufwand für die Aufrechterhaltung des Firewall-Systems kann unter verschiedenen Gesichtspunkten betrachtet werden.

Rechteverwaltung

Ein Firewall-System ist prinzipiell so aufgebaut, dass es nach Eintrag sämtlicher Rechte vollkommen selbstständig und ohne aktive Eingriffe eines Administrators betrieben werden kann.

Aus unterschiedlichen Gründen kann jedoch ein personeller Eingriff notwendig werden, und zwar zur Einrichtung neuer Mitarbeiter bzw. zur Änderung der Rechte schon eingetragener Mitarbeiter. Je nach Anzahl und Änderungen der definierten Benutzerprofile ergibt sich ein sehr unterschiedlicher personeller Aufwand des Administrators für diese Aufgaben.

Rechenbeispiel: Für die Eintragung eines neuen Mitarbeiters oder für die Veränderung der Rechte eines schon eingetragenen Mitarbeiters benötigt der Administrator im Schnitt zehn Minuten. Die Veränderung der Mitarbeiterzahl in einer Organisation, die über das Firewall-System kommunizieren darf, wird in unserem Beispiel mit 5 % im Monat veranschlagt.

neuKap13.fm Seite 390 Freitag, 18. Oktober 2002 3:52 15

Das bedeutet bei 1000 Mitarbeitern, die potenziell über das Firewall-System kommunizieren dürfen, dass 50 Veränderungen im Monat stattfinden, d.h., für die Rechteverwaltung ist ein Zeitaufwand von 500 Minuten im Monat, also ca. neun Stunden im Monat bzw. 18 Tage im Jahr notwendig.

Analyse der Logbuchdaten

Für die Analyse der Logbuchdaten, die vom Firewall-System generiert werden, ist ein Aufwand für den Administrator einzukalkulieren. Auch hier kann der personelle Aufwand sehr unterschiedlich ausfallen. Bei Firewall-Systemen, die eine automatische Vorauswertung durchführen, ist der Zeitaufwand für den Administrator weitaus geringer als bei Firewall-Systemen, bei denen der Administrator die Logbuchdaten selbst auswerten muss.

Rechenbeispiel: Für die Analyse der Logbuchdaten werden in der Woche drei Stunden veranschlagt. Dies bedeutet einen Aufwand von zwei Tagen im Monat bzw. 24 Tagen im Jahr.

Einrichtung neuer Dienste

Da die TCP/IP-Technologie einer starken Dynamik und permanenten Veränderung unterworfen ist, muss davon ausgegangen werden, dass das Firewall-System im Abstand von drei bis sechs Monaten ein Update durchführen muss, um den neuen Anforderungen gerecht zu werden. Diese Updates erfordern ebenfalls einen bestimmten Zeitaufwand, da sie getestet werden müssen, um garantieren zu können, dass der Betrieb des Firewall-Systems weiterhin gesichert möglich ist.

Rechenbeispiel: Für diese Arbeit müssen pro Update zwei Tage vorgesehen werden, das bedeutet im Schnitt sechs Tage im Jahr.

Genereller administrativer Aufwand für das Firewall-System

Für den sicheren Betrieb des Firewall-Systems müssen Backups des aktuellen Regelwerks und der Logbuchdaten, Löschen der Protokolldaten auf dem Security Management etc. durchgeführt werden.

Rechenbeispiele: Für diese generellen Arbeiten muss ein Aufwand von drei Stunden pro Woche d.h., zwei Tagen im Monat bzw. 24 Tagen im Jahr, berücksichtigt werden.

Auswertung der Logbuchdaten auf dem Security Management

Da das Security Management eines Firewall-Systems sehr sicherheitskritisch ist, muss ein Revisor in regelmäßigen Abständen alle Aktionen der Administratoren des Management Systems mithilfe der Logbuchdaten im Security Management überprüfen.

neuKap13.fm Seite 391 Freitag, 18. Oktober 2002 3:52 15

Rechenbeispiel: Für diese Arbeit sollen drei Stunden im Monat berücksichtigt werden, d.h. sechs Tage im Jahr.

Sicherer Betrieb eines Firewall-Systems

Damit mithilfe eines Firewall-Systems ein effektiver Schutz für die Kommunikation zwischen dem unsicheren Netz und dem zu schützenden Netz gewährleistet werden kann, müssen die folgenden Bedingungen erfüllt werden:

- Das Firewall-Konzept muss in das IT-Konzept der Organisation eingebunden werden.
- Der Betrieb des Firewall-Systems muss auf eine umfassende Sicherheitspolitik aufbauen.
- Das Firewall-System muss korrekt installiert sein.
- Das Firewall-System muss korrekt administriert werden.

Aus diesem Grund ist eine regelmäßige Überprüfung der umgesetzten Sicherheitsmaßnahmen notwendig. Hierbei soll festgestellt werden, ob die unterschiedlichen Sicherheitsmaßnahmen richtig eingehalten werden.

Diese Überprüfung muss alle Sicherheitsmaßnahmen einschließen, die für den sicheren Betrieb des Firewall-Systems verantwortlich sind.

- technische Sicherheitsmaßnahmen
  - Durch regelmäßige Tests sollte überprüft werden, ob die in der Sicherheitspolitik festgelegten Regeln korrekt umgesetzt worden sind.
  - Es sollte ein Integrationstest des Firewall-Systems initialisiert werden, der überprüft, ob das Firewall-System und das Regelwerk unversehrt sind.
- infrastrukturelle Sicherheitsmaßnahmen
  - In regelmäßigen Abständen sollte überprüft werden, ob die infrastrukturellen Sicherheitsmaßnahmen (zugangsgesicherter Raum, geschützte Leitungsführung, Dokumentation und Kennzeichnung der Verkabelung des Firewall-Systems usw.) eingehalten werden.
- organisatorische Sicherheitsmaßnahmen
  - In zyklischen Abständen muss überprüft werden, ob neue Verbindungen unter Umgehung des Common Point of Trust (Firewall-System) geschaffen wurden.
  - Die Logbuchdaten müssen regelmäßig überprüft werden, ob z.B. Angriffe stattgefunden haben.
- personelle Sicherheitsmaßnahmen
  - In regelmäßigen Abständen sollten Aktionen eingeleitet werden, die das Sicherheitsbewusstsein erhöhen: Rundschreiben, Schulungen, Informationsveranstaltungen.

neuKap13.fm Seite 392 Freitag, 18. Oktober 2002 3:52 15

Durchzuführende Maßnahme	Aufwand
Technische Sicherheitsmaßnahmen	4 Tage pro Jahr
Infrastrukturelle Sicherheitsmaßnahmen	4 Tage pro Jahr
Organisatorische Sicherheitsmaßnahmen	4 Tage pro Jahr
Personelle Sicherheitmaßnahmen	12 Tage pro Jahr
Zusammenfassung	24 Tage pro Jahr

Tabelle 13.4: Aufwendungen für den sicheren Betrieb eines Firewall-Systems

Durchzuführende Maßnahme	Aufwand
Rechteverwaltung	18 Tage pro Jahr
Analyse der Logbuchdaten	24 Tage pro Jahr
Einrichtung neuer Dienste	6 Tage pro Jahr
Genereller administrativer Aufwand	24 Tage pro Jahr
Auswertung der Logbuchdaten auf dem Security Management	6 Tage pro Jahr
sicherer Betrieb eines Firewall-Systems	24 Tage im Jahr
Zusammenfassung	102 Tage pro Jahr

Tabelle 13.5: Aufwendungen für die Aufrechterhaltung des Betriebs eines Firewall-Systems

Bei der Aufrechterhaltung des Betriebs eines Firewall-Systems, bei dem 1 000 Benutzer unter den beschriebenen Annahmen über das Firewall-System kommunizieren dürfen, ergibt sich ein Kostenaufwand von ca. EUR 76 500 im Jahr. Das sind ca. EUR 76,50 Kosten pro Benutzer im Jahr.

13.3.4 Zusammenfassung der Kosten im Sinne der Total Cost of Ownership

Aufwendungen für ein Firewall-System sind zum einen die Anschaffungskosten, die zwischen EUR 38 750 und EUR 236 250 liegen können, und die Kosten für die Aufrechterhaltung des Betriebs eines Firewall-Systems, die in unserem Rechenbeispiel, bei dem 1000 Benutzer über ein Firewall-System kommunizieren und eine große Anzahl von Veränderungen vorausgesetzt wurden, mit EUR 76 500 im Jahr veranschlagt.

Diese Zahlen hängen sehr stark von der Struktur und der Größe der Organisation ab. Außerdem müssen die folgenden Aspekte berücksichtigt werden:

- welches Firewall-System wird verwendet
- wie gut ist das Firewall-Konzept
- Anzahl der Benutzer, die über das Firewall-System kommunizieren dürfen

neuKap13.fm Seite 393 Freitag, 18. Oktober 2002 3:52 15

- Veränderung der Kommunikationsprofile
- Qualifikation der Administratoren des Security Management
- Betriebszeiten
- weitere Dienste, die zusätzlich angeboten werden
  - Modem Server
  - Intranet Server
  - Internet Server usw.
- Veränderungen der Benutzer
- Veränderung der Netzstruktur
- Tiefe der Auswertung der Logbuchdaten
- verwendetes Authentikationsverfahren
  - S/KEY (es müssen immer wieder neue Passwörter zur Verfügung gestellt werden)
  - Security Token (wird nur einmal eingerichtet)

13.3.5 Kosten-Nutzen-Betrachtung im Hinblick auf die Sicherheit

Am Beispiel einer Bank mit ca. 1.000 Mitarbeitern soll eine Kosten-Nutzen-Betrachtung eines Firewall-Systems durchgeführt werden. Dabei wird angenommen, dass ohne den Einsatz eines Firewall-Systems die Wahrscheinlichkeit eines erfolgreichen Angriffs sehr hoch ist.

Angenommener Profit der Bank: EUR 25.000.000/Jahr

Kosten eines Firewall-Systems

- Anschaffungskosten: EUR 250.000 (1 % vom Profit)
- Betriebskosten: EUR 80.000/Jahr

Beschreibung eines möglichen Angriffs

Eine Bank wird von einem Hacker über das Internet angegriffen. Dieser kopiert sich aus dem zu schützenden Netz der Bank die Namen und Kontostände der 500 wichtigsten Kunden. Diese werden dann im Internet veröffentlicht, Fernsehen und Presse berichten und die Bank erleidet dadurch einen enormen Imageverlust.

Möglicher Schaden durch diesen Angriff

Durch den enormen Imageverlust wechseln sehr viele Kunden zu einer anderen vertrauenswürdigeren Bank, wodurch die angegriffene Bank einen Schaden hat, der wie folgt angenommen wird:

- sofort: EUR 12.500.000 (50 % vom Gewinn)
- mittelfristig: EUR 2.500.000/Jahr

neuKap13.fm Seite 394 Freitag, 18. Oktober 2002 3:52 15

Zusammenfassung

Unter der Voraussetzung, dass der Angriff mithilfe eines Firewall-System verhindert worden und kein Schaden aufgetreten wäre, hätte sich die Investition in ein Firewall-System gelohnt. Mit der Investition von 1 % des Gewinns kann der Bank ein Schaden erspart werden, der sich auf ein Vielfaches der Investition beläuft (in diesem Beispiel das 60fache).

Mit Bekanntwerden des Angriffs werden auch Nachahmungstäter animiert, ebenfalls einen Angriff durchzuführen. Daher steigt das Risiko, erneut Opfer zu werden, und zu den Aufwendungen zur Behebung des Schadens kommen die Aufwendungen für die Anschaffung eines geeigneten Firewall-Systems, um weiteren Angriffen vorzubeugen.

Wahrscheinlichkeit eines bestimmten Profits

Die folgende Abbildung stellt dar, wie das Investment in Sicherheitsmechanismen vom eigenen Schutzbedarf und der Wahrscheinlichkeit, einen bestimmten Profit erreichen zu können, abhängt.

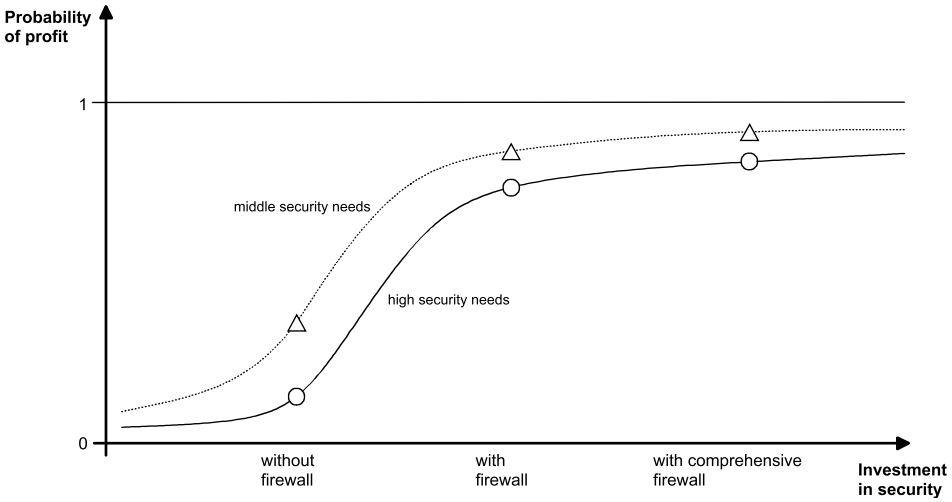


Abb. 13.6: Investment in Sicherheitsmechanismen und die Wahrscheinlichkeit eines bestimmten Profits

Die Abbildung zeigt, dass in Bereichen mit hohem Schutzbedarf (z. B. in Finanzinstituten) höhere Investitionen in Sicherheitsmaßnahmen notwendig sind, um die gleiche Chance auf einen bestimmten Gewinn zu bewahren.

Mit den Investitionen in Sicherheitsmechanismen steigt auch die Wahrscheinlichkeit, einen bestimmten Profit zu erreichen. Das heißt, die Anschaffung von Sicher-

neuKap13.fm Seite 395 Freitag, 18. Oktober 2002 3:52 15

heitssystemen wie Firewall-System, VPN, Intrusion Detection und Viren-Scanner ist ein Investment in die Absicherung des Gewinns. Die Wahrscheinlichkeit auf einen bestimmten Gewinn wird um so höher, je höher die Ausgaben für Sicherheitsmechanismen sind. Der Gewinn kann durch diese Maßnahmen allein aber nie hundertprozentig sicher sein, da immer ein Restrisiko bestehen bleibt.

Die Wahrscheinlichkeit der Gewinnerzielung hängt auch vom Schutzbedarf und damit von der Eintrittswahrscheinlichkeit eines Angriffs ab. Bei höherer Eintrittswahrscheinlichkeit steigt auch der Schutzbedarf vor einem Angriff.

Ist der Schutzbedarf sehr hoch, ist die Wahrscheinlichkeit auf einen Profit geringer als bei niedrigem Schutzbedarf.

Bei Verzicht auf Sicherheitsmechanismen ist dieser Unterschied viel größer als mit hohem Einsatz von Sicherheitsmechanismen, da die Eintrittswahrscheinlichkeit eines Angriffs bei niedrigem Schutzbedarf kleiner ist. Letztendlich ist die Unternehmensleitung für die Sicherheit in einem Unternehmen verantwortlich und muss über das richtige Kosten-Nutzen-Verhältnis entscheiden.

Die Unternehmensleitung ist gut beraten, wenn sie einen gewissen Prozentsatz des Gewinns als Gewinnversicherung für die IT-Sicherheit ausgibt. Dieser Prozentsatz wird bei Unternehmen, deren Image als vertrauenswürdiges Unternehmen die Basis ihres Erfolges darstellt (beispielsweise bei Banken und Versicherungen), höher liegen als bei Unternehmen wie Speditionen und Brauereien, bei denen die IT-Security in bezug auf das Image eine untergeordnete Rolle spielt.

13.3.6 Kosten-Nutzen-Betrachtung im Hinblick auf die Nicht-Realisierung von Kommunikation

Verzichtet ein Anwender aufgrund von Sicherheitsbedenken darauf, das Internet als geschäftliches Kommunikationsmittel zu nutzen, so kann er das darin liegende – oftmals erhebliche – Rationalisierungspotenzial nicht ausschöpfen. Auf längere Sicht droht dadurch ein Verlust geschäftlicher Handlungsmöglichkeiten.

Aus diesem Grund kann die Investition in IT-Sicherheitskomponenten, sofern sie geringer ist als die dadurch mögliche Wertschöpfung, zu einer Kostenersparnis beitragen. Dies bedeutet eine Steigerung der Effizienz, die letztendlich auch die Wachstumschancen des Unternehmens verbessern kann.

13.3.7 Gesamtwirtschaftliche Betrachtung von Firewall-Systemen

In der früheren Industriegesellschaft war die Sicherheit von Produktionsanlagen wichtig. In der heutigen Informationsgesellschaft ist die Sicherheit von IT-Systemen von hoher Bedeutung. Informationen (Informationsgüter, digitale Produkte) erlangen erstmals eine überragende Bedeutung für Produktion und Konsum. Die Produktionsweise prägt die Gesellschaft. Es ist deshalb durchaus zulässig, von der

neuKap13.fm Seite 396 Freitag, 18. Oktober 2002 3:52 15

Entstehung einer Informationsökonomie auf die Entstehung einer Informationsgesellschaft zu schließen /Welz2000/.

Bei der gesamtwirtschaftlichen Betrachtung kann von statischen und dynamischen Aspekten gesprochen werden, wenn die mangelnde IT-Sicherheit diskutiert wird.

Statische Aspekte der mangelnden IT-Sicherheit führen zu einem Verlust an Effektivität und Effizienz im privaten wie öffentlichen Sektor und belasten somit die Leistungsfähigkeit der Volkswirtschaft insgesamt. Dies kann punktuell, d.h. bei einzelnen Unternehmen oder in einzelnen Sektoren, besonders gravierende Folgen haben.

Dynamische Aspekte der mangelnden IT-Sicherheit vermindern und behindern die Nutzung der rapide wachsenden Vorteile digitaler Technologien und Märkte (»New Economy«), z.B. wegen höherer Kosten und geringerer Akzeptanz, und führen indirekt zu einem Verzicht auf strategische Vorteile aus einer Marktdominanz.

Es bleibt abzuwarten, ob die Verantwortlichen in Wirtschaft und Behörden selbst für die notwendige Sicherheit sorgen, oder ob über Gesetze Vorschriften erlassen werden müssen, damit eine ausreichende Sicherheit unserer Informationsgesellschaft erreicht werden kann.

Das Problem gesetzlicher Vorschriften ist, dass diese international sein müssten, damit sie im globalem Internet greifen könnten. Die Bemühungen um eine internationale Gesetzgebung haben bei der G8 erst in Jahr 2000 begonnen und werden sicherlich fünf bis zehn Jahre benötigen.

13.4 Evaluierung und Zertifizierung von Firewall-Systemen

Vor der Anschaffung eines Firewall-Systems stellt sich Kunden und Benutzern die Frage, welche Sicherheitskriterien ein Firewall-System wirklich erfüllt.

Mit dem Mittel der Evaluation kann überprüft werden, ob angegebene Sicherheitsfunktionalitäten tatsächlich vorhanden sind und ihre Funktion korrekt erfüllen. Ziel der Evaluierung ist, dem Anwender des Sicherheitssystems das Vertrauen zu geben, ob angegebene Sicherheitsfunktionalitäten tatsächlich vorhanden sind und ihre Funktion korrekt erfüllen.

neuKap13.fm Seite 397 Freitag, 18. Oktober 2002 3:52 15

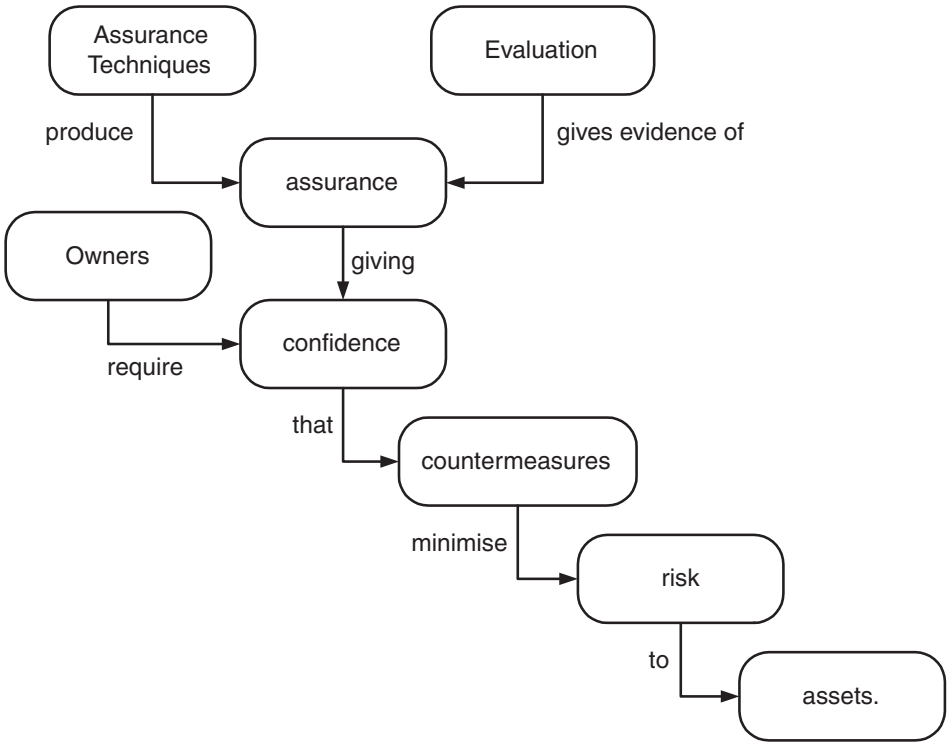


Abb. 13.7: Evaluierung und Zertifizierung

Ein Kunde oder Benutzer kann die Evaluation eines Firewall-Systems selbst durchführen oder von einem Spezialisten durchführen lassen. Eine Evaluation selbst durchzuführen, scheitert oft an der fehlenden Fachkenntnis oder an dem damit verbundenen enormen Aufwand.

Die Alternative besteht darin, die Evaluation durch eine kompetente und unabhängige Stelle durchführen zu lassen. Ein von Experten aufgrund einer durchgeführten Evaluation vergebenes Zertifikat bietet Kunden und Benutzern einen Maßstab bei der Bewertung unterschiedlicher Firewall-Systeme. Die Evaluation erfolgt dabei nach definierten Kriterien, die das BSI oder andere Stellen mit verschiedenen Firewall-Herstellern erarbeitet hat und die ein Firewall-System erfüllen muss, um zertifiziert zu werden (siehe Anhang F).

Zur Durchführung der Evaluierung und Zertifizierung von Firewall-Systemen gibt es verschiedene Möglichkeiten. In den folgenden Abschnitten werden exemplarisch die bekanntesten Zertifizierungsverfahren dargestellt, die Zertifizierung nach ITSEC- und nach ICSA-Kriterien. Zugleich wird die in der Praxis erreichbare »Tiefe« der Bewertung der beiden Verfahren beschrieben.

neuKap13.fm Seite 398 Freitag, 18. Oktober 2002 3:52 15

13.4.1 ITSEC-Zertifizierung

Die ITSEC (Information Technologie Security Evaluation Criteria) wurden von Frankreich, der Bundesrepublik Deutschland, den Niederlanden und Großbritannien auf der Grundlage von existierenden nationalen IT-Sicherheitskriterien [CESG3, DTIEC, SCSSI, ZSIEC, TCSEC] erarbeitet. Für eine Harmonisierung der unterschiedlichen Kriterien sprach die Forderung der Industrie, die in den verschiedenen Ländern verschiedene Sicherheitskriterien vorfand, und zum anderen der Vorteil, den sich die Beteiligten davon versprachen, die in den unterschiedlichen Ländern gesammelten Erfahrungen gemeinsam Gewinn bringend zu nutzen.

Die erarbeiteten Kriterien stellen die Grundlage für eine Zertifizierung durch die nationalen Zertifizierungsstellen dar, die nach diesen Kriterien erstellte Zertifikate gegenseitig anerkennen.

Eine Zertifizierung kann sowohl vom Hersteller als auch vom Vertreiber eines Firewall-Systems beantragt und durchgeführt werden. Der Vorteil einer vom Hersteller beantragten Zertifizierung liegt darin, dass die notwendigen Unterlagen bereits vorhanden sind und nicht erst erstellt werden müssen. Der mit dem Zertifizierungsprozess verbundene Aufwand ist allerdings sehr hoch. Die Zertifizierung durch einen Vertreiber lohnt nur bei einer niedrigen Evaluationsstufe, da dem Vertreiber die entsprechenden Sourcen (z. B. für die Software) nicht zur Verfügung stehen.

Im Folgenden wird exemplarisch dargestellt, welche Unterlagen vom Hersteller bzw. Entwickler bereitzustellen sind und welche Tests durchgeführt werden müssen, um eine Zertifizierung nach Stufe E3 zu erreichen.

Neben dem Hersteller bzw. Entwickler und der Zertifizierungsstelle ist eine akkreditierte Prüfstelle an der Evaluierung beteiligt. Die Prüfstelle (Prüflabor) führt die erforderlichen technischen Prüfungen im Auftrag des Herstellers unter Aufsicht der Zertifizierungsstelle durch und erstellt die jeweiligen Prüfberichte. Abschließend wird von der Zertifizierungsstelle ein Zertifizierungsreport mit allen Ergebnissen erstellt und veröffentlicht. Ergebnisse im Zertifizierungsreport sind z. B. die Beschreibung der Bedrohungen, denen das Firewall-System entgegenwirkt, die Liste der implementierten Sicherheitsmechanismen, Angaben zur genauen technischen und organisatorischen Einsatzumgebung des Firewall-Systems und Restrisiken unter bestimmten Voraussetzungen.

Die Evaluation erfolgt unter den Aspekten Korrektheit und Wirksamkeit. Bei der Bewertung der Korrektheit wird untersucht, ob die sicherheitsspezifischen Funktionen und Mechanismen korrekt implementiert wurden. Bei der Bewertung der Wirksamkeit wird beurteilt, ob die sicherheitsspezifischen Funktionen und Sicherheitsmechanismen des Firewall-Systems wirklich die vorgegebenen Ziele erreichen. Zusätzlich wird die Fähigkeit der Sicherheitsmechanismen bewertet,

neuKap13.fm Seite 399 Freitag, 18. Oktober 2002 3:52 15

Widerstand gegen einen direkten Angriff zu leisten (Stärke der Sicherheitsmechanismen).

Die für die Bewertung der Korrektheit erforderlichen Unterlagen, die der Hersteller bzw. Vertreiber zur Verfügung stellen muss, sind:

- die informelle Beschreibung der Architektur des Firewall-Systems
- die informelle Beschreibung des Feinentwurfs des Firewall-Systems
- die Testdokumentation
- die Bibliothek der Testprogramme und -werkzeuge, die für den Test des Firewall-Systems benutzt wurden
- Der Quellcode bzw. die Hardware-Konstruktionszeichnungen für alle sicherheitspezifischen und sicherheitsrelevanten Komponenten
- die informelle Zuordnungsbeschreibung, die den Bezug zwischen Quellcode bzw. Hardware-Konstruktionszeichnungen und Feinentwurf darstellt
- die Konfigurationsliste, die eindeutig die Version des Firewall-Systems identifiziert
- die Informationen über das Konfigurationskontrollsystem
- die Informationen über das Abnahmeverfahren
- die Informationen über die Sicherheit der Entwicklungsumgebung
- die Beschreibung aller benutzten Implementierungssprachen
- die Benutzerdokumentation
- die Systemverwalter-Dokumentation
- die Auslieferungs- und Konfigurationsdokumentation
- die Anlauf- und Betriebsdokumentation

Folgende Unterlagen des Firewall-Systems müssen unter dem Aspekt Wirksamkeit zur Verfügung gestellt werden:

- die Analyse der Eignung der Sicherheitsmechanismen
- die Analyse des Zusammenwirkens der Sicherheitsmechanismen
- die Analyse der Stärke der Sicherheitsmechanismen des Firewall-Systems
- die Liste der bekannten Schwachstellen in der Konstruktion
- die Analyse der Benutzerfreundlichkeit
- die Liste der bekannten Schwachstellen bei der operationellen Nutzung des Firewall-Systems

Sicherheitsvorgaben

In den Sicherheitsvorgaben werden die Sicherheitseigenschaften des Firewall-Systems beschrieben. Dabei handelt es sich um Kriterien, die die Sicherheitsmaßnahmen auf drei Ebenen betrachten:

- Sicherheitsziele: Weshalb wird die Funktionalität gebraucht?
- sicherheitsspezifische Funktionen: Welche Funktionalität wird zum Erreichen der Sicherheitsziele zur Verfügung gestellt?

neuKap13.fm Seite 400 Freitag, 18. Oktober 2002 3:52 15

- Sicherheitsmechanismen: Wie wird die Funktionalität zur Verfügung gestellt?

Die Sicherheitsvorgaben müssen die folgenden Punkte enthalten:

- eine Produktbeschreibung (welche Dienste sind implementiert, was für ein Security Management steht zur Verfügung usw.)
- die Art des Produkteinsatzes
- die vorgesehene Einsatzumgebung (technisch und administrativ)
- die Definition der Sicherheitsziele
- die angenommenen Bedrohungen, denen das Firewall-System entgegenwirkt
- die zur Verfügung gestellten sicherheitsspezifischen Funktionen
- die Sicherheitsmechanismen
- eine Beschreibung der Zweckmäßigkeit der Sicherheitsmechanismen.

Das Prüflabor prüft, ob für jede mögliche Bedrohung mindestens eine sicherheitsspezifische Funktion existiert, die ihr entgegenwirkt. Die Sicherheitsmechanismen, die die entsprechenden Funktionen zur Verfügung stellen, werden auf ihre Zweckmäßigkeit überprüft.

Architekturentwurf

Im Architekturentwurf wird die grundsätzliche Struktur des Firewall-Systems mit allen seinen externen Schnittstellen beschrieben. Hier findet eine Aufteilung des Firewall-Systems in sicherheitsspezifische und nicht-sicherheitsspezifische Komponenten statt. Sicherheitsspezifische Komponenten sind Komponenten, die direkt sicherheitsspezifische Funktionen ausführen oder daran beteiligt sind. Die Trennung von sicherheitsspezifischen und nicht-sicherheitsspezifischen Komponenten wird beschrieben und die Wirksamkeit dieser Trennung wird überprüft.

Feinentwurf

Der Feinentwurf des Firewall-Systems enthält die Spezifikation aller Komponenten und deren Schnittstellen. Alle sicherheitsspezifischen Funktionen müssen beschrieben und auf die Komponenten abgebildet werden. Alle Sicherheitsmechanismen müssen definiert und spezifiziert werden. Im Feinentwurf muss nachgewiesen werden, dass die angegebenen Sicherheitsmechanismen nicht in irgendeiner Form umgangen werden können.

Tests

Alle Sicherheitsmechanismen müssen dem Quellcode zugeordnet werden, d.h., es muss beschrieben werden, wo welcher Sicherheitsmechanismus wie implementiert ist. Jeder einzelne Sicherheitsmechanismus muss durch Tests nachgewiesen werden. Dazu muss der Hersteller neben dem Quellcode des Firewall-Systems die Testpläne, Testziele, Testverfahren, Testergebnisse und die Bibliotheken aller verwendeten Testprogramme und -werkzeuge in einer Testdokumentation festhalten.

neuKap13.fm Seite 401 Freitag, 18. Oktober 2002 3:52 15

Das Prüflabor überprüft anhand des Quellcodes und der Testdokumentation, ob alle sicherheitsspezifischen Funktionen betrachtet und alle Sicherheitsmechanismen getestet wurden. Dazu wird der Quellcode auf evtl. vorhandene Möglichkeiten zur Umgehung von Sicherheitsmechanismen analysiert, und die Tests werden wiederholt. Zusätzlich werden Penetrationstests und Tests zur Fehlersuche durchgeführt. Damit alle Sicherheitsmechanismen einzeln und gründlich getestet werden können, werden mehrere auf dem Markt verfügbare Werkzeuge – z. B. SATAN, Internet Security Scanner (ISS) – und eigene, spezielle Tools eingesetzt.

Entwicklungsumgebung

Die Entwicklungsumgebung umfasst das Konfigurationskontrollsystem, das Abnahmeverfahren, die Konfigurationsliste, die Beschreibung aller benutzten Implementierungssprachen und die Sicherheit der Entwicklungsumgebung.

Mit dem Konfigurationskontrollsystem, dem Abnahmeverfahren und der Konfigurationsliste stellt der Hersteller sicher, dass das Firewall-System mit der zur Verfügung gestellten Dokumentation übereinstimmt, nur autorisierte Änderungen daran möglich sind, das Firewall-System vollständig und die angegebene Version eindeutig sind.

Das Prüflabor prüft den Einsatz des Konfigurationskontrollsystems und das Abnahmeverfahren beim Hersteller.

Die Programmiersprachen, die für die Implementierung benutzt werden, müssen mit allen verwendeten Optionen eindeutig angegeben werden. Dies dient zu einer eventuell notwendigen Rekonstruktion des Firewall-Systems.

Der Hersteller muss mit Informationen über die Sicherheit seiner Entwicklungsumgebung beschreiben, wie die Schutzmaßnahmen bezüglich der Integrität des Firewall-Systems und die Vertraulichkeit der zugehörigen Dokumente realisiert werden. Alle dazu notwendigen Sicherheitsmaßnahmen müssen beschrieben werden. Die Maßnahmen werden eingeteilt in

- materielle, wie z. B. zugangsgeschützte Räume für die Entwicklungsrechner des Firewall-Systems, USV,
- organisatorische, wie z. B. restriktive Rechteverwaltung für die Entwicklungsrechner des Firewall-Systems, Regelung für den Modemgebrauch, und
- personelle Sicherheitsmaßnahmen, wie z. B. sicherheitsüberprüfte Entwickler und Mitarbeiter des Firewall-Systems.

Das Prüflabor prüft die Anwendung und die Einhaltung der angegebenen Verfahren bzw. der Vorschriften. Zusätzlich wird nach evtl. vorhandenen Fehlern in den angewendeten Verfahren gesucht.

neuKap13.fm Seite 402 Freitag, 18. Oktober 2002 3:52 15

Betriebsdokumentation

Die Betriebsdokumentation des Firewall-Systems unterteilt sich in Benutzerdokumentation und Systemverwalterdokumentation.

Die Benutzerdokumentation muss strukturiert aufgebaut und in sich konsistent sein. Sie muss Richtlinien für ihre sichere Anwendung enthalten und beschreiben, wie der Benutzer das Firewall-System auf sichere Art und Weise bedient.

Die Systemverwalterdokumentation muss strukturiert aufgebaut und in sich konsistent sein. Sie muss beschreiben, wie das Produkt installiert, konfiguriert und sicher verwaltet wird. Die Beschreibung der Sicherheitsparameter, der möglichen sicherheitsrelevanten Ereignisse, der Verfahren für die Sicherheitsadministration, der Sicherheitseigenschaften und deren Zusammenwirken müssen in der Systemverwalterdokumentation enthalten sein.

Betriebsumgebung

Die Betriebsumgebung unterteilt sich in zwei Aspekte:

- Auslieferung und Konfiguration
- Anlauf und Betrieb

Die Informationen zum angewendeten Verfahren der Auslieferung und Konfiguration müssen beschreiben, wie der Hersteller die Sicherheit des Firewall-Systems aufrechterhält, z. B. durch Prüfsummen der Software, Siegel, usw. Sind unterschiedliche Konfigurationen möglich, muss die Auswirkung der einzelnen Konfigurationen auf die Sicherheit beschrieben werden.

Das Prüflabor hat die korrekte Anwendung des Auslieferungsverfahrens für das Firewall-System zu überprüfen und nach Fehlern zu suchen.

Der Hersteller muss beschreiben, wie die Prozeduren für den Anlauf und Betrieb realisiert sind, und auf welche Weise sie die Sicherheit aufrechterhalten. Dazu müssen die sicherheitsspezifischen Funktionen beschrieben werden, die eventuell während des Anlaufs, des Betriebs oder der Wartung ausgeschaltet oder modifiziert werden können. Beispiele von Protokollaufzeichnungen bzw. Ergebnisse von Diagnoseprozeduren, die während des Anlaufs und des Betriebs erstellt werden, müssen vorgelegt werden. Das Prüflabor prüft die Protokollaufzeichnungen bzw. die Ergebnisse von Diagnoseprozeduren und sucht nach Fehlern in den Prozeduren.

Analyse der Eignung der Funktionalität

Bei der Analyse der Eignung der Funktionalität wird geprüft, ob es Bedrohungen gibt, denen nicht eine oder mehrere sicherheitsspezifische Funktionen des Firewall-Systems angemessen entgegenwirken.

neuKap13.fm Seite 403 Freitag, 18. Oktober 2002 3:52 15

Analyse des Zusammenwirkens der Funktionalität

Mit der Analyse des Zusammenwirkens wird gezeigt, dass die sicherheitsspezifischen Funktionen und Sicherheitsmechanismen des Firewall-Systems so zusammenwirken, dass sie sich gegenseitig unterstützen und ein wirksames Ganzes bilden. Des Weiteren wird gezeigt, dass keine sicherheitsspezifische Funktion und kein sicherheitsspezifischer Sicherheitsmechanismus existiert, die oder der in Konflikt mit anderen sicherheitsspezifischen Funktionen oder Sicherheitsmechanismen gerät oder ihnen entgegenwirkt.

Analyse der Stärke der Sicherheitsmechanismen

Diese Analyse bewertet die Fähigkeit der Sicherheitsmechanismen, direkten Angriffen zu widerstehen, die auf Mängel in den ihnen zugrunde liegenden Algorithmen, Prinzipien oder Eigenschaften zurückzuführen sind. Dabei wird auch der Aufwand an Betriebsmitteln betrachtet, die ein Angreifer benötigen würde, um einen erfolgreichen direkten Angriff durchzuführen. Analysen über die Algorithmen, Prinzipien und Eigenschaften, die diesen Sicherheitsmechanismen zugrunde liegen, müssen erstellt werden oder auf solche Analysen verweisen. Die Analyse erfolgt hinsichtlich der Einstufung der Mindeststärke und unter Verwendung aller zur Verfügung stehenden Informationen, einschließlich des Quellcodes des Firewall-Systems.

Das Prüflabor überprüft unter Verwendung aller zur Verfügung stehenden Informationen, einschließlich des Quellcodes, ob die Sicherheitsmechanismen die beanspruchte Mindeststärke gewährleisten. Zusätzlich werden aktive und agressive Penetrationstests zur Bestätigung der Mindeststärke durchgeführt.

Analyse der Benutzerfreundlichkeit

Ob sicherheitsspezifische Funktionen oder Mechanismen durch menschliche oder andere Fehler ausgeschaltet oder unbrauchbar gemacht wurden, muss einfach festzustellen und zu erkennen sein, damit Endbenutzer oder Administratoren nicht von einem sicheren Zustand ausgehen, obwohl das Firewall-System möglicherweise in einer Weise konfiguriert oder benutzt wird, die unsicher ist. Die Analyse der Benutzerfreundlichkeit muss mögliche Betriebsarten des Firewall-Systems beschreiben, einschließlich des Betriebes nach Bedien- und Betriebsfehlern, und ihre Konsequenzen für die Aufrechterhaltung eines sicheren Betriebes.

Das Prüflabor hat Analysen der Benutzerfreundlichkeit unter Verwendung aller zur Verfügung stehenden Informationen, einschließlich des Quellcodes, nach undokumentierten oder unvernünftigen Annahmen über die vorgesehene Betriebsumgebung zu überprüfen. Es muss jede Konfigurations- und Installationsprozedur nachvollziehen, um zu überprüfen, ob das Firewall-System sicher konfiguriert und benutzt werden kann.

neuKap13.fm Seite 404 Freitag, 18. Oktober 2002 3:52 15

13.4.1.1 Wirksamkeit der Firewall-Sicherheitsmechanismen

Im Folgenden werden die Wirksamkeitsaspekte von Firewall-Sicherheitsmechanismen untersucht.

Die Untersuchung der Wirksamkeit basiert auf einer Schwachstellenanalyse des Firewall-Systems. Bei dieser Analyse werden alle Wege gesucht, die es einem Angreifer erlauben würden, die sicherheitsspezifischen Funktionen und Sicherheitsmechanismen zu deaktivieren, zu umgehen, zu verändern, auszuschalten, direkt anzugreifen oder anderweitig außer Kraft zu setzen. Dabei werden alle zur Verfügung stehenden Informationen, auch der Quellcode, verwendet.

Stärke der Sicherheitsmechanismen, die im Firewall-System realisiert sind:

Selbst wenn ein Sicherheitsmechanismus nicht umgangen, außer Kraft gesetzt oder in anderer Weise korrumpiert werden kann, kann es dennoch möglich sein, ihn aufgrund von Mängeln in den zugrunde liegenden Algorithmen, Prinzipien oder Eigenschaften durch einen direkten Angriff zu überwinden. Für diesen Aspekt der Wirksamkeit muss die Fähigkeit der Sicherheitsmechanismen bewertet werden, solchen direkten Angriffen zu widerstehen. Der Aspekt der Wirksamkeit unterscheidet sich von anderen Aspekten dahingehend, dass er den Aufwand an Betriebsmitteln betrachtet, die ein Angreifer benötigen würde, um einen erfolgreichen direkten Angriff durchzuführen.

Wirksamkeit von Sicherheitssystemen:

Für die Beurteilung von Sicherheitssystemen ist es ein wichtiges Kriterium, ob die Sicherheitssysteme, die z. B. ein Firewall-System bietet, auch tatsächlich geeignet sind, den realen Angriffen entgegenzuwirken.

Im Folgenden wird dargestellt, wie die Wirksamkeit von Sicherheitssystemen generell beurteilt werden kann /ITSEM94/.

In der ersten Grafik werden die Werte einer Organisation, die es vor einem Angriff zu schützen gilt, durch einen Geldsack dargestellt. Die Angriffe, denen ein System ausgesetzt ist, werden durch Nägel repräsentiert, deren Länge proportional zur Größe der Fachkenntnisse, der Gelegenheiten und Ressourcen ist, über die der Angreifer verfügt.

Die Sicherheitsmechanismen, die eingesetzt werden, sind durch eine Wand dargestellt. Die Stärke dieser Wand ist proportional zur Stärke des Sicherheitsmechanismus. Je länger also der Nagel ist, desto schwerwiegender ist die Bedrohung. Je stärker die Wand, desto größer die Fähigkeit der Sicherheitsmechanismen diese Bedrohung der Werte einer Organisation abzuwehren.

neuKap13.fm Seite 405 Freitag, 18. Oktober 2002 3:52 15

Sicherheitsmechanismen sind dann sicher, wenn die Werte vollständig von einer Wand umgeben sind, deren Stärke an ihrer schwächsten Stelle mindestens gleich groß oder größer als die Länge des größten Nagels ist.

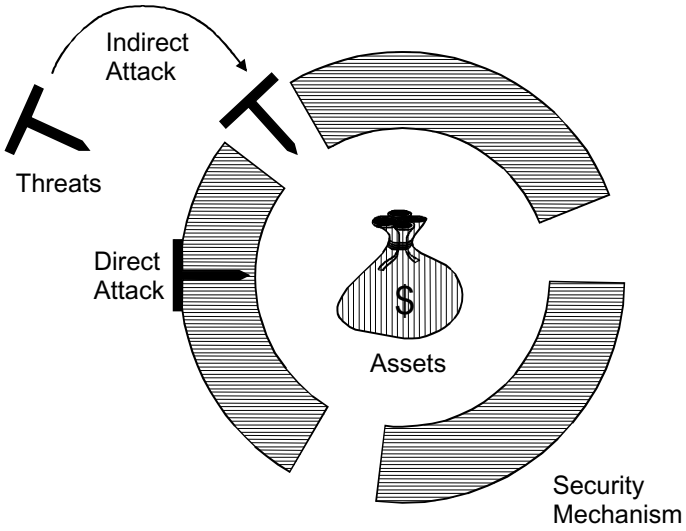


Abb. 13.8: Wirksamkeit

Es kann aber auch der Fall auftreten, dass die gewählten Sicherheitsdienste zur Abwehr der Bedrohung nicht ausreichen, obwohl ihre Sicherheitsmechanismen eigentlich stark genug sind.

Beispiele für »Indirect Attack«:

- Ein Angreifer hat die Möglichkeit, z. B. über das eingesetzte Betriebssystem die Rechteverwaltung des Firewall-Systems zu verändern.
- Nutzung des IP-Forwarding (Kernel-Funktionalität) von außen

Grundsätzlich kann die Stärke der Sicherheitsmechanismen von Sicherheitssystemen unterschiedlich bewertet werden. Hierbei wird die Bewertung niedrig, mittel und hoch verwendet.

Eine wichtige Größe für die Bewertung von Sicherheitsmechanismen ist die Mindeststärke des Sicherheitsmechanismus (SoMmin), die notwendig ist, um allen Angriffen erfolgreich entgegenzuwirken.

neuKap13.fm Seite 406 Freitag, 18. Oktober 2002 3:52 15

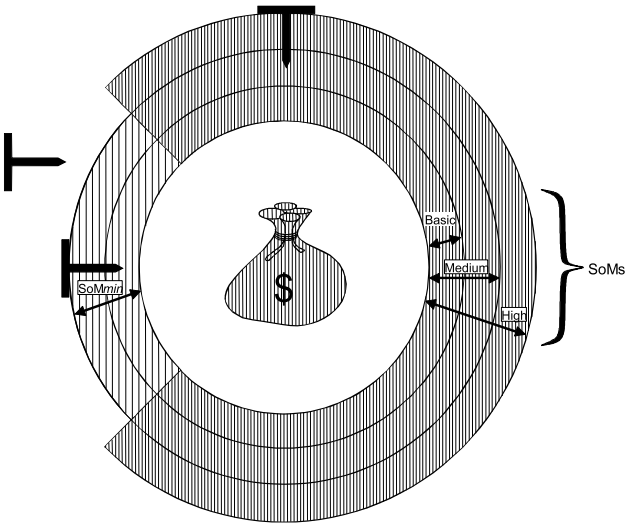


Abb. 13.9: Mindeststärke

Die nun folgenden Bilder sollen verdeutlichen, wie Schwachstellen im Firewall-System einzuschätzen sind, wie sie eingeordnet und schließlich wie sie behoben werden können.

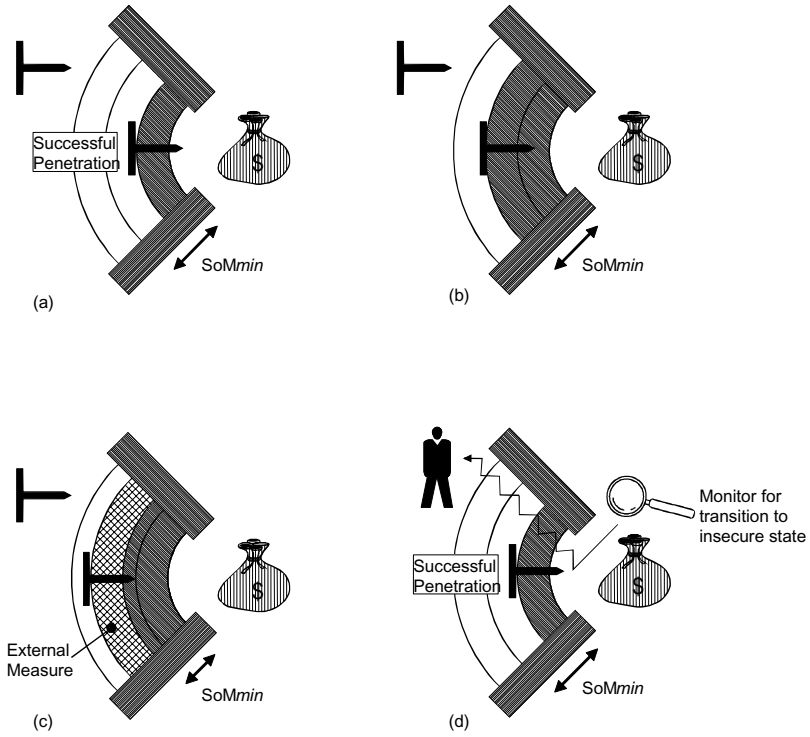


Abb. 13.10: Schwachstellen

neuKap13.fm Seite 407 Freitag, 18. Oktober 2002 3:52 15

Bild (a) zeigt eine erfolgreiche Überwindung der Sicherheitsmechanismen. Die Stärke der Wand entspricht nicht der erforderlichen Mindeststärke des Sicherheitsmechanismus. Sie kann daher vom Angreifer überwunden werden.

Beispiele:

- Die Tiefe der Analyse reicht nicht aus, den Angriff als solchen zu erkennen und damit zu verhindern.
- Maskerade-Angriff: Es gibt zwar eine Zugangskontrolle, z. B. mithilfe von Passwörtern, die aber von einem Angreifer unterlaufen werden kann, beispielsweise durch Mitlesen unverschlüsselt übertragener Passwörter.
- Über einen »well-known port« des Packet-Filters wird ein anderer Dienst ausgeführt.

In Bild (b) ist ersichtlich, dass durch die eingesetzten Mechanismen, also Algorithmen, Prinzipien und Eigenschaften, die erforderliche Mindeststärke der Sicherheitsmechanismen gewährleistet ist und der Angriff daher erfolgreich abgewehrt werden kann.

Bild (c) stellt dar, wie durch externe Maßnahmen die Wirksamkeit des Sicherheitsmechanismus noch erhöht werden kann, mit dem Ziel, den Angriff abzuwehren.

Beispiele:

- Vertrauenswürdigkeit des Netzes
- Durch die Sicherstellung der Vertrauenswürdigkeit des Netzes kann beispielsweise ein Maskerade-Angriff verhindert werden.
- Vertrauenswürdigkeit des Kommunikationspartners

Im Bild (d) ist dargestellt, dass zwar ein erfolgreicher Angriff nicht verhindert werden konnte, es jedoch möglich ist, den Angriff zu verfolgen, und dass so Maßnahmen eingeleitet werden können, um den Schaden – die Verwundbarkeit – zu reduzieren.

Beispiele:

- Protokollierung der sicherheitsrelevanten Informationen zur Erkennung und Analyse von Angriffen
- Beweissicherung, damit der erlaubte Teilnehmer nicht leugnen kann, bestimmte Aktionen durchgeführt zu haben

13.4.1.2 Mechanismenstärke und Evaluationsstufen

Dieser Abschnitt gibt die Mechanismenstärke und die Evaluationsstufen wieder, wie sie in den ITSEC-Kriterien definiert sind.

neuKap13.fm Seite 408 Freitag, 18. Oktober 2002 3:52 15

Mechanismenstärke	Beschreibung
niedrig	Es muss erkennbar sein, dass der Mechanismus Schutz gegen zufälliges Eindringen bietet, während er durch sachkundige Angreifer überwunden werden kann.
mittel	Es muss erkennbar sein, dass der Mechanismus Schutz gegen Angreifer mit beschränkten Gelegenheiten oder Ressourcen bietet.
hoch	Es muss erkennbar sein, dass der Mechanismus nur von Angreifern überwunden werden kann, die über sehr gute Fachkenntnisse, Gelegenheiten und Ressourcen verfügen, wobei ein solcher erfolgreicher Angriff als normalerweise nicht durchführbar beurteilt wird.

Tabelle 13.6: Unterscheidung der Mechanismenstärke in den Stufen niedrig, mittel und hoch.

Zur Erklärung der Begriffe **Fachkenntnisse**, **Gelegenheiten** und **Ressourcen**:

Fachkenntnisse betreffen das Wissen, über das Personen verfügen müssen, um ein Sicherheitssystem angreifen zu können. Ein Laie ist definiert als eine Person ohne besondere Fachkenntnisse, z. B. ein normaler Internet-Anwender. Eine kenntnisreiche Person hingegen ist mit den internen Arbeitsweisen des Sicherheitssystems vertraut. Ein Experte ist vertraut mit den grundlegenden Prinzipien und Algorithmen des Firewall-Systems (z. B. Hacker, Sicherheitsexperten oder Geheimdienste).

Ressourcen sind Mittel, die ein Angreifen für den erfolgreichen Angriff auf das Sicherheitssystem einsetzen muss. Unterschieden werden zwei Arten von Ressourcen, **Zeit** und **Ausstattung**. Zeit ist die Zeit, die ein Angreifer für die Durchführung eines Angriffs benötigt – nicht mitgerechnet wird hierbei die vorab für die Planung des Angriffs notwendige Zeit. Zur Ausstattung gehören Rechner, elektronische Geräte, Hardware, Werkzeuge, Software etc. Hierbei bedeutet *»innerhalb von Minuten«*, dass ein Angriff in weniger als 10 Minuten erfolgreich durchgeführt werden kann. *»Innerhalb von Tagen«* bedeutet, dass ein Angriff in weniger als einem Monat erfolgreich durchgeführt werden kann. *»Innerhalb von Monaten«* bedeutet, dass für einen erfolgreichen Angriff mindestens ein Monat benötigt wird.

»Ohne Ausstattung« bedeutet, dass die Durchführung eines Angriffs ohne besondere Hilfsmittel möglich ist, z. B. nur mit einem Browser. *»Vorhandene Ausstattung«* bedeutet Ausstattung, die ohne weiteres in der Betriebsumgebung des Firewall-Systems verfügbar oder Teil des eigentlichen Firewall-Systems ist oder käuflich erworben werden kann. *»Sonderausstattung«* heißt, dass eine besondere Ausstattung zur Durchführung eines Angriffs erforderlich ist.

Gelegenheiten bezieht sich auf Faktoren, die im Allgemeinen außerhalb der Kontrolle eines Angreifers liegen würden: Hilfestellungen durch andere Person (geheime Ab-sprachen), die Wahrscheinlichkeit eines Zusammentreffens bestimmter Umstände (Zufall), und die Wahrscheinlichkeit und die Konsequenz

neuKap13.fm Seite 409 Freitag, 18. Oktober 2002 3:52 15

einer Ermittlung des Angreifers (Entdeckung). Diese Faktoren sind generell nur sehr schwer zu bewerten. Möglich ist es aber, bezüglich der geheimen Absprachen eine Abstufung vorzunehmen:

1. *»allein«*: es ist für einen Angriff keine Absprache erforderlich.
2. *»mit einem Anwender«*: Um einen Angriff erfolgreich durchführen zu können, muss der Angreifer sich mit einem als nicht-vertrauenswürdig eingestuften Anwender des Sicherheitssystems absprechen.
3. *»mit einem Systemverwalter«*: Für einen erfolgreichen Angriff ist eine Absprache mit einem besonders vertrauenswürdigen Anwender des Firewall-Systems notwendig.

Für die Berechnung der Stärke des Sicherheitsmechanismus können folgende Regeln angewendet werden:

A. Kann der Sicherheitsmechanismus innerhalb von Minuten von einem Laien alleine überwunden werden, dann kann der Sicherheitsmechanismus nicht einmal als »niedrig« eingestuft werden.
B. Kann der Sicherheitsmechanismus nur von einem Experten mit Sonderausstattung überwunden werden, der dafür Monate braucht und eine geheime Absprache mit dem Systemverwalter treffen muss, dann ist der Sicherheitsmechanismus als »hoch« einzustufen.
C. Kann der Sicherheitsmechanismus nur in geheimer Absprache mit einem Anwender überwunden werden, ist er zumindest als »mittel« einzustufen.
D. Kann der Mechanismus nur in geheimer Absprache mit einem Systemverwalter überwunden werden, dann ist er als »hoch« einzustufen.
E. Sind für die erfolgreichen Angriffe Monate erforderlich, ist der Sicherheitsmechanismus mindestens als »mittel« einzustufen.
F. Erfordert ein erfolgreicher Angriff monatelanges Bemühen eines Experten mit Sonderausstattung, dann ist der Sicherheitsmechanismus als »hoch« einzustufen, unabhängig davon, ob eine geheime Absprache notwendig ist oder nicht.
G. Sind für einen erfolgreichen Angriff tagelange Bemühungen erforderlich, ist der Mechanismus mindestens als »niedrig« einzustufen.
H. Kann ein erfolgreicher Angriff von jedem bis auf einen Laien innerhalb von Minuten durchgeführt werden, so ist der Mechanismus als »niedrig« einzustufen.
I. Wenn ein erfolgreicher Angriff nur von einem Experten durchgeführt werden kann, der mit vorhandener Ausstattung Tage braucht, so ist der Sicherheitsmechanismus als »mittel« einzustufen.

Mit den folgenden beiden Tabellen kann die Stärke von Sicherheitsmechanismen abgeschätzt werden. Dabei sind die aus beiden Tabellen ermittelten Zahlen zu addieren. Aus dieser Summe ergeben sich die folgenden Wertungen:

neuKap13.fm Seite 410 Freitag, 18. Oktober 2002 3:52 15

	geheime Absprache		
Zeit	allein	mit einem Anwender	mit einem Systemverwalter
innerhalb von Minuten	0	12	24
innerhalb von Tagen	5	12	24
Monate/Jahr	16	16	24

	Ausstattung		
Fachkenntnisse	ohne Hilfsmittel	mit vorhandener Ausrüstung	mit Sonderausrüstung
Laie	1	entfällt	entfällt
kenntnisreiche Person	4	4	entfällt
Experte	6	8	12

Tabelle 13.7: Orientierungshilfe für die Beurteilung der Stärke von Sicherheitsmechanismen

A. Ist das Ergebnis 1, dann erreicht die Stärke nicht einmal die Stufe »niedrig«.
B. Ist das Ergebnis größer als 1, aber kleiner als 12, dann erreicht die Stärke die Stufe »niedrig«.
C. Liegt das Ergebnis zwischen 12 und 24, erreicht die Stärke die Stufe »mittel«.
D. Ist das Ergebnis größer als 24, dann erreicht die Stärke die Stufe »hoch«.

Diese Tabellen können nur als Orientierungshilfe dienen, da sie nicht unbedingt für alle Sicherheitsmechanismen und Betriebsumgebung verwendet werden können. Sie sind z. B. nicht für die Beurteilung von kryptographischen Sicherheitsmechanismen geeignet.

Für Firewall-Systeme, die zum Schutz des Zuganges zum Internet verwendet werden, muss die Mindeststärke »hoch« betragen, da im Internet Experten mit Sonderausrüstung und beliebig viel Zeit und Geld in großer Anzahl vorhanden sind.

13.4.1.3 Korrektheit der Firewall-Sicherheitsmechanismen

Die Korrektheit der Firewall-Sicherheitsmechanismen beurteilt, ob die implementierten Sicherheitsmechanismen korrekt implementiert sind und wie groß das Vertrauen in die Implementierung der Firewall-Lösung ist.

Zur Bewertung des Vertrauens in die Korrektheit werden nach ITSEC sieben hierarchische Evaluierungsstufen (E0 bis E6) definiert. E0 bezeichnet überhaupt keine Stufe, E1 bezeichnet die niedrigste Stufe und E6 entsprechend die höchste Stufe.

neuKap13.fm Seite 411 Freitag, 18. Oktober 2002 3:52 15

Wichtige Forderungen, die in der jeweils nächsthöheren Stufe hinzukommen, sind wie folgt definiert:

Evaluationsstufe	Beschreibung
E0	Stufe repräsentiert unzureichende Vertrauenswürdigkeit.
E1	Auf dieser Stufe müssen für den EVG die Sicherheitsvorgaben und eine informelle Beschreibung des Architekturentwurfs vorliegen. Durch funktionale Tests muss nachgewiesen werden, dass der EVG die Anforderungen der Sicherheitsvorgaben erfüllt.
E2	Zusätzlich zu den Anforderungen für die Stufe E1 muss hier eine informelle Beschreibung des Feinentwurfs vorliegen. Die Aussagekraft der funktionalen Tests muss bewertet werden. Ein Konfigurationskontrollsystem und ein genehmigtes Distributionsverfahren müssen vorhanden sein.
E3	Zusätzlich zu den Anforderungen für die Stufe E2 müssen der Quellcode bzw. die Hardware-Konstruktionszeichnungen, die den Sicherheitsmechanismen entsprechen, bewertet werden. Die Aussagekraft der Tests dieser Mechanismen muss bewertet werden.
E4	Zusätzlich zu den Anforderungen für die Stufe E3 muss ein formales Sicherheitsmodell Teil der Sicherheitsvorgaben sein. Die sicherheitsspezifischen Funktionen, der Architekturentwurf und der Feinentwurf müssen in semiformaler Notation vorliegen.
E5	Zusätzlich zu den Anforderungen für die Stufe E4 muss ein enger Zusammenhang zwischen dem Feinentwurf und dem Quellcode bzw. den Hardware-Konstruktionszeichnungen bestehen.
E6	Zusätzlich zu den Anforderungen für die Stufe E5 müssen die sicherheitsspezifischen Funktionen und der Architekturentwurf in einer formalen Notation vorliegen, die konsistent mit dem zugrunde liegenden formalen Sicherheitsmodell ist.

Tabelle 13.8: Unterscheidung der Evaluationsstufen

13.4.2 ICSA-Zertifizierung

Die International Computer Security Association (ICSA, vormals NCSA) ist ein von verschiedenen Anwendern und Hard- und Software-Herstellern, zu denen auch Firewall-Hersteller gehören, gegründeter Verein. Ziel dieses Vereins ist es, Benutzer bei der Erhöhung der IT-Sicherheit, der Wahrung der Integrität ihrer Informationen und der Reduzierung der Bedrohungen durch Computer-Viren zu unterstützen (siehe auch: *www.icsa.net*).

neuKap13.fm Seite 412 Freitag, 18. Oktober 2002 3:52 15

Der NCSA ist durch zahlreiche Veröffentlichungen im Bereich der Computersicherheit und durch die Erstellung eigener Kriterien für Firewall-Systeme bekannt geworden.

In diesem Abschnitt werden die ICSA-Kriterien für Firewall-Systeme vorgestellt, die in Funktions- und Sicherheitsanforderungen unterteilt sind.

Funktionsanforderungen

In den Funktionsanforderungen wird festgelegt, welche Dienste für die Anwender des zu schützenden internen Netzes, welche für die Anwender des ungeschützen externen Netzes und welche für das Management des Firewall-Systems zur Verfügung gestellt werden müssen.

Dienste für interne Anwender:

- Telnet über das Firewall-System auf externe Netze
- FTP über das Firewall-System auf externe Netze
- HTTP über das Firewall-System auf externe Netze
- SSL und/oder SHTTP über das Firewall-System auf externe Netze
- SMTP-Mail über das Firewall-System auf externe Netze
- DNS – externe DNS-Informationen für interne Anwender müssen zur Verfügung gestellt werden

Dienste für externe Anwender:

- FTP-Zugriff auf einen Server des internen Netzes oder ein Service-Netz
- HTTP-Zugriff auf einen Server des internen Netzes oder ein Service-Netz
- SSL und/oder SHTTP-Zugriff auf einen Server des internen Netzes
- SMTP-Mail muss den Anwendern des internen Netzes zugestellt werden können
- DNS

Anforderungen an das Management des Firewall-Systems

- Der Zugang zur Konsole des Firewall-Systems muss durch eine Passwort-Authentikation zu sichern sein.
- Wenn das Management remote über **externe** Netze durchgeführt werden soll,
  - müssen Einmal-Passwörter oder andere sichere Authentikationsmechanismen verwendet werden.
  - muss ein verschlüsselter Verbindungsmechanismus verwendet werden.
- Wenn das Management remote über **interne** Netze durchgeführt werden soll, darf die IP-Adresse nicht der einzige Mechanismus zur Authentikation des Security Administrators sein.

neuKap13.fm Seite 413 Freitag, 18. Oktober 2002 3:52 15

Sicherheitsanforderungen

Für die Erfüllung der Sicherheitsanforderungen werden die geforderten Funktionen getestet. Dazu werden die bekannten Einzelheiten über die Test-Konfiguration und die einzelnen Komponenten verwendet. Die Angriffe werden sowohl vom externen als auch vom internen Netz ausgeführt. Die folgenden Kriterien werden dabei zugrunde gelegt:

- Durch einen Angriff darf dem Angreifer nicht möglich sein, Kontrollmechanismen des Firewall-Systems oder des darunter liegenden Betriebssystems zu überwinden.
- Es dürfen keine anderen Protokolle oder Dateninhalte als die oben beschriebenen am Firewall-System vorbei ins interne Netz gelangen.
- Denial of Service: Das zu testende Firewall-System darf nicht durch einfache netzbasierende Angriffe funktionsunfähig gemacht werden können. Es gelten dabei die folgenden Ausnahmen:
  - Das Firewall-System verfügt über einen dokumentierten, selbstschützenden Mechanismus, mit dem ein Wechsel in einen Zustand ohne Firewall-Dienste erfolgt.
  - Wird erkannt, dass ein Angriff mit dem Ziel, das System lahm zu legen, Erfolg haben wird, muss das Produkt einen »geloggten« Alarm aussenden, bevor es sich selbst ausschaltet.

In der Testphase werden Netzwerk-Monitore sowohl das zu schützende Netz als auch der Bereich außerhalb des Firewall-Systems überwacht. Dafür wird die letzte Version des Produkts »ISS Security Scanner« unter Einbeziehung aller Daten des Firewall-Systems und des zu schützenden Systems eingesetzt.

Der ISS Security Scanner umfasst eine Zusammenstellung der zum Zeitpunkt der Versionsfreigabe bekannten und wiederholbaren Bedrohungen. NCSA führt als Teil der laufenden Tests regelmäßige Updates durch bis hin zur letzten Version bzw. letzten vorläufigen Version des Produktes.

Die Tests mit dem »ISS Security Scanner« werden zum einen aus einem benachbarten Teilnetz (External Scan) und zum anderen aus einem vertrauenswürdigen Teilnetz (Internal Scan) gegen das Firewall-System ausgeführt.

Mit einem Port Scanning Tool wird das Firewall-System mit dem Ziel getestet, die Übereinstimmung mit den Funktionsanforderungen festzustellen. Die Scans werden sowohl vom vertrauenswürdigen internen Teilnetz, als auch von einem nicht-vertrauenswürdigen benachbarten Teilnetz ausgeführt.

neuKap13.fm Seite 414 Freitag, 18. Oktober 2002 3:52 15

Diskussion ITSEC- und ICSA-Kriterien

ITSEC	ICSA
Die Stärke der Sicherheitsmechanismen wird angegeben. Dies ist auf Grund der ausführlichen Analysen möglich.	Es erfolgt keine Aussage über die Stärke der Sicherheitsmechanismen. Es muss daher von der Stufe »niedrig« ausgegangen werden.
Der Quellcode wird zur Verfügung gestellt. → Es erfolgt eine Überprüfung, ob die Sicherheitsmechanismen korrekt implementiert wurden und nicht umgangen werden können.	Der Quellcode wird nicht zur Verfügung gestellt. → Es ist keine Überprüfung der korrekten Implementation der Mechanismen möglich und evtl. vorhandene Fehler oder Trapdoors werden nicht erkannt.
Der Entwicklungsvorgang und die Umgebung des Firewall-Systems werden betrachtet.	Über den Entwicklungsvorgang und die Umgebung können keine Aussagen getroffen werden, da sie nicht betrachtet werden.
Es wird eine Aussage über die erfüllte Sicherheitsstufe gemacht.	Es wird nur ein Zertifikat erteilt oder nicht.
Es wird genau untersucht, welcher Sicherheitsmechanismus welche sicherheitsspezifische Funktion realisiert, und welcher Bedrohung damit entgegengewirkt wird.	Einzelne konkrete und zurzeit bekannte Angriffe werden abgewehrt. Sonst werden keine Aussagen gemacht.
Die Administration des Firewall-Systems durch ein Firewall-Management wird im Hinblick auf die verschiedenen Betriebsarten nach Bedien- und Betriebsfehlern analysiert.	Für das Firewall-Management werden nur Anforderungen bzgl. der Zugangskontrolle und des remote-Managements gestellt.
Die technische und administrative Einsatzumgebung muss angegeben werden und wird überprüft. Evtl. verbleibende Schwachstellen werden gezeigt.	Es werden keine Aussagen über die administrative Einsatzumgebung und die evtl. verbleibenden Schwachstellen gemacht.

Tabelle 13.9: Unterschiede in den Verfahren für die Zertifizierung von Firewall-Systemen

Zusammenfassend lässt sich sagen, dass die NCSA-Kriterien den ITSEC-Kriterien der Stufe E1 entsprechen, da nur durch funktionale Tests nachgewiesen wird, dass das Firewall-System die geforderten Sicherheitsziele erfüllt. Über die Stärke der Sicherheitsmechanismen erfolgt keine Aussage. Da die Tests aber mit einem frei verfügbaren Werkzeug durchgeführt werden, lässt sich nur eine Mechanismenstärke von »niedrig« zuordnen.

13.5 Weiterentwicklung von umfassenden Firewall-Systemen

Firewall-Systeme werden sich, wie auch die Kommunikationsanwendungen selbst, in Zukunft weiterentwickeln |Pohl 99b|. In diesem Abschnitt werden schlaglichtartig einige Aspekte der Weiterentwicklung von Firewall-Systemen beschrieben, die heute schon sichtbar sind.

neuKap13.fm Seite 415 Freitag, 18. Oktober 2002 3:52 15

Zunehmende Innovationen

Durch die zunehmenden Innovationen im Bereich der Internet-Anwendungen sollten neue Wege erforscht werden, wie die Firewall-Systeme sicher, schnell und dynamisch den neuen Anforderungen ohne Sicherheitsverlust angepasst werden können.

Integratives, zentrales Sicherheitsmanagement aller Sicherheitsmechanismen

In Zukunft wird es wichtig sein, dass die unterschiedlichen Sicherheitsmechanismen in ein gemeinsames Sicherheitssystem integriert werden, damit ein Höchstmaß an Sicherheit garantiert werden kann.

Immer höhere Geschwindigkeiten bei immer höherem Schutzbedarf

Da immer mehr Geschäftsprozesse über Kommunikationssysteme wie das Internet abgewickelt werden und der Umfang der ausgetauschten Informationen stetig steigt, werden in Zukunft höhere Bandbreiten für unsere Kommunikationssysteme notwendig. Je nach Einsatz werden sich die Bandbreiten unterschiedlich entwickeln. Für öffentliche Anschlüsse werden sie bei 34 bzw. 155 MBit/s liegen, später bei 622 MBit/s und mehr, im lokalen Bereich mit Fast Ethernet bei 100 Mbit/s, bei Gigabit Ethernet bis zu 1 GBit/s. Dies bedeutet, dass Firewall-Systeme in naher Zukunft entsprechende Geschwindigkeiten erbringen müssen, um einen hohen Datendurchsatz auch sicher bewältigen zu können.

Durch diese Entwicklung werden auch immer mehr höherwertige Informationen verarbeitet und gespeichert, die eine hohen bis sehr hohen Schutzbedarf haben.

Damit die zukünftigen Anforderungen an Geschwindigkeiten und Schutzbedarf realisiert werden können, müssen Realisierungskonzepte erarbeitet werden, wie z. B. Proxies optimiert und sicher in Hardware realisiert werden können, damit eine hohe Sicherheit bei einer hohen Geschwindigkeit erreicht werden kann.

Neue Proxies für neue Dienste

Durch die rasante Entwicklung der TCP/IP-Technologie werden in Zukunft Innovationen erwartet, die auch neue Dienste mit sich bringen. Für solche Dienste müssen, wenn sie sich etablieren, Proxies auf den Firewall-Systemen zur Verfügung gestellt werden, damit die Dienste über die Firewall-Systeme realisiert werden können und ein optimaler Schutz gewährleistet ist.

Universelle Identifikations- und Authentikationsverfahren

Durch das Signaturgesetz wird in Europa eine Sicherheitsinfrastruktur aufgebaut, die zum Vorbild für eine weltweite Regelung werden könnte. Diese Infrastruktur sorgt für eine eindeutige Identifikation aller Teilnehmer und macht Zertifikate (elektronische Ausweise) mit öffentlichen Schlüsseln für alle verfügbar. Auf der Basis

neuKap13.fm Seite 416 Freitag, 18. Oktober 2002 3:52 15

dieser Infrastruktur ist es möglich, ein einheitliches Identifikations- und Authentikationsverfahren für Firewall-Systeme, Rechnersysteme, Zugang zu Gebäuden usw. zu verwenden.

Jeder Teilnehmer dieser Infrastrukur verfügt über eine Chipkarte, mit der die Identifikation und Authentikation gegenüber den Firewall-Systemen durchgeführt werden kann. Dadurch ergeben sich für das Firewall-System Vereinfachungen. Den Zugang zu den Zertifikaten der Teilnehmer, die über das Firewall-System kommunizieren wollen, kann das Firewall-System z. B. durch eine Abfrage der öffentlichen Zertifizierungsinstanzen (TrustCenter) bekommen.

Einheitliche Darstellung der Angriffe und Sicherheitsdienste/-mechanismen

Da über die Wirksamkeit von Firwall-Systemen gegen definierte Angriffe in der Praxis keine qualitativen und vergleichbaren Aussagen gemacht werden, müssen, ähnlich wie beim TÜV, für den Anwender einheitliche Sicherheitskriterien für Firewall-Systeme von den Herstellern dargestellt werden, damit der Anwender die Möglickeit hat, die Sicherheit und die Vertrauenswürdigkeit von Firewall-Systemen einschätzen zu können. Dieser Punkt könnte z. B. durch ein einheitliches Firewall-System »Protection Profile« mithilfe der »Common Criteria« realisiert werden.

Protokollauswertung

Mithilfe von Protokollauswertungen können Sicherheitsverletzungen erkannt und eine Beweissicherung der Handlungen der Benutzer, die über das Firewall-System kommunizieren, erreicht werden. Damit diese wertvollen Sicherheitsfunktionen auch in Zukunft genutzt werden können, müssen weitere Verfahren erarbeitet werden, die ein automatisches Erkennen von Schutzverletzungen und eine effiziente Verwaltung der Protokolldaten bezogen auf die Beweissicherung ermöglichen. Hierdurch können Betriebskosten eingespart werden.

13.6 Überprüfung von Firewall-Systemen im Betrieb (Security Audit)

13.6.1 Einleitung

Ein Firewall-System besitzt wegen seiner Position als Bastion gegen ein als unsicher klassifiziertes Netzwerk in Bezug auf IT-Sicherheit einen besonders hohen Stellenwert. Die Sicherstellung der Firewall-Funktionalität ist deshalb ein wichtiges Element bei Betrieb und Wartung von Netzwerken. Da im IT-Bereich die Sicherheit von Systemen leider nur ein sehr relativer Status ist, ist die Überprüfung eines Firewall-Systems im laufenden Betrieb eine Aufgabe, die in regelmäßigen Abständen wiederholt werden muss. Die Gründe dafür liegen auf der Hand:

neuKap13.fm Seite 417 Freitag, 18. Oktober 2002 3:52 15

- Kein komplexes System ist absolut fehlerfrei. Das Betriebssystem des Firewall-Rechners und die Firewall-Software selbst müssen deshalb regelmäßig gewartet und auf den aktuellen Stand gebracht werden.
- Die Angriffsmöglichkeiten von außen sind so vielfältig und wandlungsfähig, dass ein heute als sicher geltendes System schon morgen gravierende Sicherheitslücken aufweisen kann.
- Ständig werden im Internet neue Dienste eingeführt, die – sofern sie in einer Organisation eingesetzt werden sollen – zu Konfigurationsänderungen am Firewall-System führen.

Darüber hinaus sollte bei allen Überlegungen zur Sicherheit von Firewall-Systemen stets berücksichtigt werden, dass – statistisch gesehen – die meisten Angriffe auf Rechnernetze von *innen* durchgeführt werden, zumeist von den eigenen Mitarbeitern. Deshalb muss in einem verantwortungsvoll administrierten Netz die Sicherheitsüberprüfung auf die gesamte IT-Infrastruktur ausgedehnt werden. Die im Verlauf dieses Kapitels beschriebenen Vorgehensweisen und Werkzeuge sind zwar in erster Linie auf die Kontrolle von Firewall-Systemen abgestimmt, in entsprechender Abwandlung können sie aber auch zur Überprüfung von größeren Teilen der Netz-Infrastruktur bis hin zum gesamten Netzwerk dienen.

13.6.2 Definition von Security Audit

Wenn es auch keine strenge Definition des Begriffs »Security Audit« gibt – jeder Dienstleister oder Hersteller von entsprechenden Werkzeugen versteht darunter meist genau das, was er anbietet – haben sich einige Randbedingungen und Kriterien herausgebildet, die Bestandteil jedes Security Audit sind. Herzstück eines Security Audit ist die Entdeckung von Sicherheitsmängeln jeglicher Art, sei es die Anfälligkeit für E-Mail-Bomben oder der ungehinderte Zugang zum Rechnerraum mit dem Firewall-System. Im Gegensatz zu einer bloßen Sicherheitsüberprüfung, die sich mit einer solchen Vorgehensweise zuzüglich einer Dokumentation der vorgefundenen Mängel zufrieden gibt, wird unter Security Audit die Einbettung der Überprüfung in die firmeninterne Sicherheitspolitik (Security Policy) verstanden. Voraussetzung eines Audit sind deshalb Existenz und (schriftliche) Fixierung einer Sicherheitspolitik und daraus abgeleiteter firmeninterner Sicherheitsrichtlinien. Beides ist in vielen Firmen nicht vorhanden, sodass nur die weniger effektiven Sicherheitsüberprüfungen durchgeführt werden können.

Sicherheitsaudits – ein Weg zu sicheren IT-Systemen

Sicherheitsaudits werden durchgeführt, um das bestehende Sicherheitsniveau festzustellen und gegebenenfalls erhöhen zu können.

Abbildung 13.11 stellt das Sicherheitsniveau einer Organisation im zeitlichen Verlauf dar.

neuKap13.fm Seite 418 Freitag, 18. Oktober 2002 3:52 15

Wurde in der Organisation bisher wenig für die IT-Sicherheit unternommen, so befindet sich das aktuelle Sicherheitsniveau unterhalb des angestrebten Sicherheitsniveaus (Zeitpunkt 1). Solange keine zusätzlichen IT-Sicherheitsmaßnahmen durchgeführt werden, sinkt das Sicherheitsniveau aus mehreren Gründen ständig ab (Zeitpunkt 1 bis Zeitpunkt 2):

- Die vorhandenen IT-Systeme werden ständig komplexer und damit unsicherer.
- Aus Unwissenheit oder Bequemlichkeit werden immer mehr Komponenten der IT-Systeme unsicher konfiguriert.
- Das Wissen und die Möglichkeiten potenzieller Angreifer wachsen stetig.

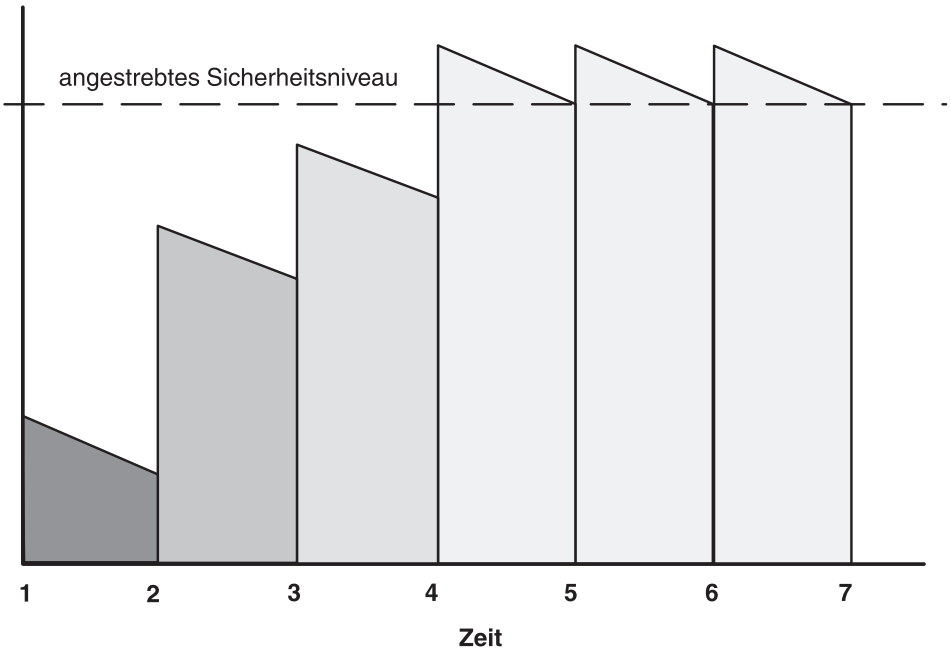


Abb. 13.11: Entwicklung des Sicherheitsniveaus im zeitlichen Verlauf

Zum Zeitpunkt 2 wird im Unternehmen eine höhere IT-Sicherheit eingeführt; beispielsweise werden eine Sicherheitspolitik und ein Sicherheitskonzept entworfen und implementiert. Dadurch steigt das Sicherheitsniveau beträchtlich. Das angestrebte Sicherheitsniveau ist jedoch noch nicht erreicht und das tatsächliche Niveau beginnt wieder abzusinken. Nun kann zum Zeitpunkt 3 ein Sicherheitsaudit durchgeführt werden, das die Anforderungen an die IT-Sicherheit mit der Realität in der Organisation vergleicht und bewertet. Sicherheitslücken werden entdeckt und angemessene Sicherheitsmaßnahmen werden vorgeschlagen. Diese Maßnahmen werden von der Organisation umgesetzt. Dadurch wird das Sicherheitsniveau erheblich angehoben. Allerdings werden die Sicherheitsmaßnahmen

neuKap13.fm Seite 419 Freitag, 18. Oktober 2002 3:52 15

bei der ersten Implementation nicht immer fehlerfrei konfiguriert, und mittel- und langfristige Maßnahmen greifen nicht sofort. Daher liegt das aktuelle Sicherheitsniveau noch unterhalb des angestrebten Niveaus.

Ein weiteres Sicherheitsaudit zum Zeitpunkt 4 ermöglicht es, noch vorhandene Sicherheitslücken und Konfigurationsfehler aufzudecken und geeignete Sicherheitsmaßnahmen vorzuschlagen. Deren Implementation hebt das Sicherheitsniveau in den angestrebten Bereich. Da wie oben beschrieben das Sicherheitsniveau ständig abnimmt, sollte von Zeit zu Zeit (Zeitpunkte 5, 6, ...) ein Sicherheitsaudit durchgeführt werden, um neue Sicherheitslücken zu entdecken und die Sicherheitsmaßnahmen daraufhin anzupassen.

Ziel eines Security Audit

Das Ziel eines Security Audit geht über die Entdeckung von Schwachstellen und Sicherheitslücken weit hinaus. Es dient der permanenten Abstimmung zwischen den Sicherheitsrichtlinien und deren praktischer Umsetzung. Deshalb beschränkt sich ein Security Audit nicht auf die Aufdeckung von technologischen Problemen wie der Überprüfung der Aktualität von Betriebssystem und Applikationen. Genauso wichtig ist die Einbeziehung von Daten, die organisatorische oder persönliche Mängel offenbaren können (siehe auch »*Theoretische Grundlagen von Firewall-Systemen*«, Kap. 14.5.12 und 14.6).

Vorgehensweise

Ausgehend von den Sicherheitsrichtlinien zur Installation und zum Betrieb des Firewall-Systems sammelt ein Security Audit mit den im Verlauf dieses Kapitels vorgestellten Werkzeugen Daten über Sicherheitsmängel. Diese werden in einem Bericht formuliert und dann – der entscheidende Punkt – in Form einer Rückkopplung in Bezug zu den Sicherheitsrichtlinien bzw. deren praktischer Umsetzung gesetzt. In den meisten Fällen werden dabei Mängel in der praktischen Umsetzung der Richtlinien festgestellt, der Bericht kann aber auch zu einer Modifikation bzw. Neudefinition der Richtlinien oder sogar der Sicherheitspolitik führen. Die Verknüpfung dieser Begriffe wird in der folgenden Abbildung verdeutlicht, wobei die Rückkopplung auf die Sicherheitspolitik aus Gründen der Übersichtlichkeit weggelassen wurde.

Ein Firewall-System stellt meist nur einen kleinen Ausschnitt einer firmeninternen Netz-Infrastruktur dar. Dennoch müssen zur Sammlung der Daten Informationsquellen aus dem gesamten Netzwerkbereich herangezogen werden. Zunächst einmal muss Ausgangsmaterial in Form von Plänen und Inventarlisten vorliegen, mit dem die weitere Vorgehensweise innerhalb des Security Audit festgelegt werden kann. Es schließen sich Interviews und Begehungen an, mit denen organisatorische, mitarbeiterbezogene und bauliche Mängel festgestellt werden. Erst dann werden durch technische Messungen Probleme im Firewall-System selbst bzw. sei-

neuKap13.fm Seite 420 Freitag, 18. Oktober 2002 3:52 15

ner Anbindung an das externe und interne Netz sichtbar gemacht. Für diesen Zweck stehen eine Reihe von kommerziellen Produkten, aber auch »Werkzeugkisten« mit Free- und Shareware zur Verfügung.

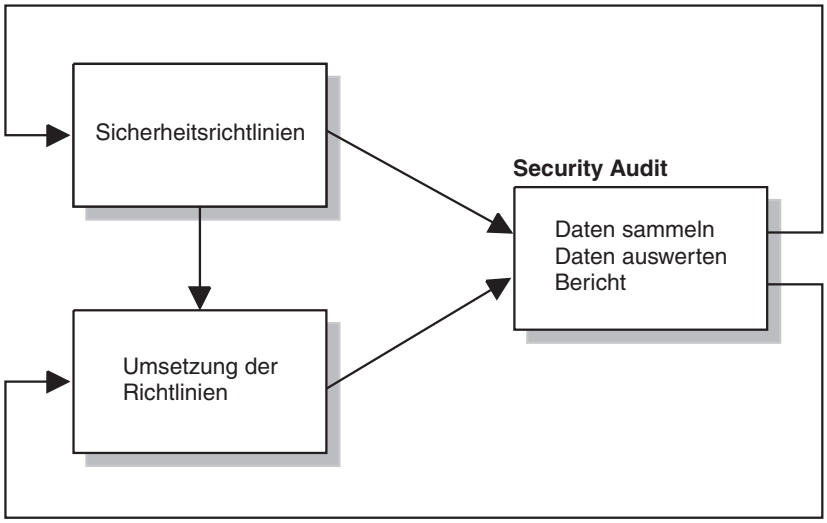


Abb. 13.12: Sicherheitspolitik

Wiederholung des Security Audit

Da die Sicherheit von Firewall-Systemen nie statisch ist, muss ein Audit in regelmäßigen Abständen wiederholt werden, auch wenn bei einer einzelnen Überprüfung keine Mängel festgestellt wurden. Als Faustformel kann ein Intervall von einem halben bis einem Jahr gelten, es sei denn, gravierende Änderungen sind erfolgt wie etwa

- Upgrade des Betriebssystems oder der Firewall-Software,
- Freischaltung neuer Dienste,
- größere Änderungen in dem durch das Firewall-System geschützten Netz oder Organisationsänderungen (Umzüge, Fusionen, Firmenübernahmen etc.),
- bauliche oder organisatorische Veränderungen, die das System betreffen,
- Entdeckung ganz neuer Klassen von Hackerangriffen.

In diesen oder ähnlichen Fällen sollte nach Abschluss der erforderlichen Maßnahmen ein Audit durchgeführt werden.

neuKap13.fm Seite 421 Freitag, 18. Oktober 2002 3:52 15

13.6.3 Komponenten eines Security Audit

Festlegung des Umfangs der Arbeiten

Trotz der Beschränkung des Audit auf ein einzelnes Firewall-System ergeben sich je nach Fragestellung und Ausgangssituation unterschiedliche Vorgehensweisen. So ist es beispielsweise ratsam, bei der Einführung eines E-Mail-Systems ein gezieltes Security Audit für diesen Dienst durchzuführen. In den meisten Fällen wird sich das Audit aber auf das Firewall-System als Ganzes beziehen, mit allen angebotenen Diensten und Protokollen. Auch die in direkter Verbindung mit Firewall-Systemen stehenden Systeme können bei Bedarf in die Untersuchungen einbezogen werden, wie die folgende Abbildung verdeutlicht.

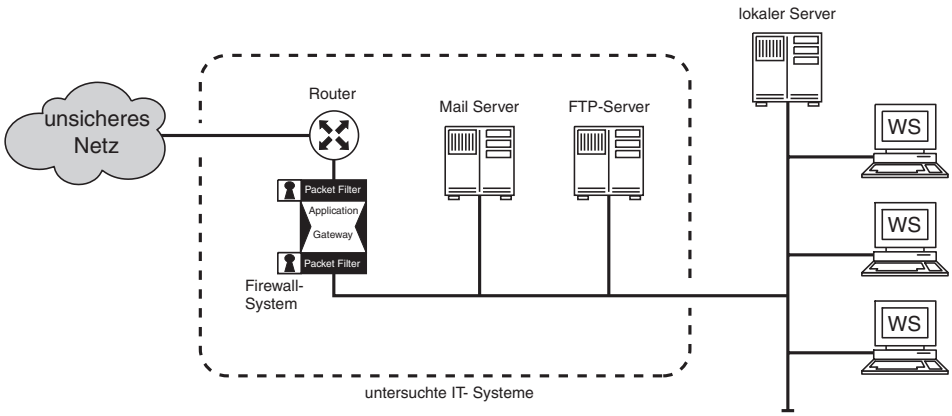


Abb. 13.13: Abgrenzung eines Security Audit

Beschaffung des Ausgangsmaterials

Der Bericht eines Security Audit kann nur so gut sein wie das Material, das der Datensammlung zugrunde liegt. Dabei kommt dem bereits vor Beginn der Arbeiten vorliegenden Ausgangsmaterial eine zentrale Bedeutung zu. Es sollte enthalten:

- Die schriftliche Formulierung der Sicherheitspolitik und den Sicherheitsrichtlinien. Sie stellt die »Brille« dar, durch die alle Recherchen und Auswertungen zu betrachten sind.
- Die Ergebnisse vorangegangener Audits, damit Fortschritte oder auch eine nachlassende Qualität der Sicherheit dokumentiert werden können.
- Inventarlisten für Hard- und Software, um Aktualität und Vollständigkeit der Systeminstallation zu überprüfen.
- Gebäudepläne, auf denen die Lage von Rechnerräumen und der Verkabelung sowie die Zugangsmöglichkeiten eingezeichnet sein müssen.

neuKap13.fm Seite 422 Freitag, 18. Oktober 2002 3:52 15

- Pläne der Netzwerktopologie, mit denen der Anschluss der Geräte kontrolliert werden kann.
- Eine Liste von Ansprechpartnern, falls weitere Informationen benötigt werden.

Je nach Größe und Struktur der Organisation kann die Beschaffung dieses Materials aufwändiger sein als die restliche Datensammlung bzw. deren Auswertung. Von der Vollständigkeit der Ausgangsdaten hängt die Qualität der im Endeffekt möglichen Rückkopplung der Ergebnisse des Audit auf Strategie und Richtlinien ab. Aus diesem Grunde werden trotz vorhandener Sicherheitsrichtlinien oft nur reine Sicherheitsüberprüfungen ohne Rückkopplung vorgenommen, die leichter durchzuführen, deren Ergebnisse aber wegen der fehlenden Einbettung in ein Gesamtkonzept oft schwieriger umzusetzen sind.

Fragestellungen

Nach der Sichtung des Ausgangsmaterials sollten die Ziele des Audit schriftlich formuliert werden. Fragestellungen könnten beispielsweise sein:

- Kontrolle der physikalischen Sicherheit des Firewall-Systems, d.h. Zugangsmöglichkeiten für Fremde, Möglichkeiten des Einloggens auf der Konsole des Firewall-Systems, Manipulation von Netzwerkverbindungen.
- Kontrolle der Aktualität der benutzten Software, d.h. Kontrolle, ob die Versionen mit den von den Herstellern als aktuell angegebenen Release-Ständen inklusive Hotfixes bzw. Patches übereinstimmen.
- Kontrolle der Installation und Konfiguration des Systems, Überprüfung auf bekannte Sicherheitsprobleme, wobei ältere Sicherheitslücken nicht von vornherein als »abgehakt« betrachtet werden dürfen.
- Kontrolle des Regelwerks des Firewall-Systems. Außer den zugelassenen Diensten müssen vor allem die gesperrten Ports, Protokolle und Benutzergruppen eingehenden Tests unterzogen werden.
- Simulation von Hackerangriffen mit den von diesen genutzten Tools.

Anschließend muss die Aufteilung der sich aus Ausgangsmaterial und Fragestellungen ergebenden Arbeiten auf die drei Komponenten des Audit »Begehungen«, »Interviews« und »technische Messungen« vorgenommen werden.

Datensammlung

Um das IT-System möglichst vollständig zu analysieren, muss während der eigentlichen Datensammlung Material aus ganz verschiedenen Quellen zusammengeführt werden:

- Daten zur Organisationsstruktur geben einen Überblick über die Verankerung des IT-Systems und seiner Betreuer innerhalb der Organisation.
- Personendaten dienen zur Überprüfung der Zuverlässigkeit der das IT-System betreuenden EDV-Mannschaft.

neuKap13.fm Seite 423 Freitag, 18. Oktober 2002 3:52 15

- Daten über die baulichen Gegebenheiten geben Aufschluss über eventuelle unbefugte Zugangsmöglichkeiten zu Netzwerk und Rechnerraum.
- Technische Daten schließlich dokumentieren die Empfindlichkeit bzw. Resistenz des IT-Systems gegenüber Angriffen. Die für die Sammlung dieser Daten benötigten Werkzeuge sind in Kapitel 13.6.3 näher beschrieben.

Dabei müssen die Zeiten der Arbeiten am IT-System sorgfältig mit den betroffenen Benutzern abgestimmt werden, um Kosten durch Arbeitsausfälle zu vermeiden. Besonders bei Denial-of-Service-Angriffen auf das Firewall-System kann ein »erfolgreicher« Angriff das Kommunikationssystem lahm legen oder sogar den Firewallrechner beschädigen, z. B. das File-System.

Erstellung des Berichtes

Der abschließende Bericht fasst das Ausgangsmaterial und die bisher gewonnenen Erkenntnisse zusammen und setzt diese in Beziehung zu Sicherheitspolitik bzw. -richtlinien. In der Praxis hat sich folgende Vorgehensweise bei der Erstellung von Berichten als günstig erwiesen:

- Der Bericht sollte keinesfalls nur Kritik an gefundenen Mängeln üben, sondern auch positive Aspekte an den vorgefundenen Sicherheitsmaßnahmen aufzeigen.
- In der Einleitung werden die Strategie des Audit und die wichtigsten Ergebnisse leicht erfassbar zusammengestellt.
- Der Rest der Auswertung sollte Top-Down erfolgen, d. h. vom Allgemeinen hin zum Detail; Lagepläne und Beispiele aus der Datensammlung gehören in den Anhang.
- Die Zusammenfassung enthält vor allem die Verbesserungsvorschläge und die Rückkopplung auf Sicherheitsstrategie und -richtlinien.
- Disketten oder eine CD-ROM mit den gesammelten Daten sollten zusammen mit dem Bericht archiviert werden.

Präsentation der Ergebnisse des Security Audit

Je nach Umfang und Bedeutung des Security Audit ist eine Präsentation der Ergebnisse gewünscht. Hier ist eine streng sachbezogene Darstellung erforderlich, da die gefundenen Fehler und Schwachstellen meist in den Verantwortungsbereich der Teilnehmer an der Veranstaltung fallen. Schuldzuweisungen sollten in einem solchen Gremium unterbleiben, positive Aspekte müssen benannt werden. Der Schwerpunkt einer Präsentation liegt auf zukünftigen Perspektiven der IT-Sicherheit und den sich aus diesen ergebenden Aufgaben und Fragestellungen, die die IT-Sicherheit noch verbessern können.

13.6.4 Werkzeuge zur technischen Datensammlung

Während die Sammlung von Daten in der Anfangsphase eines Audit überwiegend mit Papier und Bleistift durchgeführt wird, sind bei den anschließenden Messun-

neuKap13.fm Seite 424 Freitag, 18. Oktober 2002 3:52 15

gen eigene Rechner zur Aufdeckung von Sicherheitslücken und zur Simulation von Angriffen erforderlich. Einen Standard zur Ausstattung mit Hardware und Software gibt es nicht, je nach Fragestellung ist meist eine kleine »Toolbox« mit mehreren, sich ergänzenden Komponenten erforderlich.

Audit-Rechner

Aus der Konfiguration des Firewall-Systems und seiner Anbindung an das restliche Netzwerk ergeben sich die Anforderungen an die »Messrechner«, mit denen die technischen Sicherheitsprobleme entdeckt werden sollen. Drei Variationen sind denkbar und sollen am Beispiel eines Firewall-Systems mit einem gesonderten Netz für Mail- und FTP-Server erläutert werden.

Die ersten beiden Varianten arbeiten mit zwei Messrechnern, alle denkbaren Problemstellen werden nach und nach untersucht.

In Messung 1 findet die Überprüfung des Router statt, ein Angriff von außen wird simuliert:

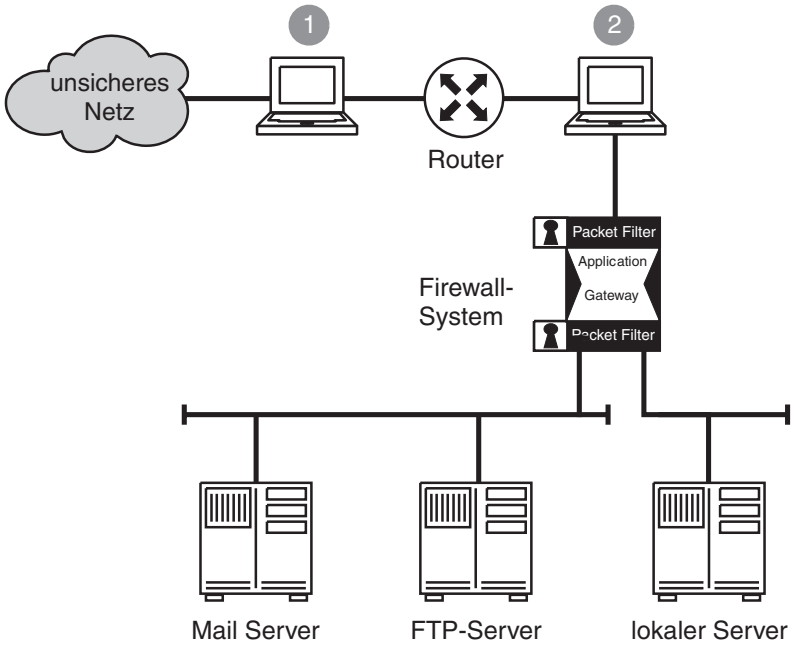


Abb. 13.14: Messung 1: Überprüfung eines Routers

Falls im Router keine Filterfunktionen aktiviert sind, kann diese Messung auch weggelassen werden. Im zweiten und dritten Schritt wird der Durchgang durch das Firewall-System geprüft, die Messungen 2 und 3 sind im folgenden Bild vereint:

neuKap13.fm Seite 425 Freitag, 18. Oktober 2002 3:52 15

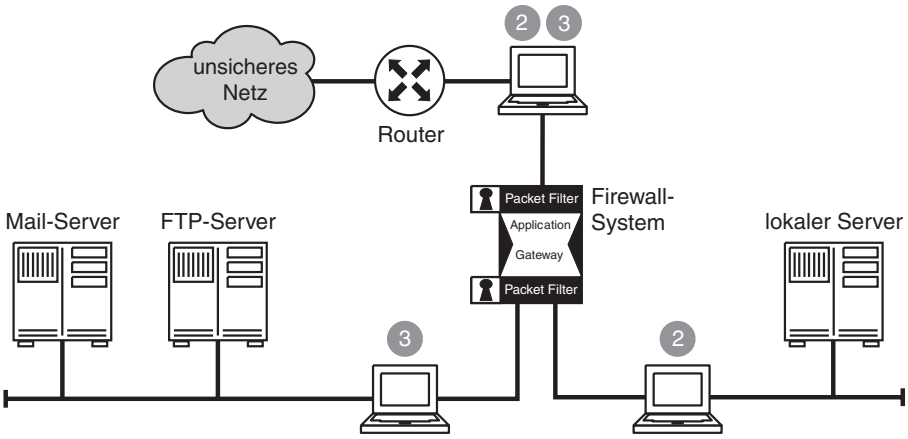


Abb. 13.15: Messung 2 und 3

Die zweite Variante betrachtet das Firewall-System als Black Box und untersucht nur die Schnittstellen nach außen. Hier reichen zwei Durchgänge bei den Messungen aus, die wieder in einem Bild vereint dargestellt sind:

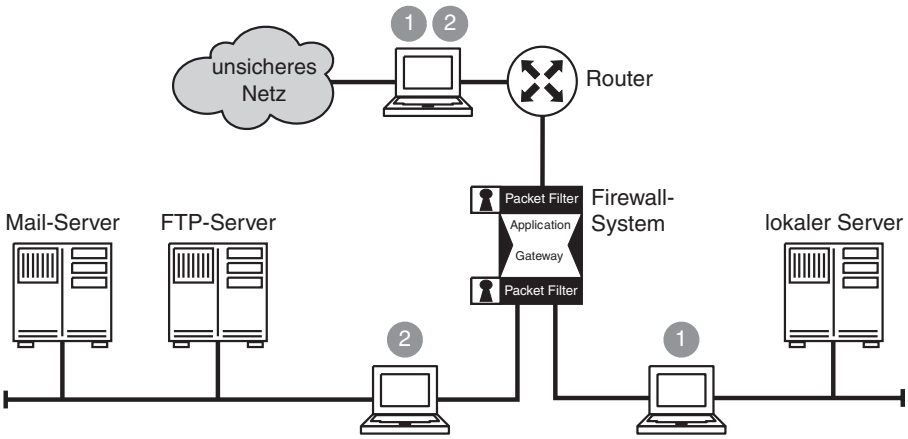


Abb. 13.16: Überprüfung der Schnittstellen

Die letzte Variante kommt mit einem einzelnen Messrechner aus. Dafür befindet sich auf dem Firewall-System eine zusätzliche Protokoll-Software, die eingehende Pakete zur späteren Auswertung aufzeichnet. Dazu werden die Protokollinformationen des Firewall-Systems verwendet. Zwei Messungen reichen aus (Mess-PC bei Messung 1 auch möglich zwischen Router und Firewall-System):

neuKap13.fm Seite 426 Freitag, 18. Oktober 2002 3:52 15

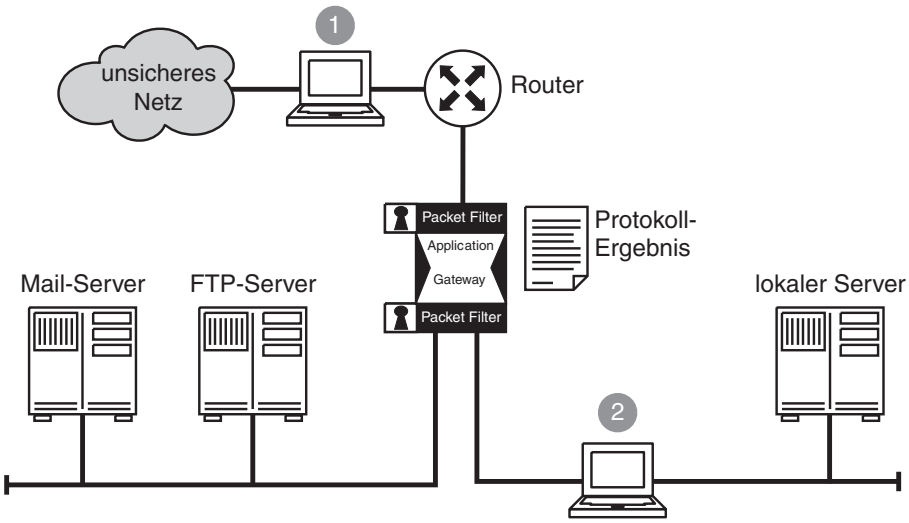


Abb. 13.17: Einzelner Messrechner mit Protokoll-Software

Messungen, die einen Angriff aus dem screened Subnet heraus simulieren, sind im Normalfall nicht nötig. Sie können hier – ebenso wie in den beiden ersten Varianten – zusätzlich durchgeführt werden, wenn die Folgen einer eventuellen »feindlichen Übernahme« des Mail- oder FTP-Servers (im Beispiel) aus dem Internet heraus simuliert werden sollen:

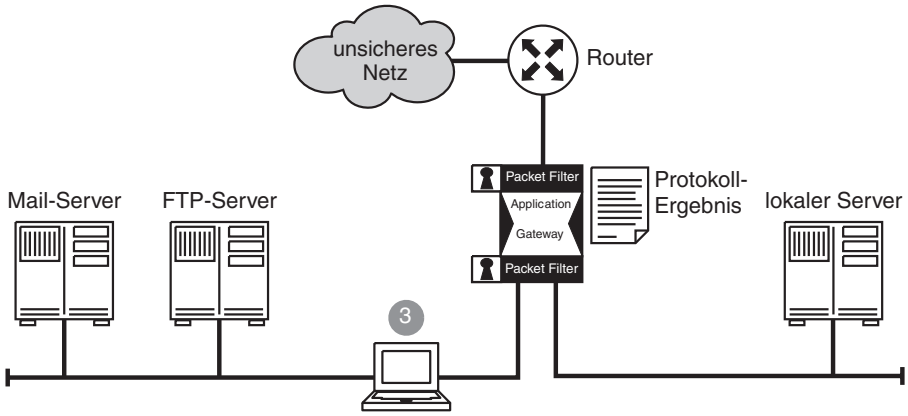


Abb. 13.18: Simulation einer »feindlichen Übernahme«

neuKap13.fm Seite 427 Freitag, 18. Oktober 2002 3:52 15

Audit-Tools

Auf dem Markt gibt es zahlreiche Software-Tools zur Unterstützung des Security Audit. Das Angebot reicht von kommerziellen Programmen bis hin zu der unüberschaubaren Menge von im Internet frei verfügbaren Tools. Die Auswahl hängt von den Sicherheitsrichtlinien und dem möglichen finanziellen Aufwand ab. Die Qualität der Ergebnisse eines Audit korreliert allerdings nicht unbedingt mit dem Preis der Tools, die Gewinnung der Daten ist mit einem der professionellen Programme natürlich komfortabler. Wie der Korb der Software-Pakete auch zusammengestellt ist, folgende Funktionalitäten müssen in jedem Falle vorhanden sein:

- Ein LAN-Analyser – am besten mit graphischer Oberfläche. Mit ihm können statistische Daten über den Netzwerkverkehr gewonnen und einzelne, besonders interessierende Pakete herausgefiltert und deren Header bzw. Daten angeschaut werden.
- Ein IP-Portscanner, mit dem die auf dem Firewall-System zur Verfügung gestellten Dienste untersucht werden können.
- Ein Tool, das die Qualität der Passwörter aller Accounts auf das Firewall-System, FTP-Server etc. überprüft.
- Ein Netzwerkscanner, mit dem das Firewall-System auf bekannte Sicherheitslücken untersucht werden kann.
- Eine Sammlung der gängigen Angriffstools, wie sie von Hackern eingesetzt und aus dem Internet gezogen werden können.

Produktübersicht

Die folgende Zusammenstellung von Produkten erhebt keinen Anspruch auf Vollständigkeit. Aus diesem Pool von kommerziellen und frei verfügbaren Werkzeugen kann ein individueller Apparat zusammengestellt werden, mit dem eine Analyse der technischen Schwachstellen von Firewall-Systemen in jeder gewünschten Tiefe möglich ist.

LAN-Analyser

- LANalyser des Novell-Programmpakets ManageWise (`http://www.novell.de`)
- Observer von Network Instruments (`http://www.netinst.com/`)
- Protokollanalysatoren von Radcom (`http://www.radcom-inc.com/`), Kombination von Hard- und Software
- Sniffer von Network Associates (`http://www.sniffer.com/`)

Netzwerkscanner

- CyberCop (`http://www.nai.com/products/security/ballista/default.asp`) von Network Associates ist ein kommerzielles Produkt und gehört zu den besten und vollständigsten auf dem Markt. Es ist besonders für den Test von Firewall-Systemen geeignet.

neuKap13.fm Seite 428 Freitag, 18. Oktober 2002 3:52 15

- Von Internet Security Systems ISS (`http://www.iss.net/`) werden frei verfügbare und kommerzielle Scanner angeboten. Der kommerzielle Scanner ist sehr komfortabel und in seiner Funktionalität mit CyberCop zu vergleichen, auch was die hervorragende Eignung für Firewall-Systeme angeht. Für Windows NT-Netze ist dieses Produkt besonders zu empfehlen.
- Der Kane Security Analyst (`http://www.intrusion.com/`) ist einer der wenigen Scanner, die auch unter Novell laufen.
- Nessus (`http://www.nessus.org/`) ist ein neues Freeware-Tool, das wesentlich aktueller als SATAN ist.
- NSS (`ftp://jhunix.hcf.jhu.edu/pub/nss/`) ist ebenfalls frei verfügbar, sollte aber nur zusammen mit anderen Tools eingesetzt werden.
- Der Cisco Secure Scanner (ehemals Cisco NetSonar Security Scanner) zeigt eine besonders übersichtliche graphische Darstellung der Ergebnisse (`http://www.cisco.com/univercd/cc/td/doc/pcat/nssq.htm`)
- SAINT (`http://www.wwdsi.com/`) ist eine kommerzielle Weiterentwicklung des Standardscanners SATAN, die den aktuellen Stand der Sicherheitslücken umfasst.
- SATAN (`ftp://ftp.porcupine.org/pub/security`) ist ein frei verfügbarer Scanner, der allerdings schon etwas in die Jahre gekommen ist und deshalb nur in Kombination mit anderen Produkten eingesetzt werden sollte.

Sonstige Tools (Freeware)

- COPS (`ftp://ftp.cert.org/pub/tools/cops`) analysiert Dateiberechtigungen und -attribute auf UNIX-Systemen.
- Crack (`http://www.users.dircon.co.uk/~crypto/`), der Standard-Passwortcracker unter UNIX.
- Dig (`ftp://venera.isi.edu/pub/`) fragt DNS Sver aus.
- Lophtcrack (`http://www.l0pht.com`) ist der Standard-Passwortcracker für NT.
- Lsof (`ftp://vic.cc.purdue.edu/pub/tools/unix/lsof`) zeigt auf UNIX-Systemen alle offenen Filehandles an.
- Merlin (`ftp://ciac.llnl.gov/pub/ciac/sectools/unix/merlin/merlin.tar.gz`) ist ein Interface zur Analyse von Daten.
- Network Toolbox Portscanner (`http://www.jriver.com`)
- Tiger (`ftp://net.tamu.edu/pub/security/TAMU/`) ist in seiner Funktionalität ähnlich zu COPS.

13.6.5 Zusätzliche Informationsquellen

Ein verantwortungsbewusster Administrator muss sich ständig über neu aufgetretene Sicherheitsprobleme informieren. Es reicht nicht aus, sich auf die Entwickler von Netzwerkscannern zu verlassen. Zum Glück gibt es eine ganze Reihe von Institutionen, die neue Nachrichten zum Thema Sicherheit bei Firewall-Systemen

neuKap13.fm Seite 429 Freitag, 18. Oktober 2002 3:52 15

über Internetseiten oder Mailinglisten frei Haus liefern. Die folgende Übersicht stellt die wichtigsten internationalen Adressen zusammen.

Informationen zur Firewall-Sicherheit im Internet

- Das CERT Coordination Center (Computer Emergency Response Team; `http://www.cert.org`) in Pittsburgh, Pennsylvania beschäftigt sich seit seiner Gründung 1984 mit Sicherheitsfragen im Internet. Hier gibt es viele Hinweise sowie eine große Sammlung von Dokumenten zu Sicherheitslücken in Rechnernetzen.
- AUSCERT (`http://www.auscert.org.au`) ist die australische Variante von CERT und ist oft etwas schneller als ihre amerikanische Schwester.
- FIRST (Forum of Incident Response and Security Teams; `http:// www.first.org`) ist eine Dachorganisation, bei der zahlreiche nationale und internationale Institutionen zum Thema »Firewall« Mitglied sind.
- CIAC (Computer Incident Advisory Capability; `http://ciac.llnl.gov`) wurde 1989 gegründet und hat wohl die umfangreichste Sammlung von Dokumenten zum Thema Sicherheit.
- Die ICSA (International Computer Security Association; `http://www.icsa.net`) ist ein Zusammenschluss von Herstellern von Firewall-Systemen und anderen Institutionen.
- Das Bugtraq-Archiv (`http://www.securityfocus.com`) ist ein unabhängiges Kommunikationsforum zum Thema, wo Fehler oft lange vor den »offiziellen« Stellen diskutiert werden.
- Das NT Bugtraq-Archiv (`http://www.ntbugtraq.com`) behandelt ausschließlich das Thema NT.
- NTSecurity (`http://www.ntshop.net`) ist ein weiteres unabhängiges Forum für NT-Systeme.
- Microsoft hat eigene Seiten zum Thema Sicherheit (`http://www.microsoft.com/security`).

13.6.6 Allgemeine Mailinglisten

- Zur Anmeldung bei CERT bitte eine E-Mail an `cert-advisory-request @cert.org` senden, als *Subject* bitte `SUBSCRIBE <eigene E-Mail Adresse>` angeben.
- Die Liste des Bugtraq-Archivs wird mit einem Formular in `http://www.securityfocus.com` bestellt. Sehr umfangreich!
- NT Bugtraq wird mit einer Mail an `listserv@listserv.ntbugtraq.com` mit dem Text `subscribe ntbugtraq <firstname> <lastname>` abonniert.
- Internet Security Systems (ISS) bietet eine herstellerübergreifende Alarmierung an. Senden Sie eine Mail an `request-alert@iss.net` mit dem Text `subscribe alert`
- Die Liste von Internet Security Systems (ISS) zum Thema NT wird mit einem Mail an `request-ntsecurity@iss.net` mit dem Text `subscribe ntsecurity` bestellt. Sehr umfangreich!

neuKap13.fm Seite 430 Freitag, 18. Oktober 2002 3:52 15

Herstellerspezifische Mailinglisten

- Der Empfang einer HP-Mailingliste wird über eines der beiden Servicecenter im Internet aktiviert, nach der Anmeldung die Rubrik »Support Information Digests« anwählen (`http://europe-support.external.hp.com` oder `http://us-support.external.hp.com`.
- Die AIX-Mailinglisten von IBM können ebenfalls über das Internet abonniert werden: `http://rs6000.ibm.com/resource/maillist.html`, oder per Mail an `aixserv@austin.ibm.com` mit dem Subject `subscribe Security`.
- Microsoft gibt eine eigene Liste heraus, die unter `microsoft_security-subscribe-request@announce.microsoft.com` bestellt werden kann.
- Redhat bietet eine Mailingliste zum Thema Linux-Sicherheit an, die mit Mails an
  `linux-security-request@redhat.com`,
  `linux-security-digest-request@redhat.com` bzw.
  `linux-alert-request@redhat.com`
  jeweils mit dem Text `subscribe` aktiviert werden.
- Silicon Graphics' Mailingliste »wiretap« wird mit einer Mail an `wiretap-request@sgi.com` und dem Text
  ```
  subscribe wiretap <eigene E-Mail Adresse>
  end
  ```
  aktiviert.
- Die Nachrichten des Customer Warning System (CWS) von Sun werden durch eine Mail an `security-alert@sun.com` mit dem Subject `subscribe cws <eigene E-mail Adresse>` bestellt.
- AIX (`http://techsupport.services.ibm.com/support/rs6000`)
- RedHat (zahlreiche Listen unter `http://www.redhat.com/community/list_subscribe.html`)
- SuSE (`http://www.suse.de/de/support/mailinglists/index.html`)
- SGI (`http://www.sgi.com/support/security/wiretap.html`)

13.7 Intrusion-Detection/Response-Systeme

13.7.1 Einleitung

Da Firewall-Systeme nur auf bereits bekannte und in ihrer Datenbank hinterlegte Ereignisse reagieren können, werden weitere ergänzende Sicherheitsmechanismen benötigt, die auf neue, also unbekannte Ereignisse reagieren können. Zu vielfältig und entwicklungsfähig sind die Möglichkeiten, mit denen von außen (via Internet) oder sogar von innen (via Intranet) die Rechnersysteme und/oder ihre Daten manipuliert werden können. Und am Schluss des Kapitel 4 *»Bedrohungen aus dem Netz«* wurde schon gesagt, dass große Organisationen unmöglich ihren IT-Betrieb herunterzufahren können, nur weil jemand den Versuch eines Hacking unternimmt – die Verfügbarkeit der IT-Infrastruktur hat oberste Priorität.

neuKap13.fm Seite 431 Freitag, 18. Oktober 2002 3:52 15

Immer größere Bedeutung erlangen daher aktive Abwehrmechanismen wie Security Audit-Systeme zur Entdeckung und Bewertung von Sicherheitslücken und Intrusion-Detection/Response-Systeme, um angemessen auf Angriffe reagieren zu können, z. B. durch teilweises Herunterfahren. Mithilfe dieser Systeme können außerdem auch interne Angriffe aufgespürt werden.

Am Markt positionieren sich Intrusion-Detection-Systeme, die zwar keinen Schutz vor E-Mail, Netzwerk- und Rechnersystem-basierte Angriffe und Anomalien versprechen, aber Versuche so rechtzeitig erkennen, bewerten und melden, dass eine geeignete Reaktion des Administrators bzw. automatisch durch das IT-System noch vor der eigentlichen Manipulation erfolgen kann.

Analogie zur Videoüberwachung

Mit Systemen zur Videoüberwachung kann man Außenanlagen oder sonstige Teile einer Organisation überwachen; Angriffe sollen frühzeitig erkannt werden. Falls z. B. Eindringlinge den Werkszaun überwinden, wird sofort der Werkschutz oder die Polizei gerufen, um dieser Gefahr unmittelbar entgegenzuwirken. Außerdem kann eine Beweissicherung durch Videoaufzeichnung erfolgen.

13.7.2 Unterscheidung zwischen Detection und Response

Die begriffliche Trennung zwischen Intrusion-Detection und der weitergehenden Intrusion-Response ist nicht einheitlich. Klar ist, dass Systeme zur Intrusion-Detection nach Entdeckung unzulässiger Aktionen im Netz reagieren, sei es durch eine E-Mail oder durch Herunterfahren einer Firewall.

Eine für die Praxis taugliche Unterscheidung zwischen Detection und Response kann nach folgendem Schema vorgenommen werden /Pohl98/:

Intrusion-Detection hat als primäre Ziele die Entdeckung von Angriffen und die Verhinderung von Schaden an den betroffenen Systemen. Das kann durch Alarme, der Umkonfiguration von Systemen oder – falls keine Alternative mehr bleibt – durch Herunterfahren von Systemen (z. B. Firewall-Systeme) geschehen.

Intrusion-Response verfolgt weitergehende Ziele, etwa das Aufspüren des Angreifers. Hier können automatische Tools wie traceroute oder DNS-Anfragen zwar helfen, aber ein geschickter Hacker tarnt sich ausreichend (Spoofing), um diese einfachen Entdeckungsmöglichkeiten auszutricksen. So sind fast immer Maßnahmen des Administrators nötig, wie Kontaktaufnahme mit einer CERT-Organisation oder der Polizei. Auch die rechtlich problematischen – und meist den Falschen treffenden – Gegenangriffe fallen in die Rubrik Intrusion-Response. Wegen des Spoofings treffen z. B. Denial-of-Service-Angriffe auf die IP-Adresse des Hackern meist nur diejenige Universität, bei der er sich letztlich eingeloggt hat. Das Lahmlegen »unschuldiger« Systeme erzeugt böses Blut bei den Administratoren der Systeme und wird kaum deren Hilfsbereitschaft bei der Suche nach den wirklich Schuldigen erhöhen.

neuKap13.fm Seite 432 Freitag, 18. Oktober 2002 3:52 15

Ein wichtiges zukünftiges Ziel für Intrusion Response ist die Flexibilität (**»Flexible Response«**). Wenn der Zugangsrechner eines Großunternehmens ein bestimmtes Angriffsszenario feststellt, unterbindet ein generelles »Dichtmachen« des Zugangs die Verfügbarkeit für alle. Idealerweise würde nur ein bestimmter Dienst abgeschaltet oder eine bestimmte Adresse blockiert.

Im Folgenden wird der Begriff Intrusion-Detection (ID) bzw. Intrusion-Detection-System (IDS) ohne den Zusatz »Response« verwendet.

13.7.3 Einbindung in Firewall-Systeme

Das Intrusion-Detection-System ist eine Ergänzung zu den aktiven Firewall-Elementen und überwacht den Datenverkehr vor und hinter der Firewall. Hierbei sind Netzwerk- und Rechnersystem-basierte Intrusion-Detection-Systeme von Bedeutung:

Netzwerk-basiertes Intrusion-Detection-System

Der Datenstrom wird in Echtzeit auf dem Netzwerk nach Angriffsmustern (Signaturen) untersucht. Alle relevanten Audit-Dateien im Firewall-System werden überwacht und ausgewertet.

Rechnersystemen-basiertes Intrusion-Detection-System

Durch weitere Detektoren (Agents) in den angeschlossenen Rechnersystemen können auch Rechnersystem-basierte Attacken erkannt werden. Auch andere systemrelevante Daten (Log-Files, CPU-Auslastung usw.) werden überwacht. Wird ein Angriff entdeckt, werden auch hier Alarme ausgesendet.

13.7.4 Hauptaufgaben des IDS

Das Ziel der Intrusion-Detection-Systeme ist die Erkennung von Sicherheitsverletzungen und eine angemessene, schnelle Reaktion darauf:

- **Missbrauchserkennung auf der Netzwerkebene**
  Erkennung von Angriffen (Denial of Service, SYN-Flooding, PING-Flooding, Pre Attack Probe (Information über Netzwerk, Angriffe über Portscan-Verfahren (half port, stealth scans))), Angriffe über World Wide Web-Dienste (Active X, Java ...)
- **Rechnersystemen-basierte Angriffserkennung**
  Alle wichtigen Audit-Dateien auf dem System werden überwacht und ausgewertet. Bei Erkennung von Angriffen werden Alarme ausgelöst.
- **Erkennung von Anomalien**
  Erkennung von untypischem System- und Benutzerverhalten

neuKap13.fm Seite 433 Freitag, 18. Oktober 2002 3:52 15

- **Intrusion Response**
  Bei Angriffen können verschiedene Gegenmaßnahmen (z. B. Alarme über E-Mail, SMS, Unterbrechung der Verbindung, Protokollierung des Angriffs) eingeleitet werden.
- **Ereignismeldung (Events)**
  Alle Ereignismeldungen können nach verschiedenen Prioritäten (hoch, mittel, niedrig) zugeordnet und angezeigt werden.
- **Protokollierung/Berichterstellung**
  Es werden Log-Dateien geführt und nach verschiedenen Kriterien ausgewertet (grafische Auswertung).

13.7.5 Aufbau und Funktionsweise von IDS

Intrusion-Detection-Systeme bestehen häufig aus drei Hauptkomponenten: Network Engine (Detektor), Agent und Management. Hierdurch kann auf Netzwerk- und Rechnerebene die Missbrauch- oder Anomalieerkennung umfassend durchgeführt werden. Eine solche Architektur soll im Folgenden beispielhaft für viele reale Implementierungen erläutert werden.

Network Engine

Die **Network Engine (Detektor)** überprüft die Datenpakete in Echtzeit, sendet Alarmmeldungen und trifft automatisch Gegenmaßnahmen (Response). Sie besteht aus fünf Haupteinheiten:

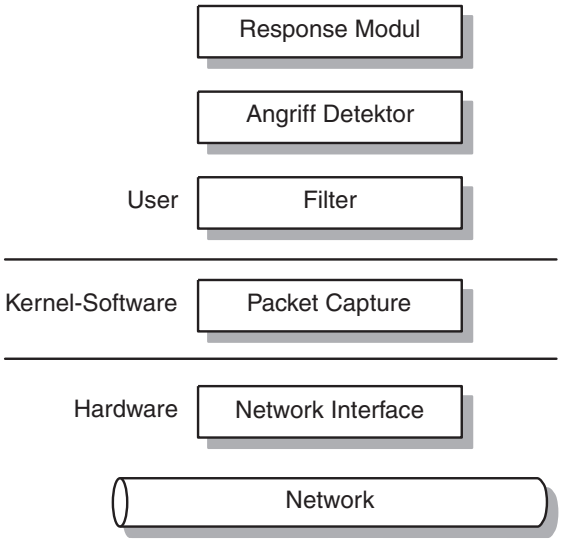


Abb. 13.19: Network Engine: Datenfluss

neuKap13.fm Seite 434 Freitag, 18. Oktober 2002 3:52 15

1. **Netzwerkadapter**

   Die Netzwerkadapter werden im Promiscuous Mode betrieben. Zusätzlich besteht die Möglichkeit, die Network Engine auch im so genannten Transparent Mode zu fahren (keine TCP/IP-Protocol Stacks).

2. **Packet Capture Modul**

   Das Packet Capture Modul organisiert den Transport von Datenpaketen vom Netzwerk zum Auswertemodul der Network Engine.

3. **Filterung**

   Auf der Netzwerk- und Transportschicht – Layer 3 und 4 im OSI-Modell – können Protokolle wie TCP, UDP oder ICMP gefiltert werden. Je nach Einstellung der Sicherheitspolicies werden Quell-IP-Adressen/Ports und Ziel-IP-Adressen/Ports gefiltert. Eine praktische Anwendung ist der parallele Betrieb von zwei Network Engines, hierdurch wird eine Lastverteilung erreicht.

4. **Angriffsdetektor**

   Der Angriffsdetektor untersucht den Datenstrom nach bekannten Angriffsmustern. Hierzu werden die Datenpakete mit vorhandenen Angriffsmustern in der Datenbank (Signaturdatenbank) verglichen. Die Signaturdatenbank enthält alle bekannten Angriffsmuster. Zusätzlich können bestimmte Systemzustände als Angriff definiert werden.

5. **Response Modul**

   Falls ein Angriffsmuster erkannt wird, können verschiedene aktive Gegenmaßnahmen (Responses) wie »Verbindung blocken« oder »Alarm senden« eingeleitet werden:

   - Überwachen aktiver Sessions,
   - Speichern von Sessions,
   - Führen von Log-Dateien,
   - Blockieren von Verbindungen (TCP-Reset).

   Für die Alarmierung stehen verschiedene Dienste zur Verfügung:

   - Alarmmeldung zur Management Console,
   - E-Mail,
   - SMS oder Pager (mit Script) oder Ausführen von benutzerdefinierten Programmen,
   - SNMP-Trap, z. B. an ein Tivoli-Überwachungssystem.

Agent

Der Agent überwacht alle Systemaktivitäten eines Rechnersystems im Netz. Alle vom Betriebssystem oder einzelnen Applikationen erzeugten Auditdaten werden

neuKap13.fm Seite 435 Freitag, 18. Oktober 2002 3:52 15

auf mögliche Angriffe und nach evidenten anormalen Ereignissen untersucht. Auch alle systemrelevanten Daten (Log-Files, CPU-Auslastung usw.) können überwacht werden, bei Entdeckung von Angriffen werden auch hier Alarme ausgesendet.

Es können alle User-LogOns und User-LogOffs überwacht werden. So kann ein nicht genehmigter Zugang verhindert werden. In diesem Rahmen können auch alle Aktivitäten des Administrators überwacht werden. Auch wichtige Dateien (Key System Files) können überwacht werden, somit kann die Manipulation dieser Dateien verhindert und die Installation von trojanischen Pferden verhindert werden. Die Parameter wie CPU-Auslastung oder Anzahl aktiver Netzverbindungen werden ausgewertet.

Die Erkennung von Anomalien hat das Ziel, die unmittelbaren Folgen eines Angriffs zu erkennen. Dadurch kann das System auch vor unbekannten Angriffen geschützt werden.

Management

Das IDS-Management (IDM) administriert und konfiguriert die Network Engines (Detektoren) und den Agent. Auch die Updates erfolgen über das Management. Die Kommunikation zwischen Network Engine und Management erfolgt verschlüsselt (symmetrisch bis 128 Bit oder asymmetrisch 1024 Bit).

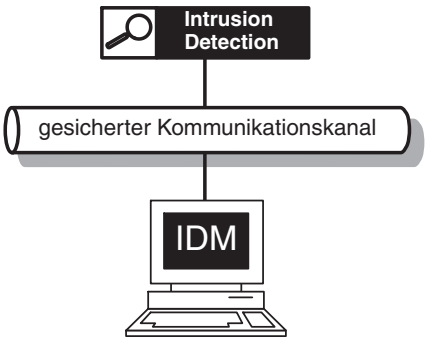


Abb. 13.20: Kommunikation mit dem ID-Management

Das IDS-Management bildet eine Sammelstelle für alle von Network Engine und Agent gesendeten Events. Auch die Log-Dateien werden vom Management abgeholt und ausgewertet. Die Angriffe können protokolliert werden, so können Informationen über Bedrohungen für Informations- und Risikomanagement zur Verfügung gestellt werden. Über das Management werden Berichte und Statistiken erstellt. Anhand dieser Berichte und Statistiken können Sicherheitspolicies im gesamten Netzwerk angepasst werden.

neuKap13.fm Seite 436 Freitag, 18. Oktober 2002 3:52 15

13.7.6 Auswertekonzepte

Im Folgenden werden drei Konzepte zur Auswertung sicherheitsrelevanter Ereignisse vorgestellt und danach verglichen.

Erkennen von bekannten sicherheitsrelevanten Aktionen

Nach diesem Auswertungskonzept wird vorab festgehalten, welche bereits bekannten und hypothetischen sicherheitsrelevanten Ereignisse oder welche Folgen von sicherheitsrelevanten Ereignissen eine Sicherheitsverletzung darstellen. Die Protokolldaten in den Logbüchern werden dann mithilfe eines Expertensystems nach solchen bekannten Ereignissen oder Ereignisfolgen, die in der Wissensbasis festgehalten sind, untersucht.

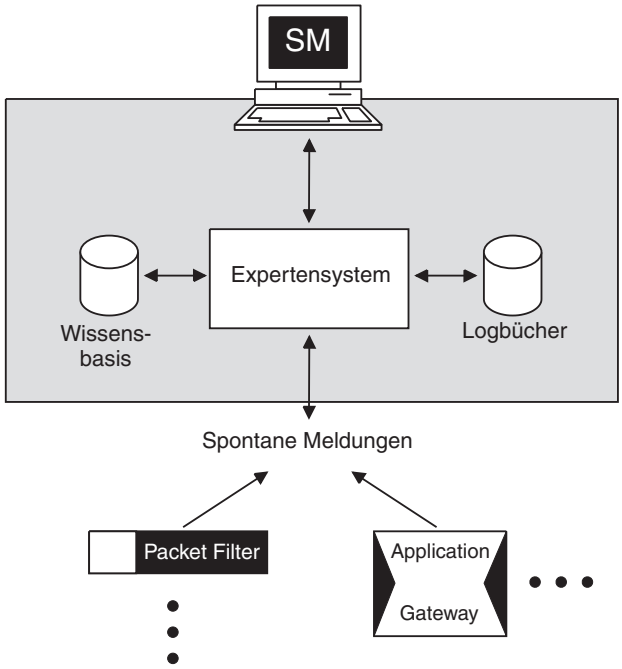


Abb. 13.21: Erkennen von bekannten sicherheitsrelevanten Aktionen

Beispiele für sicherheitsrelevante Angriffe

- fehlerhafte Authentikation eines Benutzers mit dem Firewall-System
- jemand verwendet den Befehl »debug« → (SMTP-Proxy)
- jemand versucht einen Hopping-Angriff → (Telnet-Proxy)
- Verwendung des Befehls »del«, obwohl dieser verboten wurde → (FTP-Proxy)

neuKap13.fm Seite 437 Freitag, 18. Oktober 2002 3:52 15

- Adressierung eines nicht initialisierten Port des Application Gateway, obwohl dieser im Packet Filter als »nicht erlaubt« definiert ist (Application Gateway bei einer High-level-Security-Konfiguration)
- nicht erlaubter Versuch eines Verbindungsaufbaus zu einem Rechnersystem im zu schützenden Netz

Festlegen der sicherheitsrelevanten Ereignisse und Ereignisfolgen, die als Angriffe gewertet werden

Bei dieser Methode der Erkennung von Sicherheitsverletzungen kann es ein Problem sein, zu entscheiden, in welchem Fall eine Ereignisfolge als Angriff bewertet werden muss.

Beispiel einer möglichen Strategie

Bei der Authentikation eines Benutzers gegenüber dem Firewall-System oder bei der Kontrolle der Befehle, die über FTP ausgetauscht werden, können durchaus auch Fehler passieren. Für solche sicherheitsrelevanten Ereignisse könnte z. B. die folgende Regel aufgestellt werden:

- Wenn ein Benutzer einmal einen Fehler macht, wird dieser als Versehen bewertet;
- falls der Benutzer zweimal eine falsche Aktion durchführt, wird dies als unglücklicher Zufall bewertet;
- falls der Benutzer aber dreimal dieselbe falsche Aktion innerhalb eines bestimmten Zeitraumes durchführt, wird diese Ereignisfolge als Angriff bewertet, und entsprechende Schritte werden eingeleitet.

Erkennen von Anomalien

Bei diesem Auswertungskonzept sollen über das Erkennen von Anomalien – eine Abweichung vom Normalen – Sicherheitsverletzungen entdeckt werden. Dieses Konzept basiert auf der Annahme, dass Sicherheitsverletzungen anhand gravierender Verhaltensabweichungen erkannt werden können. Solche Verhaltensabweichungen werden auf einzelne Benutzer, auf einzelne Programme, auf bestimmte Dienste oder auch auf Kommunikationsabläufe bezogen erkannt.

Grundlage der Anomalie-Erkennung ist die Beschreibung des »normalen«, für einen Aspekt typischen, regulären Verhaltens in so genannten Referenzprofilen. Diese Referenzprofile sind charakteristische Verhaltensmuster, die anhand von objektiv überprüfbaren Merkmalen beschrieben werden. Diese Merkmale können dann entweder mithilfe von Statistiken über das tägliche Verhalten oder aufgrund individueller Erfahrungswerte ausgewählt werden /Sobi99/.

neuKap13.fm Seite 438 Freitag, 18. Oktober 2002 3:52 15

Beispiele von Anomalien bei der Nutzung von Firewall-Systemen

- überdurchschnittliche Fehlerrate bei der Identifikation und Authentikation
- Art und Umfang der Inanspruchnahme von Diensten (FTP, Telnet, SMTP, HTTP, ...)
- überdurchschnittliche lange Zeit, die Benutzer über das Firewall-System arbeiten
- außergewöhnliche Zeiten, Wochentage, wann und wie über das Firewall-System kommuniziert wird
- überdurchschnittlich häufiges Auftreten von sicherheitsrelevanten Ereignissen
- Verstoß gegen das Regelwerk
- Angriffsversuche auf das Firewall-System
- Fehlverhalten der Firewall-Software und -Hardware

Bei dem Konzept der Erkennung von Sicherheitsverletzungen durch Anomalien werden die Protokolldaten der Logbücher analysiert und aufbereitet, damit sie mit den Referenzprofilen verglichen werden können. Ist die Abweichung zu groß, wird eine Sicherheitsverletzung angenommen und die notwendigen Schritte werden eingeleitet (siehe unten).

Wichtig bei dieser Methode ist, dass bei Referenzprofilen nicht nur die typische Verhaltensweise anhand konkreter Merkmale beschrieben wird, sondern dass auch festgelegt werden muss, wie stark die tolerierbare Abweichung sein darf, welche (gewichtete) Bedeutung Abweichungen bei einzelnen Merkmalen für das Gesamtergebnis der Analyse haben und wie viele solcher Abweichungen in welchen Kombinationen registriert werden müssen, ehe man davon ausgehen kann, dass eine Sicherheitsverletzung vorliegt.

- in einem bestimmten Zeitrahmen wurden überdurchschnittlich viele Fehlauthentikationen unterschiedlicher Benutzer festgestellt
- zu einer ungewöhnlichen Zeit finden überdurchschnittlich viele Aktivitäten statt (sonntags zwischen 3.00 und 6.00 Uhr)
- überdurchschnittlich viele Versuche, mit nicht erlaubten Rechnersystemen eine Verbindung aufzubauen, wurden erkannt und registriert

Diese Erkenntnisse können auf einen massiven Angriffsversuch oder sogar auf einen schon erfolgten Angriff schließen lassen.

Ein Problem bei solchen Erkennungssystemen ist die Feinabstimmung. Bei Überempfindlichkeit würden zu häufig Fehlalarme verursacht, und bei zu großzügigen Toleranzabweichungen verringert sich die Wahrscheinlichkeit, dass Sicherheitsverletzungen durch Anomalien erkannt werden.

Einige IDS, die Anomalien aufspüren können, arbeiten mit **neuronalen Netzen**, denen als Eingabeparameter System- und Netzwerkaktivitäten zugeführt werden. In einer (möglichst ungestörten) Lernphase werden Benutzer- und Rechnerprofile gebildet, die dann im regulären Betrieb überprüft werden.

neuKap13.fm Seite 439 Freitag, 18. Oktober 2002 3:52 15

Vergleich der verschiedenen Auswertungskonzepte

Beim Auswertungskonzept »Erkennen von bekannten sicherheitsrelevanten Aktionen« erhält man als Ergebnis klare Aussagen darüber, ob und welche Sicherheitsverletzung auftrat und erkannt wurde. Daraufhin können definierte Reaktionen eingeleitet werden.

Das Auswertungskonzept »Erkennen von Anomalien« hat den großen Vorteil, dass es durch die Art der Analyse von Protokolldaten der Logbücher gelingen kann, auch bislang unbekannte Sicherheitsverletzungen aufzuspüren, die von der direkten Angriffserkennung als solche nicht klassifiziert werden konnten. Damit kann dem Problem vorgebeugt werden, dass es sehr schwierig sein wird, ständig Informationen über neueste, hochaktuelle Angriffszenarien in Erfahrung zu bringen, diese zu analysieren, und für die direkte Angriffserkennung zu modellieren und in der Wissensbasis festzuhalten. Ein Nachteil dieses Auswertungskonzeptes ist, dass auch Fehlalarme generiert werden.

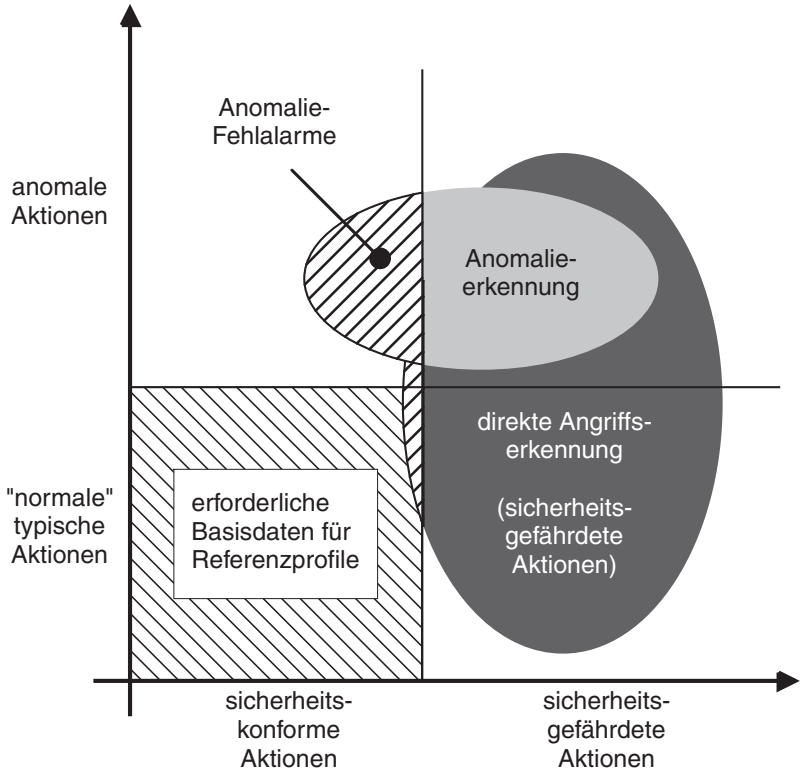


Abb. 13.22: Erkennen von Anomalien

neuKap13.fm Seite 440 Freitag, 18. Oktober 2002 3:52 15

Die Abbildung zeigt deutlich, dass mehr sicherheitsgefährdende Aktionen erkannt werden, wenn beide Auswertungskonzepte gleichzeitig eingesetzt werden. Es wird ebenfalls dargestellt, wie anomale Aktionen erkannt werden, die keine Gefährdung der Sicherheit bedeuten, aber Fehlalarme auslösen.

13.7.7 Grenzen von IDS

Leider gibt es nirgendwo eine hundertprozentige Sicherheit, auch nicht bei Systemen zur ID. Zu jedem Verfahren zur ID sind (zumindest theoretisch) raffinierte Angriffsszenarien denkbar, die vom IDS nicht entdeckt werden können. Ist der Typ des IDS dem Hacker bekannt, hat er reelle Chancen zum Angriff. Aber selbst bei unbekannten Systemen kann immer noch versucht werden, das IDS selbst mittels eines Denial-of-Service-Angriffs »abzuschießen« und dann ohne den lästigen Kontrolleur im Netz zu »wildern«. Andere Angriffsmöglichkeiten ergeben sich durch

- Angriffe, die im statistischen Grundrauschen des IDS untergehen, wie etwa der so genannte slow-scan, ein Portscan, der sich über Wochen und Monate erstreckt,
- Beimischung von deformierten Netzwerkpaketen in den Angriff. Diese Pakete stören die Mustererkennung des IDS und werden im günstigen Fall vom angegriffenen Zielsystem verworfen, sodass sich wieder der ursprüngliche Angriff ergibt,
- Manipulation der Anomalieentdeckung durch langsame Verschiebung der Profile; der Selbstlernmechanismus vieler IDS (neuronale Netze!) unterstützt dieses Vorgehen. So kann der Buchhalter Müller durch langsame Verschiebung seines Benutzerprofils in die Abendstunden nach einigen Wochen vielleicht seinen entscheidenden Angriff auf den Lohn-Server starten, ohne dass das IDS Alarm auslöst.

In jedem Falle stellt die Kombination Firewall/IDS für Angreifer eine große Hürde da, sodass in der Regel Angriffe auch entdeckt werden.

Das liegt zum einen daran, dass die meisten Hacker als so genannte »Script-Kiddies« nur bereits bekannte Angriffe (aus Internet-Quellen) wiederholen, die von einem gut gepflegten IDS natürlich entdeckt werden. Zum anderen kann sich ein Angreifer nicht so zielgerichtet in einem nicht vollständig bekannten Netz bewegen, wie er das zur Überlistung eines IDS tun müsste. Ein winziger Fehler, und der Alarm wird ausgelöst. Ein kleines Restrisiko bleibt natürlich, aber fehlerlose Hacker gibt es nur im Film (siehe auch *»Theoretische Grundlagen von Firewall-Systemen«*, Kap. 14.5.12 und 14.6).

neuKap13.fm Seite 441 Freitag, 18. Oktober 2002 3:52 15

13.8 DDoS-Angriffe – Beschreibung und Bewertung

Bereits seit einigen Jahren treten im Internet so genannte »Denial of Service«-Angriffe (DoS) auf, die Schwachstellen in der Implementierung der Netzwerkfunktionalität verschiedener Betriebssysteme ausnutzen. Die zum Teil drastischen Auswirkungen auf die Verfügbarkeit der Zielsysteme – in Verbindung mit einer freien Zugänglichkeit entsprechender Tools – erzwangen eine sehr zeitnahe Reaktion der Hersteller der Betriebssysteme und der Administratoren vor Ort. Die auch heute noch wirksamen Gegenmaßnahmen bestehen im Einspielen entsprechender Patches sowie der Aktivierung bzw. Installation von Paketfiltern auf vorgeschalteten IT-Sicherheitskomponenten/BSI00/.

Die im Verlauf des Jahres 1999 sowie zu Beginn des Jahres 2000 bekannt gewordenen »Distributed Denial of Service« (DDoS) – Angriffe stellen aufgrund einer verteilten Arbeitsweise unter Nutzung einiger weniger Master und einer Vielzahl so genannter Agenten, die mehrere konventionelle DoS-Angriffsvarianten kombinieren – mithin eine Vervielfachung der Schadenswirkung erzielen – eine neue Qualität dar. Nur durch eine koordinierte Zusammenarbeit der verantwortlich Beteiligten bei Prävention und Reaktion kann diesem Gefahrenpotenzial angemessen und wirkungsvoll begegnet werden.

13.8.1 Allgemeine Funktionsweise der DDoS-Angriffe

Der Ablauf eines DDoS-Angriffs kann in zwei Phasen unterteilt werden. Während in Phase 1 mittelbar unter Einsatz automatisiert ablaufender Tools in kompletten Netzwerkbereichen versucht wird, DDoS-Agenten zu installieren, werden die erfolgreich hinterlassenen und aktiviert im Hintergrund laufenden DDoS-Agenten in Phase 2 von einem zentralen Master unmittelbar angewiesen, ein gemeinsames Zielsystem anzugreifen.

Phase 1:

Beginnend mit einem Subnet-Scan eines Netzwerkbereichs in Verbindung mit Auswertung und Feststellung der eingesetzten Betriebssystemvarianten sowie einer Analyse der Versionen aktivierter Dienstprogramme versucht ein Angreifer – der bereits jetzt das eigentliche Ursprungssystem in Form einer Workstation unter Einbeziehung von unter Umständen mehreren Relay-Systemen sehr effektiv verbergen kann – mittels so genannter Exploits (Programme, die eine vorhandene Schwachstelle auf einem Zielsystem ausnutzen, um sich dort missbräuchlich privilegierte Rechte zu verschaffen) die oben erwähnten DDoS-Agenten zu installieren (siehe Bild). Nicht beseitigte Schwachstellen und nicht vorhandene bzw. nicht adäquat konfigurierte Firewall-Systeme – mithin eine problemlose nicht authentisierte Kontaktierung interner Netzbereiche – stellen hier die Hauptursachen für den häufigen Erfolg in dieser Phase dar. Einen Abschluss findet die

neuKap13.fm Seite 442 Freitag, 18. Oktober 2002 3:52 15

erste Phase mit der ebenfalls automatisch, d.h. ohne direkte Interaktion des Angreifers, stattfindenden Registrierung der DDoS-Agenten bei einem oder mehreren Master-Systemen. Darüber hinaus kann der Angreifer so genannte »rootkits« installieren, um die Spuren des Eindringens zu beseitigen und die auffällige Sichtbarkeit des DDoS-Agenten-Prozesses gegenüber den Administratoren dieses Systems zu verbergen. Eine Konsequenz aus dieser Vorgehensweise kann eine relativ lange Karenzzeit zwischen dem Ende der Phase 1 und dem Beginn des Angriffs in Phase 2 sein. In dieser Zeitspanne besteht jedoch die Möglichkeit, anhand spezifischer Signaturen diese missbräuchlich installierten DDoS-Agenten aufzuspüren und administrativ zu terminieren.

Eine alternative Vorgehensweise für die Installation von DDoS-Agenten besteht im vergleichsweise einfachen Programmieren und Versenden trojanischer Pferde (z.B. per E-Mail). Organisatorische Vorkehrungen im Rahmen des IT-Sicherheitskonzepts in Verbindung mit der Durchführung qualifizierter Mitarbeiterschulungen sind an dieser Stelle zwingend erforderlich, um die missbräuchliche Ausführung unbekannter Programme zu unterbinden. Eine weitere, nicht auszuschließende Alternative für die Installation eines DDoS-Agenten besteht in der Ausnutzung von Implementationsschwachstellen hinsichtlich Interpretation und Ausführung so genannter Active-Contents auf einem Arbeitsplatz-PC.

Zur Verhinderung dieser Angriffsvariante können z.B. Personal Firewalls verwendet werden.

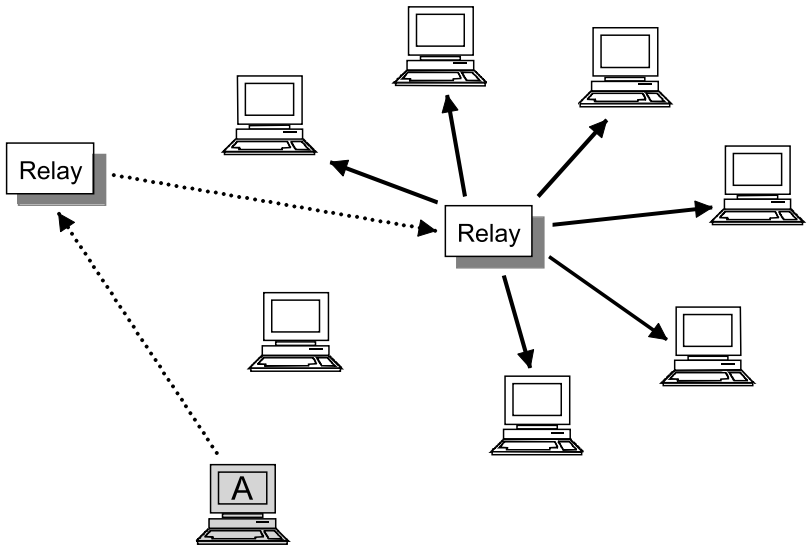


Abb. 13.23: Phase 1: Installation der DDoS-Agenten

neuKap13.fm Seite 443 Freitag, 18. Oktober 2002 3:52 15

Phase 2:

Nach Registrierung der DDoS-Agenten in Phase 1 kann der Master auf ein gezieltes Kommando des Angreifers hin veranlasst werden, mittels Absendung entsprechender Befehlssequenzen zu allen DDoS-Agenten, die dann stellvertretend die eigentlichen DoS-Pakete aussenden, einen verteilten Angriff auf ein gemeinsames Zielsystem zu initiieren (siehe Abbildung 13.24).

Zum Einsatz kommen neben den bereits genannten DoS-Angriffsmethoden auch Varianten, die über die Assemblierung zufälliger UDP-, TCP-, und ICMP-Datenpakete (so genannte core data flooding) eine massive Überflutung des Zielsystems bzw. der vorgeschalteten Netzwerkinfrastruktur zur Folge haben können.

Die Kommunikation zwischen Master und DDoS-Agent findet mit zunehmender Tendenz über Protokolle statt, die selbst bei Vorhandensein eines Filtersystems oft freigeschaltet werden. Als Beispiel sei hier die Verwendung von ICMP-Echo-Replies angeführt, die nicht selten von Paketfiltern als normale Antworten auf entsprechende Anfragen interpretiert und in ein internes Netzwerk weitergeleitet werden. Eine restriktive Konfiguration derartiger Filterkomponenten kann hier eine wirksame präventive Maßnahme zur Verhinderung der Kommunikation zwischen Master und DDoS-Agent sein.

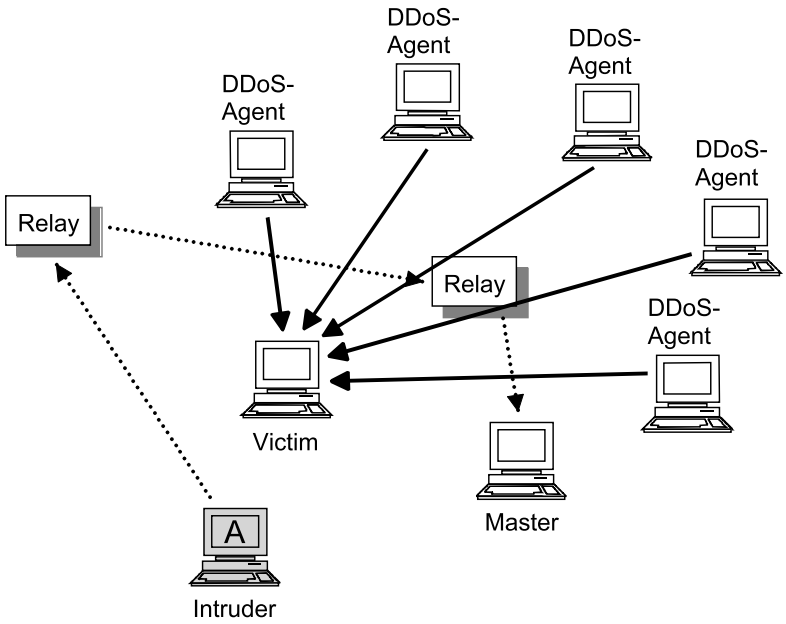


Abb. 13.24: Phase 2: Initiierung und Ausführung des Angriffs auf ein gemeinsames Zielsystem

neuKap13.fm Seite 444 Freitag, 18. Oktober 2002 3:52 15

13.8.2 Weitere Entwicklung der DDoS-Tools

In zunehmenden Maße ist weiterhin zu beobachten, dass nicht nur für die Kommunikation zwischen Master und DDoS-Agent, sondern auch für die Kommunikation zwischen Angreifer und Master einfache, in der Regel symmetrische Verschlüsselungsverfahren eingesetzt werden. Eine zusätzlich zu beobachtende Tendenz besteht in der Nutzung alternativer Protokolle für die Kommunikation zwischen Angreifer, Master und Agenten. Eine potenziell von einem Intrusion-Detection-System durchgeführte Signatur-Analyse wird in diesen Fällen massiv erschwert.

Neuere DDoS-Tools werden die Möglichkeit für ein zentral gesteuertes, weitestgehend automatisch ablaufendes Update aufweisen.

13.8.3 Zusammenfassende Bewertung

Wirksame reaktive Maßnahmen vor Ort zum Zeitpunkt eines DDoS-Angriffs stehen unter folgenden Bedingungen zur Verfügung /BSI00/:

a) Der Angriff wird richtig als DDoS-Angriff erkannt.
b) Der DDoS-Angriff basiert auf Protokollen, die nicht unmittelbar für den Wirkbetrieb benötigt werden und damit effektiv durch vorgeschaltete Filter-Komponenten blockiert werden können.
c) Das Blockieren von DDoS-Angriffen, die auf für den Wirkbetrieb zwingend erforderlichen Protokollen basieren, ist nur möglich, wenn die Varianz der Absender-Adressen nicht zu groß ist. Diese Bedingung ist insbesondere bei TCP-ACK-Flooding mit gefälschten und zufällig gesetzten Absender-IP-Adressen nicht gegeben, weshalb hier ein hohes Schadenspotenzial absehbar ist (z. B. bei dem neuen DDoS-Tool »mstream«).
d) In Kooperation mit dem jeweiligen Internet-Provider werden hinsichtlich des eintreffenden Datenverkehrs die DDoS-Pakete möglichst früh auf vorgeschalteten Filter-Komponenten (oft eine Funktionalität von IP-Routern) blockiert. Sehr oft stehen die entsprechenden Rechenkapazitäten und Leitungsbandbreiten nur bei den Internet-Providern zur Verfügung.
e) Bereits im Vorfeld wurden präventiv Betriebssystem-Patches installiert (z. B. gegen SYN-Flooding).
f) Die Administratoren sind für die IT-Sicherheitsproblematik sensibilisiert und sind im Fall eines Angriffes in der Lage, in Zusammenarbeit mit den Internet-Providern bereits vorher definierte Gegenmaßnahmen einzuleiten.

13.8.4 Bisher unbekannte Aspekte

Nur unter Kenntnis konkreter Auswirkungen und getroffener Gegenmaßnahmen vor Ort ist eine detaillierte Auswertung der Angriffe möglich. Die Beantwortung folgender zum großen Teil bisher noch offener Fragen ist dafür notwendig:

neuKap13.fm Seite 445 Freitag, 18. Oktober 2002 3:52 15

a) Welche Netzwerkkomponenten beziehungsweise Rechnersysteme sind vor Ort am stärksten betroffen gewesen? Welche Komponenten sind ausgefallen?
b) Wie lange hat es gedauert, bis der Angriff erkannt wurde?
c) Welche Hilfsmittel standen zur Erkennung des Angriffs zur Verfügung (z. B. IDS/IRS)?
d) Wie lange hat es gedauert, bis der Angriff richtig klassifiziert wurde?
e) Welche Gegenmaßnahmen wurden bereits präventiv im Vorfeld ergriffen (z. B. Einrichtung von Paketfiltern in Zusammenarbeit mit dem Internet-Provider)?
f) Welche zusätzlichen Gegenmaßnahmen wurden auf welchen Systemkomponenten nach Erkennung des Angriffs eingeleitet?
g) Wie lange nach Aktivierung der Gegenmaßnahmen lief der Angriff noch weiter?
h) Wurde der Angriff erfolgreich abgewehrt?
i) Welche Organisationen wurden in die Angriffsbehandlung einbezogen?
k) Welche Spuren des Angriffs wurden für eine spätere technische und juristische Auswertung gesichert?
l) Über welchen Zeitraum lief die Vorbereitung der Angriffe?
m) Wie viele DoS-Agenten waren am konkreten Angriff beteiligt?
n) Wie waren die DoS-Agenten verteilt? Welche Organisationen und Netzwerkbereiche waren betroffen? Wo lagen die Schwerpunkte (z. B. Firmen, Behörden, Universitäten, Privatanwender etc.)?

13.9 Personal Firewall

13.9.1 Risiken bei der Internet-Anbindung

Die Nutzung des Internets ist in vielerlei Hinsicht attraktiv. Ein gravierender Nachteil ist aber die Sicherheitsfrage. Insbesondere sind folgende Risiken zu berücksichtigen:

- **Zugriff auf wertvolle Informationen einer Organisation**
  Die Kopplung an das Internet ist keine Einbahnstraße. Alle, die an das Internet angeschlossen sind, können prinzipiell direkt oder indirekt auf das angeschlossene Rechnersystem und die darauf gespeicherten Ressourcen zugreifen (siehe ① + ④ in der folgenden Abbildung: Mobile und Telearbeitsplätze oder Rechnersysteme, die an dem zentralem Firewall-System vorbei auf das Internet zugreifen).

- **Empfangen von Malware (Hostile Code, Schadprogramme)**
  Ein Angreifer, der eine Organisation schädigen möchte, sendet Malware (Viren, trojanische Pferde, Würmer, etc.). In der Folge erleidet die Organisation eine Reduzierung ihrer Werte, einen Schaden z. B. durch die Zerstörung von Dateien (siehe ③). Das Senden dieser Malware kann auch im Rahmen der erlaubten Kommunikation über das zentrale Firewall-System erfolgen. Typischerweise wird die Malware mit Anhängen an Mails oder innerhalb von WWW-Dokumenten (Java Applets, Active-X-Controls und andere Executables) an die Rechner-

neuKap13.fm Seite 446 Freitag, 18. Oktober 2002 3:52 15

systeme gesandt. Active-X-Controls haben z.B. unbegrenzte Funktionalitäten. Sie können z.B. einen PC herunterfahren, Dateien löschen oder beliebige andere Funktionen ausführen und damit Schaden anrichten.

- **Cookies und Cache**
  Cookies werden von den Websites, die ein Benutzer besucht hat, auf die PC-Festplatte des Benutzers gespeichert, damit die Aktivitäten des Benutzers zurückzuverfolgen sind und damit der Benutzer langfristig optimal vom Website-Anbieter bedient werden kann. Diese vertraulichen, privaten Informationen können aber auch von Betreibern anderer Websites über Java oder ActiveX abgerufen werden, das Verhalten des Benutzers kann analysiert und dieses Wissen möglicherweise für kriminelle Zwecke genutzt werden.

  Im Cache befinden sich HTML-Dateien, die beim Zugriff auf eine Website automatisch heruntergeladen und auf dem Rechner des Benutzers gespeichert werden. Neben der Platzverschwendung auf der Festplatte können die HTML-Dateien zur Überwachung des Verhaltens des Benutzers missbraucht werden.

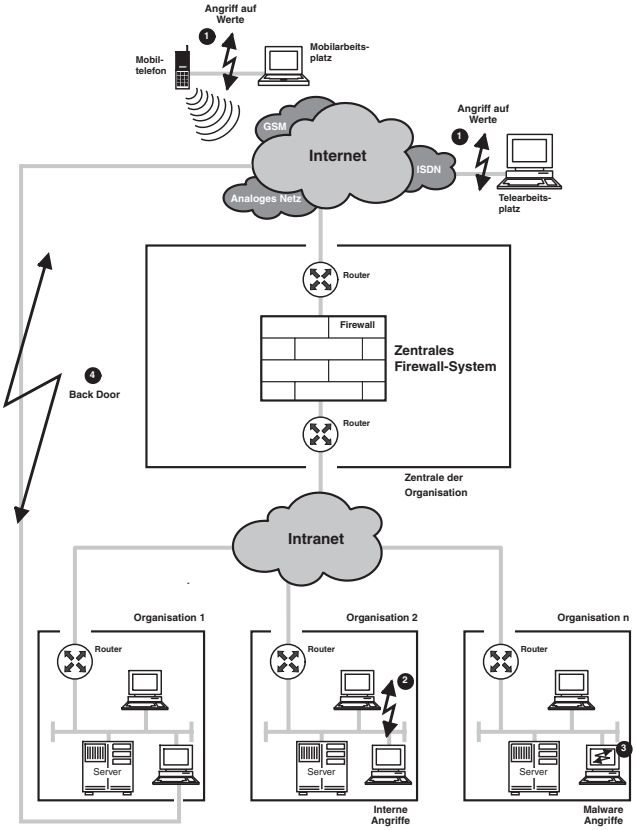


Abb. 13.25: Risiken bei der Internet-Anbindung

neuKap13.fm Seite 447 Freitag, 18. Oktober 2002 3:52 15

Trotz der vielfältigen Gefahren sollten oder müssen Unternehmen die Chancen der Internetanbindung nutzen. Zur Verdeutlichung der Situation mag folgende Analogie dienen:

Angesichts einer grassierenden Grippewelle oder anhaltend schlechten Wetters stehen jedem Einzelnen verschiedene Verhaltensweisen zur Verfügung: Im Schutze des eigenen Hauses zu bleiben, vor die Tür zu gehen und sich ungeschützt dem Risiko der Ansteckung aussetzen oder sich mit viel »Vitamin C« zu versorgen, um so die Steigerung der Abwehrkräfte zu erzielen. Die letztgenannte Variante schafft die Freiheit, dorthin zu gehen, wohin man will und reduziert die Möglichkeit der Infektion mit Viren.

Die Personal Firewall ist ein dem »Vitamin C« vergleichbares Schutzschild für den PC und stellt eine sinnvolle Ergänzung zu anderen Sicherheitsmechanismen für Unternehmen und Organisationen, also üblicherweise zu zentralen Firewall-Systemen und Virenscannern, dar.

13.9.2 Zentrales Firewall-System

Ein zentrales Firewall-System ist ein außergewöhnlich effektiver Sicherheitsmechanismus zum Schutz von Netzen. Das zentrale Firewall-System analysiert die Kommunikationsdaten und kontrolliert die Kommunikationsbeziehungen sowie die Kommunikationspartner. Außerdem reglementieren die Sicherheitsdienste eines zentralen Firewall-Systems die Kommunikation gemäß einer organisationsspezifischen Sicherheitspolitik, kontrollieren alle sicherheitsrelevanten Ereignisse und alarmieren bei Verstößen den Security Administrator. Ein zentrales Firewall-System stellt den Common-Point-of-Trust zwischen unterschiedlichen Netzen dar. Die Idee eines zentralen Firewall-Systems besteht darin, nur einen Weg vom zu schützenden in das ungeschützte Netz und umgekehrt zu gestatten und diesen einen Zugang zuverlässig und effektiv zu kontrollieren.

Es gibt aber auch konzeptionelle Grenzen eines zentralen Firewall-Systems, denen mit anderen technischen oder auch nicht-technischen Sicherheitsmechanismen entgegengewirkt werden muss:

- **Back Door**
  Konzeptionelle Grenzen eines zentralen Firewall-Systems beruhen in erster Linie auf so genannten Hintertüren (back doors). Da das Firewall-System nur Kommunikationsverbindungen schützt, die über das Firewall-System geleitet werden, greift dieser Schutz naturgemäß nicht, wenn Kommunikationsübergänge auch am Firewall-System vorbei möglich sind. In ④ (siehe letzte Abbildung) greift z. B. ein Benutzer über die Telefonanlage und einen Internetprovider an dem zentralen Firewall-System vorbei ins Internet.

neuKap13.fm Seite 448 Freitag, 18. Oktober 2002 3:52 15

- **Interne Angriffe**
  Ein zentrales Firewall-System bietet Sicherheitsdienste zur Abschirmung gegen das unsichere Netz oder zur Kontrolle der Kommunikation zwischen dem unsicheren Netz und dem zu schützenden Netz. Das zentrale Firewall-System allein bietet keinen Schutz vor internen Angriffen (siehe ②).
- **Malware-Angriffe auf Datenebene**
  Eine zentrales Firewall-System ist ursprünglich nicht in der Lage, im Bereich der erlaubten Kommunikation Angriffe auf der Datenebene zu erkennen. Dazu gehören: Angriffe durch das Senden von Malware wie E-Mail-Attachments, Downloads vom Web, Java Applets und Active-X-Controls (siehe ③).

13.9.3 Virenscanner

Zur Erkennung von Viren gibt es so genannte Virenscanner, die zentral oder auf einzelnen Rechnersystemen nach bekannten Viren suchen. Falls in einer Datei ein Virus erkannt wurde, zeigen sie dieses sicherheitsrelevante Ereignis an.

Auch bei Virenscannern gibt es konzeptionelle Grenzen:

- Virenscanner finden nur Viren, die sie bereits kennen. Das generelle Problem bei der Virenerkennung ist die mangelnde Aktualität der Programme. Zu der Vielzahl bestehender Viren kommen praktisch täglich neue hinzu, der Virenscanner kann die Neuentwicklungen nicht erkennen. Folge: Es ist kein hundertprozentiger Schutz vor Viren gegeben. Das Problem steigt bei der Datenübertragung, hier ist die Erkennungsrate von Viren noch geringer.
- Wird der Virenscanner zentral eingesetzt, müssen komprimierte Daten immer noch zuerst dekomprimiert werden, um geprüft zu werden. Verschlüsselte Daten können gar nicht geprüft werden.
- Ein Virenscanner kann nicht »ausprobieren«, ob eine Datei mit einem Virus etwas Schädliches tut.

13.9.4 Ziel einer Personal Firewall

Ziel einer Personal Firewall ist es, die konzeptionellen Lücken (z. B. »Back Doors«, »Interne Angriffe« und »Malware-Angriffe auf Datenebene«) zu schließen, die bei einem zentralen Firewall-System und bei den bekannten Virenscannern noch vorhanden sind /Pohl2000a/.

Für Tele- und Mobil-Arbeitsplätze ist die Personal Firewall das Firewall-System beim Anschluss an das Internet.

Die Personal Firewall (auch Desktop-Firewall, dezentrale Firewall oder distributed Firewall genannt) ist auf dem PC (Notebook oder Desktop) installiert und schützt ihn umfassend vor Zugriffen aus dem Netz und vor Bedrohungen, die im Rahmen der erlaubten Kommunikation durch bösartige Inhalte gesendeter Daten (Malware, Mobile Codes) entstehen können.

neuKap13.fm Seite 449 Freitag, 18. Oktober 2002 3:52 15

Dazu wird neben der Reglementierung der Kommunikation auf dem PC eine sichere Umgebung nach dem Sandbox-Modell realisiert, um jede Anwendung, die innerhalb des Betriebssystem läuft, zu isolieren. Alle schützenswerten Systemressourcen und Dateien können gegen unerwünschte Zugriffe durch lokale Applikationen oder Malware, die in das System eindringen, abgeschirmt werden.

Die Architektur einer Personal Firewall ist so aufgebaut, dass die Sicherheitsmechanismen in der Lage sind, den Zugriff auf schützenswerte Ressourcen innerhalb des Anwendungs- und Benutzerkontextes zu beschränken. Die Sicherheitsmechanismen sind transparent in das Betriebssystem eingebunden und nutzen deren Programme, DLLs und Kernel-Gerätetreiber. Somit können alle Ereignisse überwacht und ein Maximum an Betriebssicherheit und Kompatibilität erreicht werden.

13.9.5 Komponenten

Der »Agent« ist die Benutzerschnittstelle zur Personal Firewall und zeigt dem Benutzer Statusinformationen an. Er überwacht bestimmte Zugriffe auf die Rechnerumgebung und die Ressourcen /Pohl2000b/.

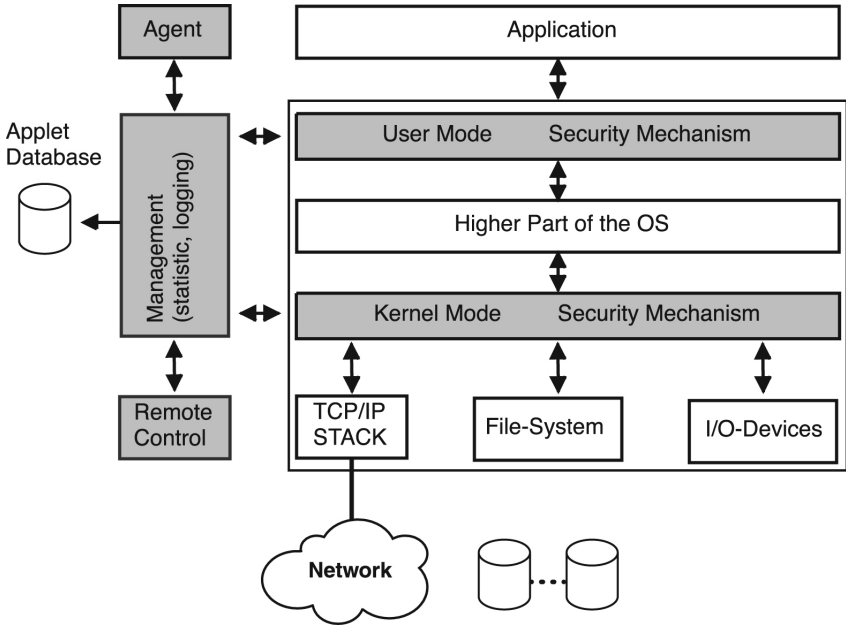


Abb. 13.26: Architektur einer Personal Firewall

Der »User Mode Security Mechanism« bietet Schutzmaßnahmen auf höherer Ebene und schützt die Laufzeitumgebung benutzerorientiert.

neuKap13.fm Seite 450 Freitag, 18. Oktober 2002 3:52 15

Der »Kernel Mode Security Mechanism« bietet erweiterte Schutzmaßnahmen auf niedriger Ebene und schützt die Laufzeitumgebung. Eine Einbindung in die Kernel-Ebene ermöglicht eine maximale Kontrolle.

Das »Remote Control Module« erlaubt es, über ein zentrales Security Management die Sicherheitspolitik einer Organisation einfach umzusetzen.

Im »Management Module« werden die Ereignisse analysiert, protokolliert und Statistiken berechnet. Außerdem ist im Management Module typischerweise eine Cache- und Cookie-Verwaltung realisiert, mit deren Hilfe die Benutzung gesteuert und kontrolliert werden kann.

In der »Applet Database« sind Referenzen von bekannten bösartigen Applets gespeichert. Mit diesen Referenzen ist es möglich, zusätzliche Warnungen über eingehende aktive Inhalte auszugeben oder diese Applets automatisch zu blockieren /Sandoo/.

Eine Personal Firewall kann offline oder online konfiguriert werden. Offline wird die Personal Firewall direkt am PC konfiguriert, Online wird die Konfiguration zentral gesteuert.

13.9.6 Sicherheitskomponenten einer Personal Firewall

Firewallkomponente Packet Filter

Die Firewallkomponente Packet Filter interpretiert die Pakete und verifiziert, ob die Daten in den entsprechenden Headern der Kommunikationsebenen den definierten Regeln entsprechen. Die Regeln werden so definiert, dass nur die notwendige Kommunikation erlaubt ist und bekannte sicherheitskritische Einstellungen vermieden werden.

Cookie Management

Mithilfe eines Cookie Management ist die Gestaltung des eigenen Datenschutzprogramms möglich. Hier wird festgelegt, was mit welchen Cookies passieren soll. Welche werden geladen, welche nicht, sollen die Cookies sofort wieder gelöscht werden oder sollen sie gelöscht werden, wenn die Personal Firewall heruntergefahren wird, um datenschutzrelevante Angriffe zu vermeiden.

Advanced Sandbox-Modell

Das Advanced Sandbox-Modell, das auch in Java definiert ist, ist ein Konzept, das Programme (Java Applets, Active-X-Controls und andere Executables – siehe folgende Abbildung) in einem abgeschlossenen Bereich kontrolliert zur Ausführung bringt, in dem sie beliebig agieren können, ohne den Rest des Systems zu beeinflussen.

neuKap13.fm Seite 451 Freitag, 18. Oktober 2002 3:52 15

Der Begriff Sandbox stammt daher, dass man Sprengkörper in einer Sandkiste bzw. einem entsprechenden Raum ferngesteuert kontrolliert zur Explosion bringt und so unschädlich macht.

Auf diese Weise kann eine potenziell bösartige Anwendung nur dann auf das zu schützende System (einschließlich der System- und Netzdateien, Ressourcen und verbundenen Geräte) zugreifen, wenn die Personal Firewall dies zulässt. Hierdurch werden in einer anwendungs- und benutzerdefinierten Umgebung alle Systemressourcen vor nicht vertraulichen, unbekannten oder bösartigen Applikationen geschützt. Mithilfe der Rechteverwaltung kann z. B. definiert werden, mit welchen Rechten die Browser auf Dateien oder Verzeichnisse zugreifen können. Mithilfe des Advanced Sandbox-Konzepts können die Ressourcen auch vor unbekannten Bedrohungen geschützt werden.

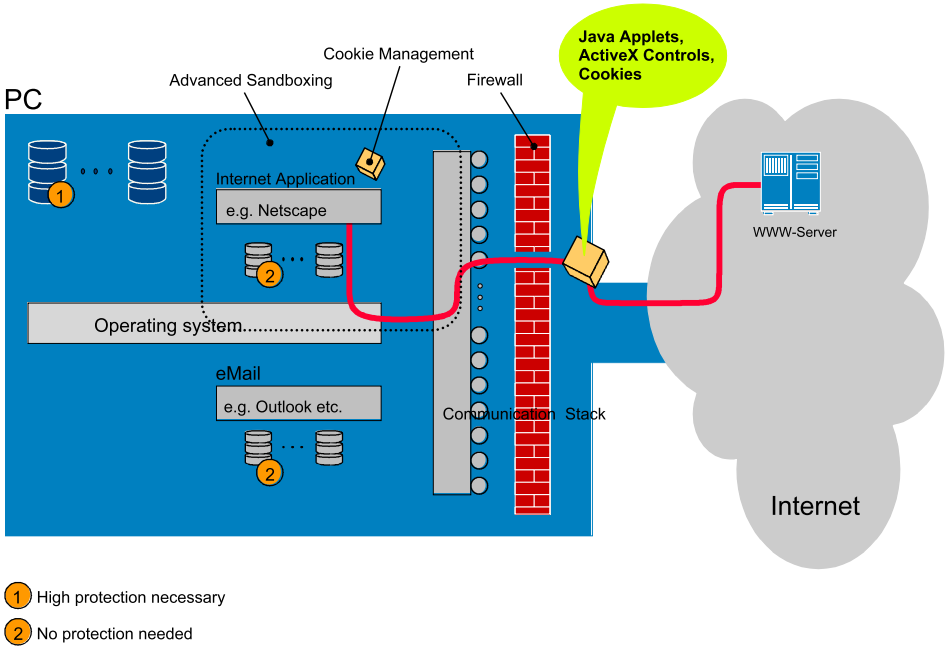


Abb. 13.27: Erweitertes Sandboxing: Schutz der Daten

13.9.7 Beispiel: Schutz vor dem »I love You«-Virus

Im Mai 2000 verursachte der »I love you«-Virus binnen 24 Stunden Schäden in Schwindel erregender Höhe: weltweit schätzungsweise 30 Milliarden US-Dollar. Erst einen Tag später hatten die renommierten Antivirus-Unternehmen ein Gegenmittel parat. Jedoch blieben durch »Advanced Sandbox« geschützte Systeme verschont.

neuKap13.fm Seite 452 Freitag, 18. Oktober 2002 3:52 15

Würde auf einem Rechnersystem, auf dem eine Personal Firewall installiert ist, beispielsweise eine E-Mail mit dem »I love you«-Virus als Anhang empfangen, so würde der Benutzer vor der Ausführung dieses Anhangs gefragt,

- ob er wirklich möchte, dass Bilddateien gelöscht werden und
- ob eine E-Mail an alle, die in seinem Adressverzeichnis stehen, gesendet werden solle (der Virus verfolgt damit das Ziel, sich so weit und schnell wie möglich zu verbreiten).

Mit der Personal Firewall hat der Benutzer also die Möglichkeit, großen Schaden für seinen Bereich, seine Organisation und weitere Kommunikationspartner zu verhindern.

13.9.8 Sichere Umgebung für digitale Signaturen

Eine weitere Möglichkeit ist der Schutz der Signaturfunktion. Im deutschen Signaturgesetz und in der europäischen Richtlinie wird definiert, dass eine digitale Signatur in einer sicheren Umgebung ausgeführt werden muss und jegliche Angriffsmöglichkeit von außen auszuschließen ist. Mit einer Personal Firewall kann man dafür sorgen, dass während der Signatur die Firewall die gesamte Kommunikation schließt, sodass kein Angriff erfolgen kann. Es können auch keine anderen Prozesse auf die Daten zugreifen, die signiert werden, wodurch ein optimaler Schutz und eine sichere Umgebung für die Signaturoperation realisiert wird.

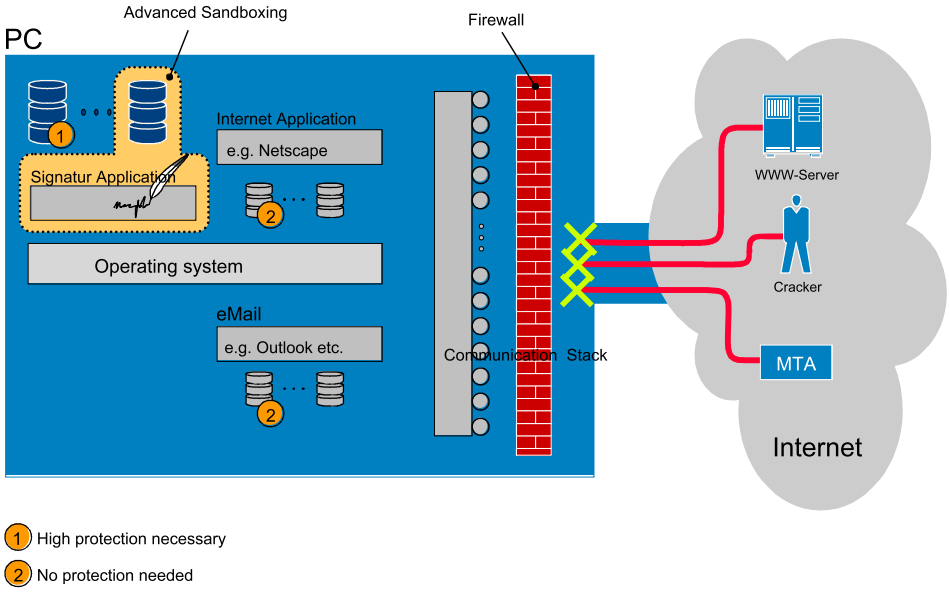


Abb. 13.28: Erweitertes Sandboxing: Schutz der Signaturfunktion

neuKap13.fm Seite 453 Freitag, 18. Oktober 2002 3:52 15

13.9.9 Darstellung, Protokollierung und Statistik sicherheitsrelevanter Ereignisse

Der Benutzer am PC wird informiert, wenn aktive Inhalte (Java Applets, ActiveX-Controls, usw.) installiert und/oder auf dem Rechnersystem gestartet werden. In einem Logbuch werden alle verdächtigen Aktivitäten festgehalten. Über statistische Informationen können Auswertungen durchgeführt werden.

13.9.10 Fazit

Durch den Einsatz von Personal Firewalls kann eine sehr große Wirkung gegen die verschiedenen Angriffsarten, wie das »Empfangen von Malware«, »Java, ActiveX, ... Angriffe« und »interne Angriffe« erzielt werden. Für die Rechnersysteme, insbesondere bei Tele- und Mobil-Arbeitsplätzen, stellt die Personal Firewall einen umfassenden Basisschutz dar (siehe auch »*Theoretische Grundlagen von Firewall-Systemen*«, Kap. 14.5.12 und 14.6).

neuKap13.fm Seite 454 Freitag, 18. Oktober 2002 3:52 15

neuKap14.fm Seite 455 Freitag, 18. Oktober 2002 5:12 17

Kapitel 14

Theoretische Grundlagen von Firewall-Systemen

In diesem Kapitel werden auf einer formalen Ebene die Möglichkeiten und Grenzen von Firewall-Systemen diskutiert und die Anforderungen an ein umfassendes Firewall-System beschrieben.

Als Erstes wird ein eingeschränktes theoretisches Modell vorgestellt, mit dessen Hilfe einheitliche Kriterien über die Möglichkeiten und Grenzen von Firewall-Systemen im Sinne von Sicherheit und Vertrauenswürdigkeit abgeleitet werden können.

Es gibt zwar einige theoretische Modelle im Bereich der Zugangskontrolle, wie z. B. das Bell-LaPadula-Modell, aber diese sind für die Betrachtung von Firewall-Systemen nicht geeignet (siehe auch /BLP74/, /AbO92/, /AHKP91/), weil sie nicht die Kommunikationssicherheit betrachten. Aus diesem Grund wurde ein eigenes eingeschränktes Modell erarbeitet, um die Einflussfaktoren auf die Sicherheit und Vertrauenswürdigkeit ableiten und diskutieren zu können.

14.1 Definition eines Kommunikationsmodells

Eine Kommunikation ist die Zusammenarbeit von Kommunikationssystemen mit dem Ziel, eine gemeinsame Aufgabe zu bewältigen, wobei jedes Kommunikationssystem Daten in einer für diese Aufgabe spezifischen Weise zu verarbeiten hat. Die Zusammenarbeit erfordert die Einhaltung von Regeln, die in einem Satz von Normen festgelegt werden/Tann98/.

Ein Kommunikationssystem ist aus mehreren logischen Schichten aufgebaut. Die TCP/IP-Protokollarchitektur besteht aus vier logischen Schichten:

- In einer Schicht N kommunizieren (Peer) Entities miteinander.
- Zwischen den Entities werden Protokollelemente (x_i) ausgetauscht.
- Protokollelemente bestehen aus Headern und/oder Nutzdaten.
- Header enthalten Steuerinformationen wie z. B. Adressen, laufende Nummern, Zähler, Informationen über den Übertragungsweg, Hinweise auf die Verwendung der Daten. Die Header-Informationen können feste Größen, aber auch Variablen sein.

  Jede Schicht hat eigene Header, die auch leer sein können.

neuKap14.fm Seite 456 Freitag, 18. Oktober 2002 5:12 17

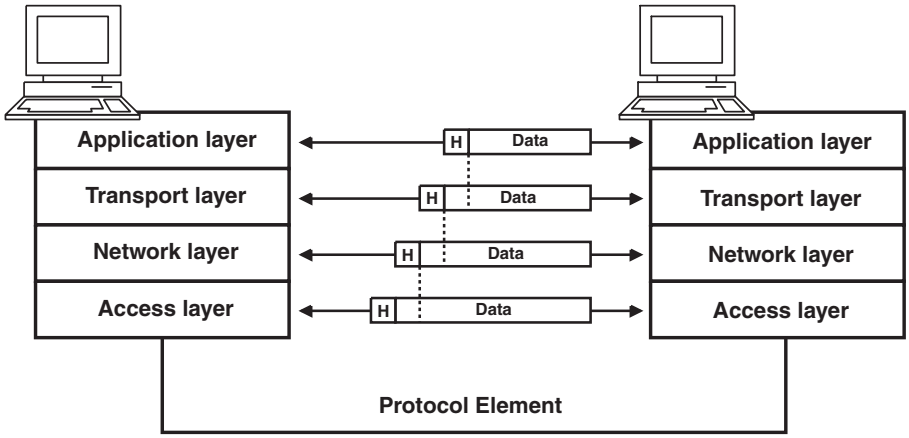


Abb. 14.1: TCP/IP-Protokollarchitektur

- In welcher Reihenfolge die Protokollelemente ausgetauscht werden, wird im Kommunikationsprotokoll festgelegt.
- Die Implementierung des Kommunikationsprotokolls ist Sache des Herstellers und nicht festgelegt.

Schichten der TCP/IP-Protokollarchitektur

In der TCP/IP-Protokollarchitektur bestehen analog zum OSI-Referenzmodell unter-schiedliche Kommunikationsschichten, die Daten von der übergeordneten Schicht zur nächst tieferen Schicht weiterreichen. Jede Kommunikationsschicht fügt den Daten eigene Kontrollinformationen hinzu, bis sie über das Netz gesendet werden. Der Empfänger reicht diese Daten dann Schicht für Schicht nach oben weiter, wobei jede Schicht nur die für sie relevanten Daten auswertet und diese aus dem Datenpaket entfernt, bevor sie an die nächsthöhere Schicht weitergegeben werden.

- Die Netzzugangsschicht ermöglicht es einem Rechnersystem, Daten zu einem anderen Rechnersystem innerhalb des direkt angeschlossenen Netzes (z. B. Ethernet) zu übertragen. Dazu sind genaue Kenntnisse des zugrunde liegenden Netzaufbaus nötig. Die Netzzugangsschicht umfasst die zwei unteren Schichten des OSI-Modells und beinhaltet die Kapselung von IP-Paketen in Netzrahmen (Frames) und die Zuordnung von IP-Adressen zu physikalischen Netzadressen, z. B. MAC-Adressen.
- Die Netzwerkschicht definiert den Aufbau von IP-Paketen und bestimmt, auf welchem Weg die Daten durch das Internet übertragen werden (Routing).
- Die Transportschicht stellt eine Verbindung zwischen zwei Endpunkten oder Rechnersystemen her. Die wichtigsten Protokolle sind TCP und UDP.

neuKap14.fm Seite 457 Freitag, 18. Oktober 2002 5:12 17

- Die Anwendungsschicht beinhaltet sämtliche Programme und Dienste, die über die Netzwerkverbindung durchgeführt werden sollen. Dazu gehören vor allem Dienste wie Telnet (LogIn auf einem anderen Rechnersystem), FTP (Datentransfer zwischen zwei Rechnersystemen), SMTP (E-Mail-Funktionen), HTTP (World Wide Web), usw.

Vereinfachtes logisches Kommunikationsmodell

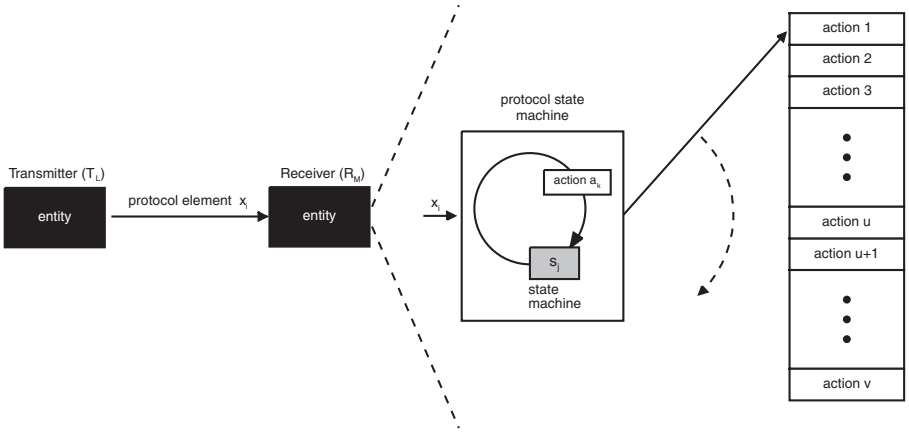


Abb. 14.2: Vereinfachtes logisches Kommunikationsmodell

Dieses vereinfachte logische Kommunikationsmodell soll das grundsätzliche Prinzip eines Kommunikationsablaufs darstellen. Jede Schicht hat eine eigene »protocol state machine«, die dem jeweiligen Kommunikationsprotokoll der entsprechenden Schicht entspricht.

Zur Bewältigung der spezifischen Aufgabe der Entities in einer bestimmten Schicht führt diese in Abhängigkeit vom empfangenen Protokollelement x_i, vom aktuellen Zustand s_j und von weiteren Ereignissen (Timerabläufen, Statusmeldungen, ...) eine definierte Aktion ak aus. Dabei sind die Header-Informationen für die Aktionen in der Regel entscheidend. Die Schichten sind im Normalfall voneinander unabhängig.

Die Komplexität der jeweiligen Schichten kann sehr unterschiedlich sein. Pro physikalischem Protokollelement können mehrere Schichten beteiligt sein.

neuKap14.fm Seite 458 Freitag, 18. Oktober 2002 5:12 17

14.1.1 Definition der Transmitter

Es gibt eine endliche Menge von Transmittern, die wie folgt definiert werden:

Transmitter (T) = $\{t_1, \ldots t_l\}$

Aufteilung der Transmitter

Erlaubte Transmitter $\{t_1, \ldots t_g\}$:

Erlaubte Transmitter sind solche Transmitter, die Aktionen beim Receiver veranlassen dürfen. Erlaubte Transmitter stellen ein kalkulierbares Risiko bezüglich der Verwundbarkeit der Werte da.

Nicht erlaubte Transmitter $\{t_{g+1}, \ldots t_l\}$:

Nicht erlaubte Transmitter sind solche Transmitter, die keine Aktionen beim Receiver veranlassen dürfen. Nicht erlaubte Transmitter (Angeifer, Fremde, Unbefugte) stellen ein sehr hohes Risiko bezüglich der Verwundbarkeit der Werte da.

Welche Transmitter erlaubt sind und welche nicht, wird durch die Sicherheitspolitik festgelegt.

14.1.2 Definition der Receiver

Es gibt eine endliche Menge von Receivern, die wie folgt definiert werden.

Receiver (R) = $\{r_1, \ldots r_m\}$

Aufteilung der Receiver

Erlaubte Receiver $\{r_1, \ldots r_h\}$:

Erlaubte Receiver sind solche Receiver, bei denen erlaubte Transmitter erlaubte Aktionen veranlassen dürfen. Erlaubte Receiver stellen ein kalkulierbares Risiko bezüglich der Verwundbarkeit der Werte dar.

Nicht erlaubte Receiver $\{r_{h+1}, \ldots r_m\}$:

Bei nicht erlaubten Receivern (Unbefugte) dürfen keine Aktionen veranlasst werden.

Welche Receiver erlaubt sind und welche nicht, wird durch die Sicherheitspolitik festgelegt.

14.1.3 Definition der Protokollelemente

Die Protokollelemente, die zwischen Sender und Empfänger ausgetauscht werden, können wie folgt klassifiziert werden: Summe alle Protokollelemente: $\sum = 2^n$

Protokollelemente X = $\{x_1, \ldots x_t, x_{t+1}, \ldots x_u, x_{u+1}, \ldots x_v, x_{v+1}, \ldots x_n\}$

neuKap14.fm Seite 459 Freitag, 18. Oktober 2002 5:12 17

<table>
<tr><td rowspan="5">$\{x_1, ... x_n\}$

mögliche</td><td colspan="2">Menge der Protokollelemente, die möglich sind (mögliche Codierung der Bits und Bytes).</td><td></td></tr>
<tr><td>$\{x_1, ... x_u\}$</td><td>Menge der Protokollelemente, die in der Norm definiert sind (ISO, RFC, ...).</td><td rowspan="2"></td></tr>
<tr><td rowspan="3">genormt</td><td>$\{x_1, ... x_t\}$
genormt und erlaubt</td><td>Menge der Protokollelemente aus der Norm, die für eine spezielle Aufgabe notwendig und damit erlaubt sind z. B. die Kommandos »cdir« (Change Directory) and »put« (Transmit), um mithilfe vom FTP eine Datei vom Sender zu versenden und auf der Empfängerseite zu speichern</td><td>erlaubt</td></tr>
<tr><td>$\{x_{t+1}, ... x_u\}$
genormt und nicht erlaubt</td><td>Menge der Protokollelemente aus der Norm, die für die spezielle Aufgabe nicht notwendig und damit nicht erlaubt sind. z. B. bei FTP das Kommando »del« (Löschen von Dateien)</td><td rowspan="3">nicht erlaubt</td></tr>
<tr><td rowspan="3">nicht genormt</td><td>$\{x_{u+1}, ... x_n\}$</td><td>Menge der Protokollelemente, die nicht in der Norm definiert sind, und für die eigentliche Aufgabe nicht notwendig und damit in der Regel nicht erlaubt sind.</td></tr>
<tr><td>$\{x_{u+1}, ... x_v\}$

Hersteller-definiert</td><td>Menge der Protokollelemente, die nicht in der Norm definiert sind, aber zusätzliche Dienste anbieten. Hersteller haben bei ihrer Implementierung der Kommunikationsprotokolle oder -dienste weitere, eigene Protokollelemente definiert, um z. B. folgende Aufgaben durchführen zu können:
● Fehleranalyse (Zustand des Protokoll-Automats, Zustand des Betriebssystems, ...)
Diese zusätzlichen Dienste werden von den Herstellern angeboten, um aus der Ferne eine Fehleranalyse oder sonstige Servicearbeiten durchführen zu können.
● Trap-Doors, mit denen Angriffe realisiert werden und nicht definierte oder erlaubte Aktionen auf der Empfängerseite unautorisiert durchgeführt werden können.
Diese Protokollelemente sind in der Regel nicht erlaubt.</td></tr>
<tr><td>$\{x_{v+1}, ... x_n\}$

nicht definiert</td><td>Menge der Protokollelemente, die nicht in der Norm und nicht vom Hersteller definiert und damit nicht erlaubt sind. Im Normalfall werden solche Protokollelemente von der Implementierung als Fehler erkannt und entsprechend behandelt. Es werden aber immer wieder Implementierungen bekannt, die beim Empfang von nicht definierten Protokollelementen eine fehlerhafte Aktionen durchführen, die für einen Angriff verwendet werden kann.</td></tr>
<tr><td colspan="4">t <= u
u <= n (ist u=n, dann v=n, dann gibt es keine undefinierten Protokollelemente)
v <= n (ist v=n, dann gibt es keine undefinierten Protokollelemente)</td></tr>
</table>

Tabelle 14.1: Definition der Protokollelemente

Welche Protokollelemente erlaubt sind und welche nicht, wird durch die Sicherheitspolitik festgelegt.

Bei der Betrachtung über die Sicherheit von Protokollelementen $\{x_1, ... x_n\}$ müssen weitere Aspekte berücksichtigt werden:

- Nicht alle Felder in den Protokollelementen sind sicherheitsrelevant in Bezug auf die Möglichkeiten eines Firewall-Systems (z. B. Laufzahler, Zufallszahlen, ...). Aus diesem Grund reduziert sich die praktische Anzahl der Protokollelemente, die betrachtet werden müssen, sehr stark.
- Bestimmte Protokollelemente sind in Abhängigkeit vom Zustand des Kommunikationsprotokolls erlaubt oder nicht erlaubt. Aus diesem Grund muss die obrige Tabelle immer in Abhängigkeit vom Zustand des Kommunikationsprotokolls betrachtet werden. Protokollelemente können in einem bestimmten Zustand erlaubt und in einem anderen Zustand nicht erlaubt sein.

neuKap14.fm Seite 460 Freitag, 18. Oktober 2002 5:12 17

- Die Möglichkeit, über verdeckte Kanäle Informationen zu übertragen, wird in diesem Modell nicht betrachtet.
- Erlaubte Protokollelemente $\{x_1, \ldots x_t\}$ dürfen nur zwischen erlaubten Transmittern $\{t_1, \ldots t_g\}$ und Receivern $\{r_1, \ldots r_h\}$ zu erlaubten Zeiten ausgetauscht werden.

14.1.4 Definition der Aktionen

Die Aktionen auf der Empfängerseite sind wie folgt definiert.

Aktion (A) = $\{a_1, \ldots a_f\}$:

Eine Aktion, die aus einer definierten Anzahl von Teilaktionen besteht, ist z. B. das Schreiben einer Datei auf die Festplatte des Empfängers mithilfe von FTP. Teilaktionen sind z. B. das Selektieren der Subdirectory, das Empfangen von Teildatenmengen, das Abspeichern der Daten, usw.

Aufteilung der Aktionen

Erlaubte Aktionen $\{a_1, \ldots a_t\}$:

Erlaubte Aktionen sind solche Aktionen, die für die erlaubten Anwendungen (Aufgabenstellung) notwendig sind. Erlaubte Anwendungen auf definierte assets stellen ein kalkulierbares Risiko bezüglich der Verwundbarkeit der Werte da.

Im Bereich der erlaubten Aktionen fallen auch die Fehlerbehandlungen bzgl. der nicht definierten Zustände und Ereignisse.

Nicht erlaubte Aktionen $\{a_{t+1}, \ldots a_f\}$:

Nicht erlaubte Aktionen sind solche Aktionen, die zwar die Implementierung eines Kommunikationsprotokolls oder -dienstes auf der Empfängerseite ermöglichen, aber für die eigentliche Aufgabenstellung nicht notwendig und deshalb nicht erlaubt sind, damit das Risiko eines beabsichtigten oder auch unbeabsichtigten Schadens minimiert wird.

Welche Aktionen erlaubt sind und welche nicht, wird durch die Sicherheitspolitik festgelegt.

Erlaubte Aktionen $\{a_{t+1}, \ldots a_f\}$ dürfen nur durch erlaubte Protokollelemente $\{x_1, \ldots x_t\}$ ausgelöst werden, die zwischen erlaubten Transmittern $\{t_1, \ldots t_g\}$ und Receivern $\{r_1, \ldots r_h\}$ zu erlaubten Zeiten ausgetauscht werden.

neuKap14.fm Seite 461 Freitag, 18. Oktober 2002 5:12 17

14.1.5 Kommunikationsabläufe

Der Transmitter sendet dem Receiver Protokollelemente über das Netz. Der Receiver interpretiert die empfangenen Protokollelemente als externe Ereignisse und startet mit diesen und weiteren Informationen seine »protocol-state-machine«.

Action of the Receiver

$$\mathbf{a_k} = \textit{protocol-state-machine}(\mathbf{x_i}^*, \mathbf{s_j})$$

a_k Teil-Aktion in einer Schicht, die in Abhängigkeit vom empfangenen Protokollelement x_i und vom aktuellen Zustand s_j ausgeführt wird
x_i Protokollelement
s_j aktueller Zustand (actual state)

Das Protokoll wird als State-Machine betrachtet, in der sich der Zustand s_j in Abhängigkeit von den empfangenen Protokollelementen und von weiteren Ereignissen (Timerabläufen, Statusmeldungen, ...) verändern kann.

Ablauf der Aktionen beim Receiver

Mithilfe der Aktionen (a_k), die in Abhängigkeit vom empfangenen Protokollelement (x_i) sowie von weiteren Ereignissen (Timerabläufen, Statusmeldungen, ...) und vom aktuellen Zustande (s_j) ausgeführt werden, werden beim Receiver erlaubte Informationen (assets) verarbeitet oder Ressourcen (assets: Drucker, Berechnungen, ...) genutzt. Das folgende Bild verdeutlicht die Verbindung der Aktionen mit den Informationen und anderen Ressourcen.

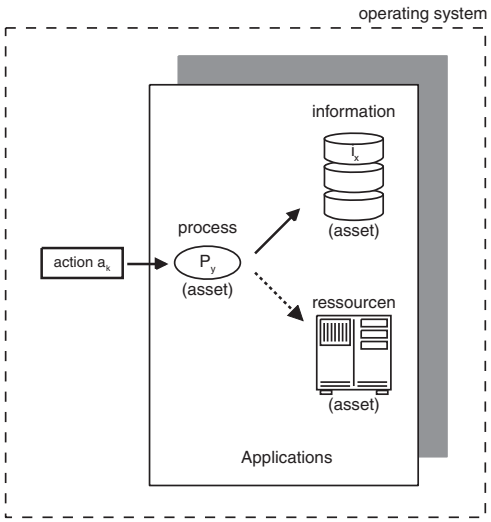


Abb. 14.3: Ablauf der Aktionen beim Receiver

neuKap14.fm Seite 462 Freitag, 18. Oktober 2002 5:12 17

Welche konkreten Informationen oder andere Ressourcen mit einer definierten Aktion genutzt werden dürfen, wird in der Regel mithilfe der Rechteverwaltung des Betriebssystems (Windows, UNIX, MVS, ...) und der Rechteverwaltung der Anwendungen (Datenbank, SAP, ...) detailliert definiert.

Aus Sicht des Kommunikationsmodells ist es egal, welche Rechnersysteme oder Betriebssysteme der Transmitter (T) oder Receiver (R) nutzt. Beide müssen nur die entsprechenden Kommunikationsprotokolle und -dienste, z. B. TCP/IP-Familie nach den definierten Standards realisieren.

14.1.6 Angriffe aus dem Netz

In diesem Abschnitt werden die grundlegenden potenziellen Angriffe, die im Weiteren betrachtet werden sollen, definiert und beschrieben /Pohl2000a/. Ein Firewall-System soll Sicherheitsmechanismen zur Verfügung stellen, die wirkungsvoll gegen diese Angriffe wirken und damit das Risiko minimieren.

Idee eines Angriffs

Ein Angreifer versucht gezielt und absichtlich, den Receiver zu beeinflussen, um

- an bestimmte Informationen (assets) zu gelangen, die nicht für ihn bestimmt sind,
- Reaktionen auszulösen, die er nicht auslösen darf, oder
- Ressourcen (assets) zu nutzen, die er nicht nutzen darf.

Dies tut der Angreifer,

- um mit den Informationen Geld zu verdienen (z. B. Entwicklungsdaten),
- oder ohne materielle Gewinnabsicht.

Letzteres hat Gründe, die meist in den Formenkreis »gestörte Persönlichkeit« fallen. Stichworte: um dem (Zufalls)-Opfer zu schaden; aus Zerstörungswut, ähnlich wie Vandalismus oder Brandstiftung (Nero-Syndrom); aus purer Langeweile (»just for fun«); bei Unterforderung an der Arbeitsstätte, wie z. B. die bulgarischen Programmierer, die Virenprogramme schrieben; aus Geltungsbedürfnis, um fehlendes Selbstbewusstsein, fehlende Anerkennung oder versagte Liebe zu kompensieren; aus reiner Spielleidenschaft, bis hin zur Spielsucht und der Jagd nach dem ultimativen Hacking oder Virusprogramm, das seinen »Schöpfer« in die Schlagzeilen bringt; oft aus jugendlichem Übermut (»Script-Kiddies«, die »erprobte« Hack-Listings adaptieren), um fame (Ruhm) zu erlangen, ähnlich wie Sprayer, die traces (Spuren) legen und mit ihren tags (Zeichen) in einer uns unverständlichen Subkultur – hier: der »Hacker-Gemeinde« – leben; aus vorgeblich ideellen oder politischen Gründen (Kampf »gegen das Establishment« oder Intoleranz gegen bestimmte Weltanschauungen).

neuKap14.fm Seite 463 Freitag, 18. Oktober 2002 5:12 17

Es gibt unterschiedliche Angriffsarten, die in den folgenden Unterkapiteln definiert und beschrieben werden.

14.1.6.1 Angriffe durch Dritte

Bei dieser Art der Angriffe werden durch einen Dritten (Attacker) aktiv Protokollelemente wiederholt, verändert, gelöscht oder neu zusätzlich eingespielt.

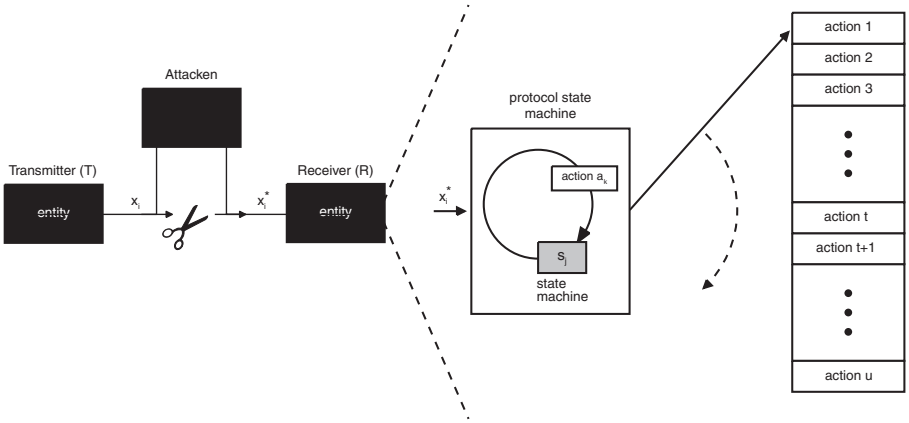


Abb. 14.4: Angriffe durch Dritte

	Angriffe durch Dritte	
Angriffsart	Ziel des Angriffs	Beispiel
Wiederholen oder Verzögern eines oder mehrerer Protokollelemente(s)	Durch das Wiederholen oder Verzögern eines oder mehrerer Protokollelemente(s) kann der Receiver irritiert oder zu einer falschen Aktion veranlasst werden.	Mehrfache Überweisung eines Geldbetrags oder Wiederholung eines abgefangenen Logins.
Einfügen oder Löschen bestimmter Daten in den Protokollelementen	Um den Receiver zu manipulieren, fügt ein Angreifer bestimmte Daten im Protokollelement ein oder löscht sie. Der Receiver kann durch Unterdrückung oder zusätzlichen Empfang entscheidender Informationen zu einem falschen Verhalten (falsche Aktion oder Aktionen) veranlasst werden.	In einem Protokollelement einer E-Mail, in der »Kaufen Sie keine Aktien auf« wird das »keine« während der Übertragung gelöscht, sodass der Receiver die Instruktion »Kaufen Sie neue Aktion« erhält.

Tabelle 14.2: Angriffe durch Dritte

neuKap14.fm Seite 464 Freitag, 18. Oktober 2002 5:12 17

	Angriffe durch Dritte	
Angriffsart	Ziel des Angriffs	Beispiel
Modifikation der Daten in den Protokoll-elementen	Modifikation der Daten bedeutet, dass die Veränderung der Daten vom Receiver nicht erkannt wird. Durch Ändern der Daten während der Datenübertragung ist es einem Angreifer möglich, falsche Aktionen zu veranlassen.	Die Veränderung einer Kontonummer bei einer Geldüberweisung führt dazu, dass ein anderer als der intendierte Kontobesitzer das Geld bekommt.
Boykott des Receivers	Wenn der Umfang von eingefügter oder unterdrückter Daten zu groß wird oder realzeitorientierte Daten zu lange verzögert werden, kann hierdurch der Receiver boykottiert werden.	Durch permanenten Verbindungsaufbau zum Receiver kann dieser blockiert und isoliert werden. Die so genannten »distributed denial of service«- oder DDoS-Angriffe haben gezeigt, dass Service im Internet im großen Stil verhindert werden und ein enormer Schaden auftreten kann.
Trittbrettfahrer	Ein Angreifer aus dem unsicheren Netz kann die bestehende Verbindung des Benutzers aus dem unsicheren Netz übernehmen und ist damit als Trittbrettfahrer in der Lage, die gleichen Aktionen auszuführen wie der berechtigte Benutzer.	Nach der erfolgreichen Authentikation eines Home-Banking Kunden übernimmt der Angreifer die Verbindung, um sich selbst zu bereichern.
Senden von Malware (Viren, Würmer, Trojanische Pferde, ...)	Der Angreifer sendet Malware, um den Receiver zu schädigen. Typischerweise werden die Malware mithilfe von Anhängen an E-Mails oder innerhalb von WWW-Dokumenten zum Receiver gesendet.	Senden von Viren (z. B. »I-Love-You«-Virus),die die Daten des Receivers zerstören.

Tabelle 14.2: Angriffe durch Dritte (Forts.)

neuKap14.fm Seite 465 Freitag, 18. Oktober 2002 5:12 17

14.1.6.2 Angriffe durch den Kommunikationspartner

Bei dieser Art der Bedrohung ist der eigentliche Kommunikationspartner der Angreifer, der aktiv eine Gefahr darstellt.

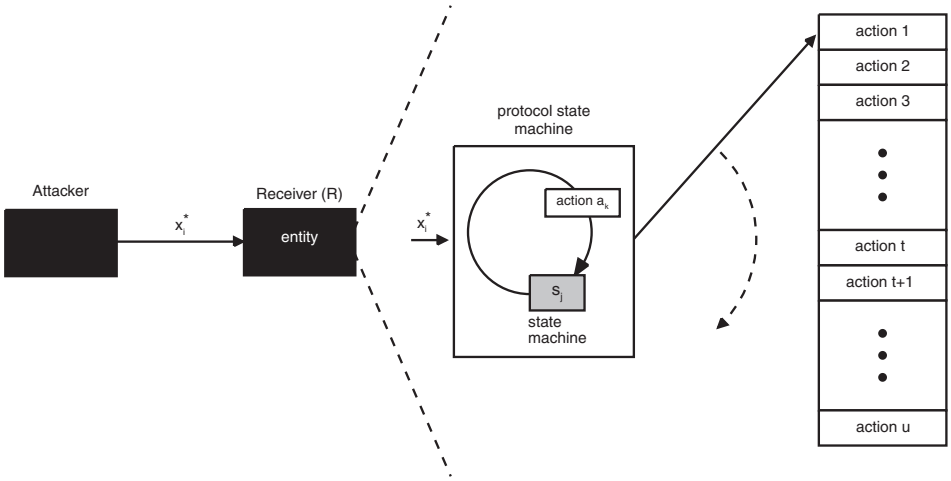


Abb. 14.5: Angriffe durch den Kommunikationspartner

	Angriffe durch den Transmitter	
Angriffsart	Ziel des Angriffs	Beispiel
Unberechtigter Aufbau und Nutzung von Kommunikationsverbindungen	Ein Angreifer nutzt eine bereits bestehende Kommunikationsverbindung, um sich Vorteile zu verschaffen oder den Receiver zu schädigen.	Ein Angreifer nutzt eine bestehende Verbindung, um Entwicklungsdaten im zu schützenden Netz zu stehlen, auf die er nicht zugreifen darf.
Unberechtigte Nutzung von Kommunikationsprotokollen und -diensten	Ein Angreifer nutzt die grundsätzliche Möglichkeit eine Kommunikation durchzuführen, um sich Vorteile zu verschaffen oder den Receiver zu schädigen.	Der Angreifer nutzt z. B. den Telnet-Dienst, um ein Rechnersystem zu manipulieren.
Vortäuschen einer falschen Identität (Maskerade-Angriff)	Wenn sich der Kommunikationspartner für einen anderen ausgibt, kann er sich Informationen (assets) erschleichen, die nicht für ihn bestimmt waren, Ressourcen (assets) nutzen, die er nicht nutzen darf oder Reaktionen auslösen, die nur ein anderer Kommunikationspartner veranlassen darf.	Ein Kommunikationspartner verschafft sich unerlaubt Zugang zur einer Datenbank.

Tabelle 14.3: Angriffe durch den Transmitter

neuKap14.fm Seite 466 Freitag, 18. Oktober 2002 5:12 17

Angriffe durch den Transmitter		
Angriffsart	Ziel des Angriffs	Beispiel
Nutzung der Kommunikationsverbindung zum Receiver für gezielte Angriffe (z. B. Java-Applets, ActiveX-Controls)	Der Angreifer nutzt die vom Receiver aufgebaute Kommunikationsverbindung, um sich Vorteile zu verschaffen oder den Receiver zu schädigen.	Der Benutzer (Receiver) baut zu einem Web-Server eine Verbindung auf. Dieser nutzt diese, um z. B. per Java-Applets Informationen zu stehlen oder zu löschen.
Nutzung einer falschen Konfiguration	Für jeden Dienst, der über einen Netzzugang ermöglicht werden soll, existiert ein »Daemon-Prozess«, dieser kann falsch konfiguriert oder installiert sein, sodass sich beim Receiver beliebige privilegierte Kommandos (ein oder mehrere Protokollelemente) ausführen lassen, mit denen ein Angriff durchgeführt werden kann.	Der Angreifer nutzt die Tatsache, dass eine falsche Konfiguration vorliegt, um z. B. an die »root«-Rechte des Receivers zu gelangen, die ihm dann Zugang zu seinen Angriffszielen verschaffen. Beispiel: WWW-Server mit root-Rechten und fehlerhaften CGI-Scripten.
Nutzung von Implementierungsfehler	Der Angreifer nutzt Implementierungsfehler der Kommunikationsprotokolle oder -dienste des Receivers, um nicht erlaubte Aktionen ausführen zu können.	Komplexe Anwendungen, wie z. B. »sendmail«, wiesen in der Vergangenheit Implementierungs- und Designfehler auf, die es ermöglichten, beim Receiver beliebige privilegierte Kommandos ausführen zu lassen, mit denen Angriffe durchgeführt werden konnten.
Leugnen der Kommunikationsbeziehung	Der wachsende Einsatz von Datenkommunikation zur Abwicklung vertraglich relevanter Vorgänge erfordert, dass sowohl der Kommunikationspartner das Senden einer Nachricht (ein Protokollelement oder mehrere) als auch der Receiver den Empfang der Nachricht nicht abstreiten kann.	Bestellung von Waren über das Internet bei einem Händler oder Abschluss von Verträgen über das Internet. Durchführung einer Service-Arbeit über das Netz.

Tabelle 14.3: Angriffe durch den Transmitter (Forts.)

neuKap14.fm Seite 467 Freitag, 18. Oktober 2002 5:12 17

14.1.6.3 Vorbereitung für Angriffe

Diese Art der Angriffe wird genutzt, um andere Angriffe besser durchführen zu können.

	Vorbereitung für Angriffe	
Angriffsart	Ziel des Angriffs	Beispiel
Social Engineering	Der Angreifer nutzt seine soziale Kompetenz (z. B. Redegewandtheit, sicheres Auftreten, usw.), um jemanden zu überzeugen, ihm sein Passwort zu überlassen oder bestimmte Operationen für ihn vorzunehmen. Dazu spioniert der Angreifer Lebensumstände wie übliche Arbeitszeiten, Namen nahe stehender Personen, Hobbys etc. aus.	Der Angreifer gibt sich am Telefon als Vorgesetzter, Kollege oder Systemadministrator aus. Meist erzeugt er eine künstliche Dringlichkeit (»Ich stehe hier mit einem potenziellen Großkunden und muss ihm das System zeigen«), um sein Opfer davon zu überzeugen, ihm ohne Überprüfung sein Passwort zu geben.
Analyse mithilfe von Scannerprogrammen	Mit so genannten Scannerprogrammen ist ein Angreifer in der Lage festzustellen, aus welchen IP-Adressen und Betriebssystemen (Rechnersystemen) und aus welchen Benutzern und welchen Diensten das zu schützende Netz besteht.	**Rechnersysteme:** Die aktiven IP-Adressen eines Netzes können z. B. mithilfe des »ping«-Befehls analysiert werden. Ein Angreifer sendet den »ping«-Befehl an alle möglichen IP-Adressen eines Adressbereiches. Bei einem Klasse-C-Netz bedeutet dies, es wird an die IP-Adresse A.B.C.1 bis A.B.C. 254 ein »ping«-Befehl gesendet. An den empfangenen Antworten kann abgelesen werden, hinter welcher IP-Adresse sich ein real angeschlossenes Rechnersystem befindet. **aktive Benutzer:** Mit dem Befehl »finger« ist ein Angreifer in der Lage, festzustellen, welche Benutzer zum jeweiligen Zeitpunkt an einem bestimmten Rechnersystem aktiv sind, ob sie schon die empfangenen Mails gelesen haben usw.

Tabelle 14.4: Vorbereitung für Angriffe

neuKap14.fm Seite 468 Freitag, 18. Oktober 2002 5:12 17

Vorbereitung für Angriffe		
Angriffsart	Ziel des Angriffs	Beispiel
		aktive Dienste: Durch Ansprechen der einzelnen Ports kann ein Angreifer analysieren, für welche Dienste ein Daemon-Prozess auf dem entsprechenden Rechnersystem installiert ist. **Schwachstellenanalyse auf den einzelnen Rechnersystemen:** Mit weiteren Hilfsprogrammen (z. B. »ISS«, »SATAN«) kann dann der Angreifer gezielt eine Schwachstellenanalyse durchführen. Hier wird überprüft, ob z. B. durch Konfigurationsfehler der Daemon-Prozesse der aktiven Dienste oder durch die Verwendung fehlerhafter alter Versionen ein Angriff auf das Rechnersystem möglich ist.

Tabelle 14.4: Vorbereitung für Angriffe (Forts.)

Interne Angriffe		
Angriffsart	Ziel des Angriffs	Beispiel
Interne Angriffe	Mit Informationen (Entwicklungsdaten, Kundendaten, usw.) Geld verdienen, der Organisation schaden, Geltungsbedürfnis, Spielleidenschaft.	Die Mitarbeiter der Organisation greifen von innen auf die Rechnersysteme der Kollegen zu, um an schützenswerte Informationen zu gelangen.

Tabelle 14.5: Interne Angriffe

14.2 Definition eines Firewall-Elements

Ein Firewall-System besteht aus Firewall-Elementen, die aktiv in die Kommunikation zwischen dem zu schützenden und dem unsicheren Netz eingreifen sowie einem Security Management, das für die Verwaltung der aktiven Firewall-Elemente verantwortlich ist.

neuKap14.fm Seite 469 Freitag, 18. Oktober 2002 5:12 17

Grundsätzliches

Ein Firewall-System ist ein separates Kommunikationssicherheitssystem. Es besteht in der Regel keine direkte Verbindung mit den Sicherheitsfunktionen der Betriebssysteme und der Rechnersysteme (Receiver, Transmitter). Ein Firewall-System hat keinen Einfluss (Erweiterung, Veränderung) auf die verwendeten Kommunikationsprotokolle und -dienste. Ein Firewall-System wird von der Organisation verwaltet, die es betreibt, und ist im Prinzip unabhängig von allen anderen Organisationen in dieser Verwaltung.

Im Folgenden wird der prinzipielle Aufbau der aktiven Firewall-Elemente, die in die Kommunikationsschnittstelle zwischen dem unsicheren Netz und dem zu schützenden Netz eingefügt werden, definiert. Ein so umrissenes Firewall-Element kann Packet Filter, Stateful Inspection, Application Gateway, Proxies und Adaptive Proxies repräsentieren.

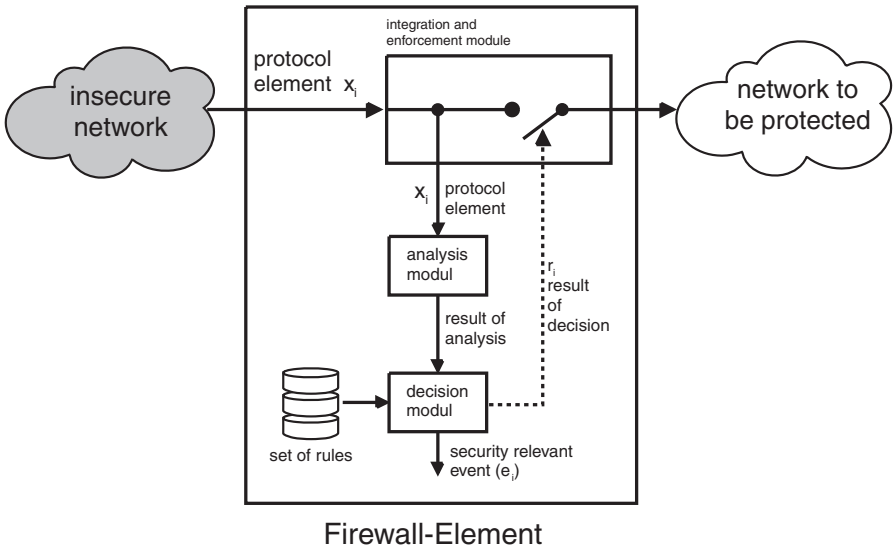


Abb. 14.6: Firewall-Element

In einem Firewall-Element wird das Protokollelement eventuell verändert, bevor es weiterversendet wird (siehe z. B. Kapitel 5.4 *»Application Gateway/Proxy-Technik«*).

neuKap14.fm Seite 470 Freitag, 18. Oktober 2002 5:12 17

Einbindungs- und Durchsetzungsmodul

Das Einbindungs- und Durchsetzungsmodul realisiert die Einbindung des aktiven Firewall-Elements in das Kommunikationssystem sowie die Durchsetzung der im Regelwerk festgehaltenen Sicherheitspolitik.

Die Einbindung in das Kommunikationssystem muss so realisiert werden, dass die Kommunikationsdaten nicht am Einbindungsmodul vorbeifließen können, ohne einer Analyse und einer Entscheidung unterzogen worden zu sein. Aus diesem Grund ist die Einbindung besonders sicherheitskritisch. In Abhängigkeit vom verwendeten Protokollelements wird das Einbindungsmodul an unterschiedlichen Stellen der Protokollarchitektur eingebunden.

Analysemodul → analysis(x_i)

Im Analysemodul werden die Kommunikationsdaten des Protokollelements (x_i) den Möglichkeiten des aktiven Firewall-Elements entsprechend analysiert. Die Ergebnisse der Analyse werden an das Entscheidungsmodul weitergeleitet. Im Analysemodul können mithilfe von Zustandsautomaten Statusinformationen (z. B. Verbindungsaufbau, Transferzustand oder Verbindungsabbau) der Kommunikation festgehalten werden.

Entscheidungsmodul

Im Entscheidungsmodul werden die Analyseergebnisse ausgewertet und mit den im Regelwerk festgelegten Definitionen der Sicherheitspolitik verglichen. Hier wird anhand von Access-Listen überprüft, ob das ankommende Protokollelement (x_i) passieren darf oder nicht (r_i = result of the decision). Falls ja, wird das Einbindungsmodul zum Durchlass aktiviert. Falls nein, wird das Protokollelement (x_i) nicht durchgelassen; das Ereignis (e_i) wird als sicherheitsrelevant eingestuft und entsprechend weiterverarbeitet.

Regelwerk → security management *(rules)*

Das Regelwerk ist die technische Umsetzung der Sicherheitspolitik und wird mithilfe eines Security Management erstellt.

Im Regelwerk stehen alle Informationen (rules: Schlüssel, Access-Listen, Attribute usw.) über Benutzer, Authentikationsverfahren, Kommunikationsverbindungen, Kommunikationsprotokolle und -dienste, die notwendig sind, um eine Entscheidung für oder gegen eine Übertragung des Protokollelements (x_i) über das aktive Firewall-Element fällen zu können, und wie mit sicherheitsrelevanten Ereignissen (e_i) verfahren werden soll.

neuKap14.fm Seite 471 Freitag, 18. Oktober 2002 5:12 17

14.3 Definition des Kommunikationsmodells mit integriertem Firewall-System

Im Folgenden wird das Kommunikationsmodell mit integriertem Firewall-System definiert und beschrieben. Das Firewall-System soll den Receiver $\{r_1, \ldots r_m\}$ vor Angriffen auf seine Werte aus dem unsicheren Netz schützen.

Es wird davon ausgegangen, dass, in Übereinstimmung mit der vorher festgelegten Sicherheitspolitik, mithilfe eines Security Managements die Rechte in das Firewall-System eingetragen worden sind, die es ermöglichen sollen, die erlaubten Protokollelemente $\{x_1, \ldots x_t\}$ über das Firewall-System übertragen zu können. Bei einer fehlerfreien Implementierung des Firewall-Systems und der Kommunikationsprotokolle und -dienste auf der Empfängerseite werden auch nur erlaubte Aktionen $\{a_1, \ldots a_t\}$ zu den erlaubten Zeiten beim Receiver $\{r_1, \ldots r_h\}$ ausgeführt.

Bei dem Kommunikationsmodell mit integriertem Firewall-System müssen beliebig viele Transmitter und Receiver berücksichtigt werden.

Kommunikationsmodell mit integriertem Firewall-System

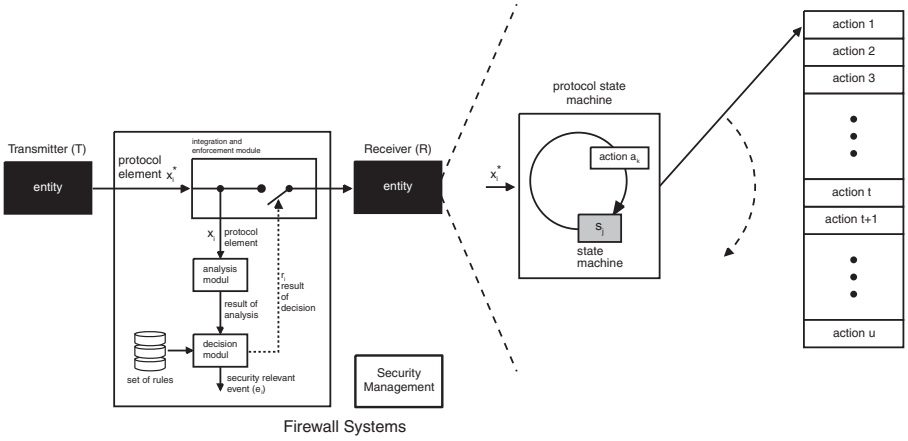


Abb. 14.7: Kommunikationsmodell mit integriertem Firewall-System

Mithilfe der Betrachtung der möglichen Einflussfaktoren auf die Auswahl und Durchführung der Aktionen beim Receiver sollen Kriterien abgeleitet werden, mit deren Hilfe eine Aussage über die Möglichkeiten und Grenzen im Sinne der Sicherheit und Vertrauenswürdigkeit des Kommunikationsmodell mit integriertem Firewall-Systemen gemacht werden kann.

neuKap14.fm Seite 472 Freitag, 18. Oktober 2002 5:12 17

Definition der Funktionen für die Auswahl der Aktion auf der Empfängerseite für »$\mathbf{r_n}$«

a_k = *action-select*(*protocol-state-machine*(x_i, s_j),
authenticity(x_i, t_l),
*result-of-decision***(***analysis*(x_i)),
*security management***(rules))**,
*functionality-of-the-firewall-system***())**

Action-select ist eine Funktion, die in Abhängigkeit von der Echtheit des empfangenen Protokollelements $\mathbf{x_i}$ und des Transmitters $\mathbf{t_l}$ sowie von der Überprüfung der Rechte und der vorhandenen und vertrauenswürdigen Sicherheitsdienste im Firewall-System und des Protokollautomaten auf der Empfängerseite die Auswahl der Aktion beschreibt.

a_k	Teil-Aktion in einer Schicht, die in Abhängigkeit vom empfangenen Protokollelement x_i und vom aktuellen Zustand s_j ausgeführt wird
x_i	Protokollelement, welches auf der Empfängerseite ankommt
s_j	aktueller Zustand (actual state)
t_i	Transmitter, der das Protokollelement x_i sendet
rules	technische Umsetzung der Sicherheitspolitik (Access-Listen, ...)

Neben »r_n« sind in der Regel weitere Empfänger {r_1, ... r_g} zu berücksichtigen.

Definition: »protocol-state-machine«

a_i = *protocol-state-machine***(**$\mathbf{x_i}$, $\mathbf{s_j}$**)**

Protocol-state-machine ist ein Automat, der auf ein Ereignis (Protokollelement $\mathbf{x_i}$, Timerabläufe, Statusmeldungen, ...) im Zustand $\mathbf{s_j}$ eine Aktion a_i auf der Empfängerseite durchführt.

Definition: »authenticity«

y_i = *authenticity***(**$\mathbf{x_i}$, $\mathbf{t_l}$**)**,

Authenticity ist eine Funktion, die die Echtheit des Protokollelementes $\mathbf{x_i}$ und des Transmitters $\mathbf{t_l}$ im Firewall-System verifiziert.

y_i = true
das Protokollelement x_i und der Transmitter t_l sind echt
y_i = false
das Protokollelement x_i und/oder der Transmitter t_l sind nicht echt

Definition: »result-of-decision«

r_i = *result-of-decision***(** *analysis***(**$\mathbf{x_i}$**)**, *security management***(rules))**

Result-of-decision ist eine Funktion, die entscheidet, ob das analysierte Protokollelement x_i mit den definierten Regeln im Firewall-System übereinstimmt.

neuKap14.fm Seite 473 Freitag, 18. Oktober 2002 5:12 17

r_i = true
das Protokollelement x_i wird weitergeleitet, evtl. als Beweissicherung der Aktion in einem Logbuch festgehalten
r_i = false
das Protokollelement x_i wird nicht weitergeleitet und es wird ein sicherheitsrelevantes Ereignis e_i erzeugt.

Definition: »analysis«

$e^* = analysis(\mathbf{x_i})$

Analysis ist eine Funktion, die das Protokollelement $\mathbf{x_i}$ analysiert. Die Funktion liefert in Abhängigkeit von vorherigen Analysen und sonstigen Zuständen des Firewall-Systems ein definiertes Ereignis **e***.

Definition: »security management«

$e^{**} = security\ management(\mathbf{rules})$

Security management ist eine Funktion, die in Abhängigkeit des Kommunikationspartners überprüft, welche Protokollelemente $\mathbf{x_i}$ oder Folgen von Protokollelementen zu welchen Zeiten durch das Firewall-System übertragen werden dürfen.

Definition: »functionality-of-the-firewall-system«

$z_i = functionality\text{-}of\text{-}the\text{-}firewall\text{-}system()$

In der Funktion »*functionality-of-the-firewall-system*« sind alle Standard-Sicherheitsdienste realisiert.

z_i = true
alle Funktionalitäten, die definiert sind, sind vorhanden und vertrauenswürdig
z_i = false
nicht alle Funktionalitäten, die definiert sind, sind vorhanden und/oder vertrauenswürdig

14.4 Angriffe auf das Firewall-System

In diesem Abschnitt werden die zusätzlichen potenziellen Bedrohungen in Verbindung mit der Einführung eines Firewall-Systems beschrieben.

	Angriffe auf das Firewall-Systems	
Angriffsart	Ziel des Angriffs	Beispiel
Manipulation des Firewall-Systems	Das Firewall-System wird von einem Angreifer manipuliert, um eine nicht erlaubte Aktion zu erlauben und dann durchzuführen.	Der Angreifer ändert das Regelwerk des Firewall-Systems so, dass er z. B. auf zu schützende Rechnersysteme zugreifen kann

Tabelle 14.6: Angriffe auf das Firewall-System

neuKap14.fm Seite 474 Freitag, 18. Oktober 2002 5:12 17

	Angriffe auf das Firewall-Systems	
Angriffsart	Ziel des Angriffs	Beispiel
Einbau einer Trap-Door	Der Hersteller des Firewall-Systems hat durch selbst definierte Protokollelemente, spezielle Abfolgen von Protokollelementen oder spezifischen Datenkonstellationen die Möglichkeit eingebaut, das Firewall-System zu überwinden.	Der Angreifer (Geheimdienste, Mafia, Konzerne, ...) kann von außen ungehindert auf die zu schützenden Rechnersysteme zugreifen.
Nutzung einer falschen Konfiguration des Firewall-Systems	Für jeden Dienst, der über einen Netzzugang ermöglicht werden soll, existiert ein »Daemon«, der falsch konfiguriert oder installiert werden kann, sodass er es ermöglicht, im Firewall-System beliebige privilegierte Kommandos ausführen zu lassen, mit denen ein Angriff durchgeführt werden kann.	Der Angreifer nutzt die Tatsache, dass eine falsche Konfiguration vorliegt, um z. B. an die »root«-Rechte des Firewall-Systems zu gelangen, um damit seine Ziele zu erreichen, z. B. die Rechte im Firewall-System zu ändern.
Nutzung von Implementierungsfehlern des Firewall-Systems	Der Angreifer nutzt Implementierungsfehler der Kommunikationsprotokolle oder -dienste des Firewall-Systems, um unerlaubte Aktionen ausführen zu können.	Der Angreifer nutzt einen Implementierungs- oder Designfehler, um z. B. die Rechte im Firewall-System zu ändern.

Tabelle 14.6: Angriffe auf das Firewall-System (Forts.)

14.5 Grundsätzliche Einflussfaktoren auf die Auswahl und Durchführung der Aktion auf der Empfängerseite

Im Folgenden werden die Funktionen und deren grundsätzlichen Einflussfaktoren aufgezeigt, die bei dem Kommunikationsmodell mit integriertem Firewall-System eine Rolle spielen. Es werden die Gründe festgehalten und erläutert, die sich für ein mögliches Fehlverhalten der Kommunikationsabläufe trotz integriertem Firewall-System herauskristallisiert haben.

14.5.1 Fehlerquellen durch Angriffe aus dem Netz

Funktion: authenticity(x_i, t_l)

Für den richtigen Kommunikationsablauf ist es wichtig, dass sowohl der Transmitter(t_l) authentisch/echt ist als auch das Protokollelement x_i authentisch/echt und unversehrt übertragen worden ist.

Einflussfaktoren:

- Vertrauenswürdigkeit des Netzes
- Vertrauenswürdigkeit des Kommunikationsteilnehmers

neuKap14.fm Seite 475 Freitag, 18. Oktober 2002 5:12 17

und/oder

- Gewährleistung der Authentikation des Kommunikationspartners
- Gewährleistung der Authentikation des Ursprungs der Daten

14.5.2 Fehlerquellen der Kommunikationslösung beim Receiver

Verantwortung des Anwenders

Funktion: protocol-state-machine(x_i, s_j)

Einflussfaktoren:

- **Konfiguration beim Empfänger:**
  Die Konfiguration des Kommunikationsprotokolls oder -dienstes hat Fehler, die zur Folge haben, dass trotz erlaubter Protokollelementen (x_i) eine nicht erlaubte Aktion auf der Empfängerseite durchgeführt wird.

Verantwortung des Herstellers der Kommunikationslösung

Funktion: protocol-state-machine(x_i, s_j)

Einflussfaktoren:

- **Implementierung beim Empfänger:**
  Die Implementierung des Kommunikationsprotokolls oder -dienstes hat Fehler, die zur Folge haben, dass trotz erlaubter Protokollelemente (x_i) eine nicht erlaubte Aktion auf der Empfängerseite durchgeführt wird.

14.5.3 Fehlerquellen des Firewall-Systems

Verantwortung des Anwenders

Funktion: security management(rules)

Einflussfaktoren:

- **Sicherheitspolitik**
  - Es wird mehr erlaubt, als für die eigentliche Aufgabenstellung der einzelnen Nutzer erforderlich ist.
  - Die unbeabsichtigte falsche Eingabe der Regeln führt zu einem Fehlverhalten des Firewall-Systems.
  - Die beabsichtigte falsche Eingabe der Regeln verfolgt das Ziel, das Firewall-System zu umgehen.
  - Die Einschränkung der Protokollelemente kann, z. B. durch Unwissenheit oder unrichtige Vorgabe, unzureichend sein.
  - Neue Angriffsmethoden, die dem Verantwortlichen der Firewall-Systems nicht bekannt sind, können deshalb auch nicht durch eine explizite Einschränkung verhindert werden.

neuKap14.fm Seite 476 Freitag, 18. Oktober 2002 5:12 17

Verantwortung des Herstellers des Firewall-Systems

Funktion: analysis(x_i)

Einflussfaktoren:

- **Tiefe der Analyse:**
  Die Analyse der Protokollelemente kann nicht detailliert genug Aussagen treffen, und damit nur eingeschränkt Aktionen verhindern. Sie kann in der Feststellung der Entscheidungskriterien und in deren Verdichtung zur Entscheidung »Durchlass oder Sperren« zu sehr begrenzt sein. Bei der Analyse der Protokollelemente können wichtige und/oder neue Entscheidungskriterien unberücksichtigt bleiben. Bei der Synthese der Kriterien zu Entscheidungen können Entscheidungsregeln nicht ausgereift oder nicht umfassend umgesetzt sein.

  Dieser Punkt geht einher mit der Komplexität der möglichen Einschränkungen.

Funktion: result-of-decision(analysis(x_i), security management(rules))

Einflussfaktoren:

- **Vertrauenswürdige Implementierung:**
  Unzureichende Qualität der Realisierung des Firewall-Systems:
  - Die Qualität der Realisierung eines Firewall-Systems ist derart, dass in bestimmten Situationen ein Fehlverhalten auftritt.
  - folgende Komponenten müssen betrachtet werden
    - Betriebssystem, auf dem die Firewall-Applikation läuft
    - Firewall-Applikation, Security Management
    - Hardware der Firewall-Elemente und des Security Managements
    - Authentikationskomponenten der Kommunikationspartner

14.5.4 Sicherheitsdienste eines Firewall-Systems

Funktion: functionality-of-the-firewall-system( )

Die folgende Tabelle beschreibt die Standardsicherheitsdienste eines Firewall-Systems. Für jeden Dienst wird aufgelistet, welche Informationen vom Firewall-Systemen überprüft werden, welche Festlegungen und Maßnahmen getroffen werden, was geprüft wird und welchen Einfluss das auf Sicherheit und Vertrauenswürdigkeit von Firewall-Systemen hat.

.

neuKap14.fm Seite 477 Freitag, 18. Oktober 2002 5:12 17

Sicherheitsdienst	Überprüfung/Festlegung/Maßnahme	Was wird geprüft?	Einfluss auf Sicherheit und Vertrauenswürdigkeit
Zugangskontrolle auf Netzwerkebene	Welche Rechnersysteme (Transmitter, Receiver) dürfen über das Firewall-System miteinander kommunizieren?	– IP-Adressen der beteiligten Rechnersysteme – Zeit, zu der eine Aktion zulässig ist	– Vertrauenswürdige Implementierung – Vertrauenswürdigkeit des Netzes – Vertrauenswürdigkeit des Kommunikationspartners – Sicherheitspolitik
Zugangskontrolle auf Benutzerebene	Welche Benutzer dürfen über das Firewall-System eine Kommunikation aufbauen?	– Identität des Benutzers – Authentikation des Benutzers – Zeit, zu der eine Aktion zulässig ist	– Vertrauenswürdige Implementierung – Gewährleistung der Authentikation des Kommunikationspartners – Sicherheitspolitik
Zugangskontrolle auf Datenebene	Dürfen die Daten eines definierten Benutzers über das Firewall-System übertragen werden?	– Identität des Absenders der Daten – Authentikation des Absenders der Daten – Integrität der Daten – Zeit, zu der eine Aktion zulässig ist	– Vertrauenswürdige Implementierung – Gewährleistung der Authentikation des Ursprungs der Daten – Sicherheitspolitik
Rechteverwaltung	Festlegung, mit welchen Protokollen und Diensten und zu welchen Zeiten über das Firewall-System eine Kommunikation stattfinden darf.	– Header-Informationen auf den verschiedenen Schichten – Zeit, zu der eine Aktion zulässig ist	– Vertrauenswürdige Implementierung – Gewährleistung der Datenunversehrheit – Tiefe der Analyse – Sicherheitspolitik
Kontrolle auf Anwendungsebene	Überprüfung, ob Kommandos genutzt oder Dateninhalte übertragen werden, die nicht zur, durch die Anwendung definierten, Aufgabenstellung gehören.	– Kommandos und Dateninhalte der verschiedenen Anwendungen – Zeit, zu der eine Aktion zulässig ist	– Vertrauenswürdige Implementierung – Gewährleistung der Datenunversehrheit – Tiefe der Analyse – Sicherheitspolitik

Tabelle 14.7: Standardsicherheitsdienste eines Firewall-Systems

neuKap14.fm Seite 478 Freitag, 18. Oktober 2002 5:12 17

Sicherheitsdienst	Überprüfung/Festlegung/Maßnahme	Was wird geprüft?	Einfluss auf Sicherheit und Vertrauenswürdigkeit
Entkoppelung von Diensten	Entkoppeln verhindert, dass Implementierungsfehler, Schwachstellen und Konzeptionsfehler der Dienste Möglichkeit für Angriffe bieten.	– Kommandos – Zeit, zu der eine Aktion zulässig ist	– Vertrauenswürdige Implementierung – Konzept der Entkopplung
Beweissicherung und Protokollauswertung	Verbindungsdaten und sicherheitsrelevante Ereignisse werden protokolliert und können für die Beweissicherung von Benutzerhandlungen und für die Erkennung von Sicherheitsverletzungen ausgewertet werden.	– Aktionen und sicherheitsrelevante Ereignisse – Zeit, zu der eine Aktion zulässig ist	– Vertrauenswürdige Implementierung – Sicherheitspolitik – Konzept der Beweissicherung und Protokollauswertung
Alarmierung	Besonders sicherheitsrelevante Ereignisse werden an ein Security Management gesendet, damit bei Sicherheitsverletzungen schnell reagiert werden kann.	– Zeit, zu der eine Aktion zulässig ist	– Vertrauenswürdige Implementierung – Vertrauenswürdigkeit des Netzes – Sicherheitspolitik
Verbergen der internen Netzstruktur	Die Struktur des zu schützenden Netzes soll gegenüber dem unsicheren Netz verborgen werden. Es soll nicht sichtbar sein, ob im zu schützenden Netz 10, 100, 1 000 oder 10 000 Rechnersysteme vorhanden sind.	– IP-Adressen	– Vertrauenswürdige Implementierung – Konzept des Verbergens der internen Netzstruktur (dual-homed Gateway)

Tabelle 14.7: Standardsicherheitsdienste eines Firewall-Systems (Forts.)

neuKap14.fm Seite 479 Freitag, 18. Oktober 2002 5:12 17

14.5.5 Sicherheitsziele bei der Umsetzung eines Firewall-Systems

Es gibt keine hundertprozentige Sicherheit von Firewall-Elementen. Über die Wirksamkeit gegen die definierten Angriffe werden in der Praxis keine qualitativen und vergleichbaren Aussagen gemacht, da es keine einheitlichen Sicherheitskriterien gibt.

Aus diesem Grund ist es zweckmäßig, die Betrachtung auf die Unsicherheit von Firewall-Elementen zu lenken. Ziel ist es, diese Unsicherheit umfassend zu erkennen, zu benennen und zu minimieren, denn durch ein sinkendes Maß an Unsicherheit steigt die Sicherheit über die Einschätzung des Risikos.

Idee dieser Betrachtung

Die Wahrscheinlichkeit, dass eine Unsicherheit im Firewall-System (im Sicherheitsmechanismus, der gegen einen definierten Angriff wirken soll) einen erfolgreichen Angriff ermöglicht und dadurch ein Schaden auftritt, wird folgendermaßen definiert:

Schaden = p(Unsicherheit-1) * p(Unsicherheit-2) * ... * p(Unsicherheit-n)

Beispiele von Unsicherheiten

1. Kryptographische Algorithmen

In diesem Beispiel wird die »Sicherheit« von kryptographischen Algorithmen, mit denen die Authentikation oder die Verschlüsselung durchgeführt wird, betrachtet.

Annahme:

Ein Angreifer versucht, durch die vollständige Suche aller möglichen Schlüsselkombinationen den richtigen Schlüssel zu finden und dann einen Angriff durchzuführen. Dazu braucht er bei der Verwendung des IDEA-Algorithmus (128-Bit-Schlüssel) im Durchschnitt die folgende Anzahl von Versuchen:

2^{127} -> 1,7 * 10^{38}

Die angenommene Rechnenzeit eines Angreifers beträgt pro Versuch einer Schlüsselkombination 0.000 001 s (1 µs).

Damit benötigt ein potenzieller Angeifer 5,3 * 10^{24} Jahre.

Die Wahrscheinlichkeit, dass dieser Angriff erfolgreich durchgeführt werden kann, kommt praktisch nicht vor, denn sie wird mit unvorstellbar geringen 1,7*10^{-38} beziffert!

neuKap14.fm Seite 480 Freitag, 18. Oktober 2002 5:12 17

2. Hacker im Internet

Einer der unzähligen Hacker im Internet greift auf ein schützenswertes Rechnersystem zu und kopiert die Werte des Unternehmens. Da nach einer Studie im Mittel innerhalb von 12 Minuten der erste Hacker versucht zuzugreifen, wenn man sich an das Internet ankoppelt, wird die Wahrscheinlichkeit, dass ein Schaden auftritt, mit 99% festgelegt.

Aus diesen Überlegungen heraus sollen Ziele für eine praktische Sicherheit definiert werden.

Sicherheitsziele bei der Umsetzung eines Firewall-Systems sind:

1. alle Unsicherheiten mit großer Wahrscheinlichkeit vollständig zu eliminieren
2. möglichst vielen Unsicherheiten mit passenden Sicherheitsmechanismen entgegenzuwirken und damit die Wahrscheinlichkeit eines Schadens durch einen erfolgreichen Angriff auf eine praktisch nicht vorkommende Größe zu minimieren
3. Unsicherheiten, die nicht verhindert werden können, zu erkennen, um nach einem eventuellen Angriff angemessen reagieren zu können, mit dem Ziel, den Schaden zu minimieren
4. Angriffe im Vorfeld zu erkennen, damit erst kein Schaden auftreten kann

Damit Firewall-Systeme in ihrer Gesamtheit zur Reduzierung der Verwundbarkeit eingesetzt werden können, ist es Ziel, nachvollziehbare Aussagen über die Wirkung von Firewall-Systemen gegen definierte Angriffe sowie über Faktoren, die deren Möglichkeiten und Grenzen beeinflussen, zu erarbeiten.

Außerdem werden Randbedingungen und Einschränkungen für einen vertretbaren Einsatz von sicheren und vertrauenswürdigen Firewall-Systemen aufgezeigt.

14.5.6 Einflussfaktoren auf die Sicherheit und Vertrauenswürdigkeit von Firewall-Systemen

Im folgenden Abschnitt werden unter Berücksichtigung der grundsätzlichen Ergebnisse der Diskussion des Kommunikationsmodells mit integriertem Firewall-System die Faktoren herausgearbeitet, die auf die Sicherheit und Vertrauenswürdigkeit von Firewall-Systemen Einfluss haben.

Die Einflussfaktoren eines Firewall-Systems werden unterteilt in:

- Sicherheitsdienste und -mechanismen des eigentlichen Firewall-Systems,
- die Einsatzumgebung eines Firewall-Systems,
- die Evaluierung und Zertifizierung des Firewall-Systems und
- die Einflussfaktoren der eigenen Organisation.

neuKap14.fm Seite 481 Freitag, 18. Oktober 2002 5:12 17

Außerdem wird dargestellt, wie die Einflussfaktoren gegen die verschiedenen Angriffsarten wirken.

Die strukturellen Zusammenhänge über Angriffe und die Wirkung der verschiedenen Einflussfaktoren wie Sicherheitsdienste/-mechansimen/-funktionen werden im Folgenden erarbeitet und in Form von Tabellen zusammenfassend dargestellt.

Definition der verwendeten Symbole:

Symbol	Kurzbeschreibung	Definition
●	sehr große Wirkung	Der entsprechende Sicherheitsmechanismus wirkt so stark gegen den definierten Angriff, dass praktisch kein Schaden auftreten kann. Stärke des Sicherheitsmechanismus: »hoch«
◕	große Wirkung	Der entsprechende Sicherheitsmechanismus wirkt stark gegen den definierten Angriff, sodass normalerweise kein Schaden auftreten kann. Stärke des Sicherheitsmechanismus: »hoch/mittel«
◑	Wirkung	Der entsprechende Sicherheitsmechanismus wirkt gegen den definierten Angriff, sodass typischerweise kein Schaden auftreten kann. Stärke des Sicherheitsmechanismus: »mittel«
◔	geringe Wirkung	Der entsprechende Sicherheitsmechanismus wirkt gering gegen den definierten Angriff, sodass unbeabsichtigt kein Schaden auftreten kann. Stärke des Sicherheitsmechanismus: »niedrig«
○	keine Wirkung	Der entsprechende Sicherheitsmechanismus hat gegen den definierten Angriff keine Wirkung, sodass ein Schaden auftreten kann.
✦	Grundlage für die Wirkung	Der entsprechende Sicherheitsmechanismus ist eine Grundlage, damit das Firewall-System überhaupt gegen Angriffe wirken kann.

Tabelle 14.8: Definition der verwendeten Symbole

Definitionen von »niedrig«, »mittel« und »hoch« siehe Kapitel 13.4.1.1.

14.5.7 Die Wirkung der Sicherheitsdienste

In der folgenden Tabelle wird die Wirkung der einzelnen Sicherheitsdienste gegen die definierten Angriffe dargestellt.

neuKap14.fm Seite 482 Freitag, 18. Oktober 2002 5:12 17

Angriffsart	Sicherheitsfunktionen	Zugangskontrolle auf Netzwerkebene	Zugangskontrolle auf Benutzerebene	Zugangskontrolle auf Datenebene	Rechteverwaltung	Kontrolle auf Anwendungsebene	Entkoppelung von Diensten	Beweissicherung u. Protokollauswertung	Alarmierung	Verbergen der internen Netzstruktur
Angriffe durch einen Dritten	Wiederholen oder Verzögern von Protokollelementen	◔	◕	◕	◕	◕	○	◔	◔	○
	Einfügen oder Löschen von Daten in den Protokollelementen	○	○	●	◕	◕	○	◔	◔	○
	Modifikation der Daten in den Protokollelementen	○	○	●	◕	◕	○	◔	◔	○
	Boykott des Receivers	○	○	○	○	○	○	◔	◔	◕
	Trittbrettfahrer	◔	◕	●	○	○	○	○	○	○
	Senden von Malware (Viren, Würmer, Trojanische Pferde,...)	○	○	○	◑	◕	○	◔	◔	○
Angriffe durch den Transmitter	Aufbau u. Nutzung von Kommunikationsverbindungen	◔	◔	◔	◕	◕	○	◑	◔	○
	Nutzung von Kommunikationsprotokollen und -diensten	○	○	○	●	●	○	◑	◔	○
	Vortäuschen einer falschen Identität (Maskerade-Angriff)	◔	●	●	○	○	○	○	○	○
	Java, ActiveX, ... Angriffe	○	○	○	○	◕	○	◔	◔	○
	falsche Konfiguration/Implementierungsfehler	○	○	○	○	○	◕	◑	◔	○
	Leugnen der Kommunikationsbeziehung	○	○	○	○	○	○	◕	○	○
Vorbereitung für Angriffe	Social Engineering	○	○	○	○	○	○	○	○	○
	Analyse mit Hilfe von Scannerprogrammen	○	○	○	○	○	○	◔	◔	●
Angriffe auf das Firewall-System	Manipulation des Firewall-Systems	○	○	○	○	○	○	○	○	○
	Einbau einer Trap-Door	○	○	○	○	○	○	○	○	○
	Nutzung einer falschen Konfiguration des Firewall Systems	○	○	○	○	○	○	○	○	○
	Nutzung von Implementierungsfehlern des Firewall Systems	○	○	○	○	○	○	○	○	○
	interne Angriffe	○	○	○	○	○	○	○	○	○

● sehr große Wirkung ◕ große Wirkung ◑ Wirkung
◔ wenig Wirkung ○ keine Wirkung ◆ Grundlage für die Wirkung

Abb. 14.8: Die Wirkung der Sicherheitsfunktionen

Bewertung der eigentlichen Sicherheitsdienste

Die beschriebenen Sicherheitsdienste erbringen sehr unterschiedliche Sicherheitsfunktionalitäten und wirken gegen sehr unterschiedliche Angriffe. Im Folgenden werden die Sicherheitsdienste beschrieben und anschließend die Wirkung gegen die definierten Angriffe begründet.

14.5.7.1 Zugangskontrolle auf der Netzwerkebene

Der Sicherheitsdienst »Zugangskontrolle auf der Netzwerkebene« überprüft, welche Rechnersysteme (Transmitter, Receiver, bzw. deren IP-Adressen) über das Firewall-System miteinander kommunizieren dürfen.

neuKap14.fm Seite 483 Freitag, 18. Oktober 2002 5:12 17

Beurteilung der Wirkung gegen die verschiedenen Angriffsarten:

Da im Prinzip jeder Transmitter jede IP-Adresse annehmen kann, ist mit diesem Sicherheitsdienst nur eine geringe Wirkung gegen die entsprechenden Angriffe zu erzielen (siehe Tabelle).

14.5.7.2 Zugangskontrolle auf Benutzerebene

Der Sicherheitsdienst »Zugangskontrolle auf Benutzerebene« sorgt für die Identifikation und Authentikation der Benutzer, die über das Firewall-System eine Kommunikation durchführen dürfen.

Beurteilung der Wirkung gegen die verschiedenen Angriffsarten:

Falls die Zugriffskontrolle auf der Benutzerebene mit starken Authentikationsmechanismen durchgeführt wird, ist mit diesem Sicherheitsdienst eine große bis sehr große Wirkung gegen die entsprechenden Angriffe zu erzielen (siehe Tabelle).

14.5.7.3 Zugangskontrolle auf Datenebene

Der Sicherheitsdienst »Zugangskontrolle auf Datenebene« überprüft, ob die Daten eines definierten Benutzers über das Firewall-System übertragen werden dürfen. Dieser Sicherheitsdienst stellt die Unversehrtheit sowie die Urheberschaft der gesendeten Daten sicher.

Technisch ist denkbar, dass alle Protokollelemente vom Transmitter digital signiert und im Firewall-System überprüft werden. Es könnte aber auch ein ganzes Datenobjekt, z. B. eine E-Mail, signiert werden. Dann müsste die Überprüfung der Signatur beispielsweise in einem SMTP-Proxy des Firewall-Systems realisiert werden.

In der Praxis werden Sicherheitsmechanismen wie die Digitale Signatur aber oft in der Client-Software wie Microsoft Outlook, Microsoft Office oder Lotus Notes realisiert, sodass die Daten das Firewall-System ungeprüft passieren.

Beurteilung der Wirkung gegen die verschiedenen Angriffsarten:

Falls die Zugriffskontrolle auf der Datenebene mit starken Sicherheitsmechanismen durchgeführt wird, ist mit diesem Sicherheitsdienst eine große bis sehr große Wirkung gegen die entsprechenden Angriffe zu erzielen (siehe Tabelle).

14.5.7.4 Rechteverwaltung

Der Sicherheitsdienst »Rechteverwaltung« kontrolliert, mit welchen Kommunikationsprotokollen und -diensten und zu welchen Zeiten über das Firewall-System eine Kommunikation stattfinden darf. Hierdurch kann die Kommunikation über das Firewall-System auf das notwendige Maß reduziert werden.

neuKap14.fm Seite 484 Freitag, 18. Oktober 2002 5:12 17

Beurteilung der Wirkung gegen die verschiedenen Angriffsarten:

Durch die Reglementierung der Kommunikationsmöglichkeiten ist mit diesem Sicherheitsdienst eine große Wirkung gegen die entsprechenden Angriffe zu erzielen (siehe Tabelle).

14.5.7.5 Kontrolle auf der Anwendungsebene

Mithilfe des Sicherheitsdienstes »Kontrolle auf der Anwendungsebene« wird überprüft, ob Kommandos und Klassen von Applets (Java, ActiveX, ...) genutzt oder Dateninhalte übertragen werden, die nicht gewünscht sind. Dadurch können unerwünschte Aktionen verhindert werden.

Beurteilung der Wirkung gegen die verschiedenen Angriffsarten:

Durch die Reglementierung der Kommunikationsmöglichkeiten auf der Anwendungsebene ist mit diesem Sicherheitsdienst eine große Wirkung gegen die entsprechenden Angriffe zu erzielen (siehe Tabelle).

14.5.7.6 Entkopplung von Diensten

Der Sicherheitsdienst »Entkoppeln von Diensten« verhindert, dass Implementierungsfehler, Schwachstellen und Konzeptionsfehler der Kommunikationsdienste beim Receiver Möglichkeiten für Angriffe bieten. Die Rechnersysteme im zu schützenden Netz werden durch diesen Dienst (Application-Gateway mit Proxy) entkoppelt.

Beurteilung der Wirkung gegen die verschiedenen Angriffsarten:

Durch die Entkopplung von Diensten ist eine große Wirkung gegen die entsprechenden Angriffe zu erzielen (siehe Tabelle).

14.5.7.7 Beweissicherung und Protokollauswertung

Durch den Sicherheitsdienst »Beweissicherung und Protokollauswertung« werden Verbindungsdaten und sicherheitsrelevante Ereignisse protokolliert und können für die Beweissicherung von Benutzerhandlungen sowie die Erkennung von Sicherheitsverletzungen ausgewertet werden.

Durch die Protokollierung von Benutzerhandlungen werden die Benutzer motiviert, nur das zu tun, was sie für ihre Aufgabenstellung wirklich benötigen.

Mithilfe der Auswertung von sicherheitsrelevanten Ereignissen ist es möglich, im Nachhinein auf Angriffe zu reagieren und so eventuelle weitere Angriffe zu verhindern.

neuKap14.fm Seite 485 Freitag, 18. Oktober 2002 5:12 17

Beurteilung der Wirkung gegen die verschiedenen Angriffsarten:

Durch die Beweissicherung und Protokollauswertung ist in Abhängigkeit von den Angreifern (von anonymen Fremden bis hin zu bekannten Kommunikationspartnern) eine geringe bis große Wirkung gegen die entsprechenden Angriffe zu erzielen (siehe Tabelle). Eine große Wirkung kann bei dem Angriff »Leugnen der Kommunikationsbeziehung« erreicht werden, wenn der Kommunikationspartner bekannt ist. Ein solcher Sicherheitsdienst kann auch Bestandteil in einem Wartungsvertrag sein, z. B. bei einem Service, der über ein Firewall-System realisiert wird.

14.5.7.8 Alarmierung

Mithilfe des Sicherheitsdienstes »Alarmierung« werden besonders sicherheitsrelevante Ereignisse an ein Security Management gesendet, damit bei Sicherheitsverletzungen schnell reagiert werden kann. Für die erlaubten Transmitter stellt dieser Sicherheitsdienst auch eine Abschreckung dar.

Beurteilung der Wirkung gegen die verschiedenen Angriffsarten:

Durch die Alarmierung ist wenig Wirkung gegen die entsprechenden Angriffe zu erzielen (siehe Tabelle). Es kann aber im Nachhinein auf Angriffe reagiert werden, um zukünftige Angriffe möglichst zu verhindern und damit Schäden zu minimieren.

14.5.7.9 Verbergen der internen Netzstruktur

Mithilfe des Sicherheitsdienstes »Verbergen der internen Netzstruktur« wird die Struktur des zu schützenden Netzes gegenüber dem unsicheren Netz verborgen. Dadurch kann die Analyse des zu schützenden Netzes verhindert werden. Einem Angreifer ist es nicht mehr möglich, festzustellen, wie viele Rechnersysteme im zu schützenden Netz angeschlossen sind und welche Dienste auf den Rechnersystemen aktiviert sind.

Beurteilung der Wirkung gegen die verschiedenen Angriffsarten:

Durch das Verbergen der internen Netzstruktur ist eine sehr große Wirkung gegen Analysen mithilfe von Scannerprogrammen zu erzielen (siehe Tabelle).

14.5.7.10 Grundlegende Aspekte für die Erbringung der Sicherheitsdienste

Im Folgenden werden die wichtigsten grundlegenden Aspekte, die für die Erbringung der Sicherheitsdienste notwendig sind, dargestellt und die entsprechenden Einflussfaktoren aufgezeigt.

neuKap14.fm Seite 486 Freitag, 18. Oktober 2002 5:12 17

Tiefe der Analyse

- Die Tiefe der Analyse, die ein Firewall-Element in einem Firewall-System erreichen kann, ist ein entscheidender Faktor für die Sicherheit des Systems. Die folgenden Einflussfaktoren sind dabei von großer Bedeutung:
- Protokollschichten, auf denen eine Analyse stattfindet
  - Netzzugangsschicht
  - Netzwerkschicht
  - Transportschicht
  - Anwendungsschicht
- Komplexität der Kontrolle in den Schichten
- Erkennen von dynamischen Prozessen durch Protokollierung von Ereignissen
- Überprüfung der Zeiten, wann eine Kommunikation stattfinden darf
- Zeitpunkt der Analyse
  - nur bei Beginn der Kommunikation
  - kontinuierlich während der gesamten Kommunikation

Komplexität der Regeln

Auch die Komplexität der Regeln ist ein wichtiger Aspekt für die Sicherheit von Firewall-Systemen. Die folgenden Einflussfaktoren spielen hierbei eine Rolle:

- Eindeutigkeit der Regeln (organisatorische Anforderung)
  Bei der Festlegung der Regeln muss darauf geachtet werden, dass Regeln immer eindeutig zu interpretieren sind, damit ein hohes und eindeutiges Maß an Sicherheit gewährleistet werden kann. Mithilfe des Einbindungskonzepts und des Netzkonzepts kann konzeptionell darauf geachtet werden, dass die Anzahl der Regeln per Definition klein bleibt.
- Anzahl der notwendigen Regeln
  - Einbindungskonzept: An welcher Stelle werden die Sicherheitsfunktionen eingebunden?
  - Firewall-Konzept: Packet Filter, dual-homed Application Gateway, ...
  - Netzkonzept: Beispielsweise kann die Definition der IP-Adressen und der Domänen eine klarere Übersicht schaffen und damit dem Admisitrator die Definition der Regeln extrem vereinfachen.

Komplexität der möglichen Einschränkungen

Der Umfang der Einschränkungen, die mithilfe eines Firewall-Systems realisiert werden können, ist auch in Abhängigkeit von der Tiefe der Analyse zu betrachten. Je größer der Umfang ist, desto besser können Angriffe verhindert werden. Folgende Einflussfaktoren können betrachtet werden:

- Zeit (Datum, Uhrzeit, ...), zu der eine Kommunikation stattfinden darf
- Ort (innen, außen, Abteilung, ...)
  - Strukturierung der IP-Adressen

neuKap14.fm Seite 487 Freitag, 18. Oktober 2002 5:12 17

- Protokolle (IP, TCP, UDP, ICMP, ...)
- Eigenschaften (Fragmentierung, Source-Routing, ...)
- Dienste (HTTP, FTP, ...)
- Rechnersysteme (IP-Adressen, ...)
- Personen (ID, Profile, ...)

Stärke des Authentikationsmechanismus

Da es besonders wichtig ist, zu erkennen, welcher User tatsächlich über das Firewall-System eine Kommunikation durchführt, ist die Stärke des Authentikationsmechanismus von hoher Relevanz. Die folgenden Einflussfaktoren sind zu berücksichtigen:

- kryptographische Verfahren: anerkanntes sicheres Verfahren, Schlüssellänge, richtige Implementierung, sichere Schlüsselgenerierung
- Zufallszahlengeneratoren: Gütekriterien, Streuung, Periodizitität, Gleichverteilung
- Security Token: sicheres Security Management, sichere Schlüsselspeicherung, sichere Distribution, sicheres Verfahren zur Aktivierung von Security Token, etc.
- Schlüsselspeicherung: nicht auslesbar über Angriffe
- Schutzmechanismen des Schlüssels: verschlüsselte Speicherung, Speicherung in einem Security-Modul
- Sicherheitsinfrastruktur
- eindeutige Namensvergabe: Es muss sichergestellt werden, dass alle User, die über das Firewall-System kommunizieren, einen eindeutigen Namen besitzen, damit sie eindeutig zu identifizieren sind. Idealerweise sollte hier auf eine internationale Infrastruktur aufgebaut werden (PKI, Directory Service, ...).
- Methode: auch die Methode der Authentikation spielt für die Sicherheit eine besondere Rolle.
  - einmalige Authentikation (Problem:Trittbrett-Fahrer)
  - anhaltende Authentikation
  - explizite Authentikation
  - implizite Authentikation durch die Verschlüsselung

Application Gateway mit Proxy-Technik

Das Konzept des Application Gateway mit Proxy-Technik hat auf die Qualität der Sicherheit einen starken Einfluss. Folgende Einflussfaktoren sind zu betrachten:

- sicheres Design-Konzept, da kleine, gut überprüfbare Module (Proxies)
- Konzentration auf das Wesentliche
- höhere Sicherheit durch die ausnahmslose Übertragung aller Pakete durch den Proxy
- Der Kommunikationspartner der Rechnersysteme, die über das Application Gateway kommunizieren, ist der Proxy; dadurch kann eine echte Entkopplung der Dienste erreicht werden.

neuKap14.fm Seite 488 Freitag, 18. Oktober 2002 5:12 17

- Verbindungsdaten und Applikationsdaten können protokolliert werden, wodurch die Handlungen der Benutzer, die über das Application Gateway kommunizieren, festgehalten werden können.
- Verbergen der internen Netzstruktur
- Sicherheitsfunktionen für die Anwendungen werden zur Verfügung gestellt
- (Kommando-, Datei- und Daten-Filter usw.)
- Durchführung einer Network Address Translation

14.5.8 Die Wirkung der Einsatzumgebung

In der folgenden Tabelle wird die Wirkung der Einsatzumgebung gegen Angriffe dargestellt.

Angriffsart	Einsatzumgebung	Kommunikationssystem			Firewall-System		
		Vertrauenswürdigkeit des Netzes	Vertrauenswürdigkeit des Kommunikationspartners		sicheres Security Management	sicheres Betriebssystems	Firewall-Schutzmechanismen
Angriffe durch einen Dritten	Wiederholen oder Verzögern von Protokollelementen	◕	○		◑	○	○
	Einfügen oder Löschen von Daten in den Protokollelementen	◕	○		◑	○	○
	Modifikation der Daten in den Protokollelementen	◕	○		◑	○	○
	Boykott des Receivers	◕	○		◑	○	○
	Trittbrettfahrer	◕	○		◑	○	○
	Senden von Malware (Viren, Würmer, Trojanische Pferde,...)	◕	○		◑	○	○
Angriffe durch den Transmitter	Aufbau u. Nutzung von Kommunikationsverbindungen	○	◕		◑	○	○
	Nutzung von Kommunikationsprotokollen und -diensten	○	◕		◑	○	○
	Vortäuschen einer falschen Identität (Maskerade-Angriff)	○	◕		◑	○	○
	Java, ActiveX, ... Angriffe	○	◕		◑	○	○
	falsche Konfiguration/Implementierungsfehler	○	◕		◑	◑	○
	Leugnen der Kommunikationsbeziehung	○	◕		◑	○	○
Vorbereitung für Angriffe	Social Engineering	○	○		○	○	○
	Analyse mit Hilfe von Scannerprogrammen	◕	○		○	◑	○
Angriffe auf das Firewall-System	Manipulation des Firewall-Systems	◑	◑		◑	◕	●
	Einbau einer Trap-Door	◑	◑		○	○	○
	Nutzung einer falschen Konfiguration des Firewall-Systems	◑	◑		◑	◕	◕
	Nutzung von Implementierungsfehlern des Firewall Systems	◑	◑		◑	◕	◕
	interne Angriffe	○	○		○	○	○

● sehr große Wirkung ◕ große Wirkung ◑ Wirkung
◔ wenig Wirkung ○ keine Wirkung ◆ Grundlage für die Wirkung

Abb. 14.9: Die Wirkung der Einsatzumgebung

neuKap14.fm Seite 489 Freitag, 18. Oktober 2002 5:12 17

Bewertung der Einsatzumgebung eines Firewall-Systems

Die Einsatzumgebung eines Firewall-Systems bestimmt ebenfalls den Wirkungsgrad der Sicherheitsmechanismen und stellt somit einen großen Einflussfaktor auf die Sicherheit von Firewall-Systemen da.

Wenn ein Firewall-System z. B. in der internen Organisation eingesetzt wird und vorausgesetzt werden kann, dass die internen Mitarbeiter keine potenziellen Angreifer sind, kann eine höhere Sicherheit dargestellt werden, als wenn das Firewall-System im Internet eingesetzt wird, wo per Definition alle anderen als aktive Angreifer zu sehen sind.

Die Einflussfaktoren auf die Wirkung von Sicherheit und Vertrauenswürdigkeit werden im Folgenden beschrieben. Dies sind wichtige Randbedingungen für den sicheren und vertrauenswürdigen Einsatz von Firewall-Systemen.

14.5.8.1 Vertrauenswürdigkeit des Netzes

Damit eine Wirkung gegen Angriffe erzielt werden kann, müssen die folgenden Aspekte sicher und vertrauenswürdig realisiert sein.

- Wenn das Netz in der eigenen Verantwortung liegt:
  - Eine Evaluierung der Sicherheitsdienste des Netzes wurde durchgeführt.
  - Die Sicherheit des Netzes wird regelmäßig überprüft.
  - Das Netz ist nicht für jeden offen.
- Wenn das Netz nicht in der eigenen Verantwortung liegt:
  - Die Sicherheitsdienste (VPN, geschlossene Benutzergruppe, ...), die das Netz selbst anbietet, werden genutzt.
  - Die Vertrauenswürdigkeit der Betreiber des Netzes ist überprüft worden.
  - Die Teilnehmer im Netz haben den gleichen oder einen ähnlichen Schutzbedarf.
  - Eine Evaluierung der Sicherheitsdienste des Netzes wurde durchgeführt.
  - Die Sicherheit des Netzes wird regelmäßig überprüft.

Beurteilung der Wirkung gegen die verschiedenen Angriffsarten:

Durch die Vertrauenswürdigkeit des Netzes ist eine große Wirkung gegen Angriffe durch Dritte zu erzielen (siehe Tabelle).

14.5.8.2 Vertrauenswürdigkeit des Kommunikationspartners

Die Kommunikationspartner sind Teil der eigenen Organisation und arbeiten unter der gleichen Sicherheitspolitik. Deshalb wird das Angriffspotenzial der Kommunikationspartner als sehr gering eingeschätzt.

neuKap14.fm Seite 490 Freitag, 18. Oktober 2002 5:12 17

Beurteilung der Wirkung gegen die verschiedenen Angriffsarten:

Durch die Vertrauenswürdigkeit des Kommunikationspartners ist eine große Wirkung gegen Angriffe durch den Kommunikationspartner zu erzielen (siehe Tabelle).

14.5.8.3 Sicheres Security Management

Das Security Management muss gegen Angriffe resistent sein. Folgende Einflussfaktoren sind dabei zu berücksichtigen:

- Benutzerfreundlichkeit
- Verhinderung von Mehrfacheinträgen
- Widerspruchsfreiheit von Regeln
- Zugangskontrolle im Security Management
- Rechteverwaltung der Aktionen des Security Managements
- Verschlüsselung der sicherheitsrelevanten Informationen im Security Management
- Protokollierung der Ereignisse im Security Management
- von den Firewall-Elementen getrenntes Security Management

Das Security Management muss in verschiedenen Umgebungen einsetzbar sein und muss daher die folgenden Eigenschaften aufweisen:

- zentrales Security Management
- Verwaltung mehrerer Firewall-Systeme
- Verwaltung geschachtelter Firewall-Systeme

Ein sicheres Management ist die Grundlage für die Wirkung der eigentlichen Sicherheitsdienste des Firewall-Systems.

Beurteilung der Wirkung gegen die verschiedenen Angriffsarten:

Durch die Verwendung eines sicheren Security Managements bei einer Firewall-Lösung ist eine Wirkung gegen die entsprechenden Angriffe zu erzielen (siehe Tabelle).

14.5.8.4 Sicheres Betriebssystem

Für den sicheren Betrieb eines Firewall-Systems ist die Verwendung eines sicheren Betriebssystems von entscheidender Wichtigkeit. Dazu müssen unterschiedliche Faktoren bei der Software-Entwicklung berücksichtigt werden /Pres97/. Die folgenden Gesichtspunkte stellen einen Überblick da:

- schlanker Kernel, damit die Gefahr von Sicherheitslücken oder funktionellen Fehlern minimal ist

neuKap14.fm Seite 491 Freitag, 18. Oktober 2002 5:12 17

- Kernel als monolithischen Block aufbauen, damit sichergestellt wird, dass einzelne Module nicht ausgetauscht werden können
- nur die Treiber und Netzwerkeigenschaften aktivieren, die für den Firewall-Betrieb notwenig sind (z. B. kein IP-Forwarding)

Durch die Verwendung eines sicheren Betriebssystems werden die Unsicherheiten des Firewall-Systems selber weiter minimiert.

Beurteilung der Wirkung gegen die verschiedenen Angriffsarten:

Durch die Verwendung eines sicheren Betriebssystems bei einer Firewall-Lösung ist eine bis zu große Wirkung gegen die entsprechenden Angriffe zu erzielen (siehe Tabelle). Ein solches sicheres Betriebssystem sorgt dafür, dass weniger Konfigurationsfehler auftreten können und dass weniger Implementierungsfehler vorhanden sind. Besonders bei Angriffen auf das Firewall-System kann hierdurch eine große Wirkung erzielt werden.

14.5.8.5 Firewall-Schutzmechanismen

Das Firewall-System selbst bietet Sicherheitsfunktionen, die gegen Angriffe auf das Firewall-System wirken. Folgende Einflussfaktoren müssen berücksichtigt werden:

- Überprüfung der Veränderung der Software und des Regelwerkes
- sicherer Betrieb des Firewall-Systems
- Überprüfung des Überlaufs von Logbüchern und Speichermedien
- Überprüfung, ob sich die Firewall-Software in einem definierten Zustand befindet
- Vertauenswürdiger Zugriff des Security Managements auf das Regelwerk

Mithilfe der Firewall-Schutzmechanismen können Manipulationen am Firewall-System erkannt und verhindert werden.

Beurteilung der Wirkung gegen die verschiedenen Angriffsarten:

Durch die Verwendung von Firewall-Schutzmechanismen ist eine große bis sehr große Wirkung gegen die entsprechenden Angriffe auf das Firewall-System zu erzielen (siehe Tabelle).

Wenn ein Firewall-System z. B. in der internen Organisation eingesetzt wird und vorausgesetzt werden kann, dass die internen Mitarbeiter keine potenziellen Angreifer sind, kann eine höhere Sicherheit dargestellt werden, als wenn das Firewall-System im Internet eingesetzt wird, wo per Definition alle anderen als aktive Angreifer zu sehen sind.

Dies sind wichtige Randbedienungen für den sicheren und vertrauenswürdigen Einsatz von Firewall-Systemen.

neuKap14.fm Seite 492 Freitag, 18. Oktober 2002 5:12 17

14.5.9 Die Wirkung einer vertrauenswürdigen Realisierung eines Firewall-Systems

Die vertrauenswürdige Realisierung und die Evaluierung und Zertifizierung von Firewall-Systemen erhöhen das Vertrauen in die Nutzung einer Firewall-Lösung insofern, dass die Sicherheitsfunktionen und -mechanismen gegen die bekannten Angriffe tatsächlich und in der angegebenen Stärke wirken und die eigenen Werte angemessen geschützt werden. Auch die eigenen Firewall-Schutzmechanismen werden betrachtet.

Hier spielt in der Gesamtsicherheit die Überprüfung, ob eine Trap-Door eingebaut ist, eine besondere Rolle.

Die vertrauenswürdige Realisierung eines Firewall-Systems ist die Grundlage für die Wirkung aller seiner Sicherheitsfunktionen. In der folgenden Tabelle wird die Wirkung einer vertrauenswürdigen Realisierung eines Firewall-Systems gegen Angriffe dargestellt.

Angriffsart	Vertrauenswürdigkeit	Wirksamkeit	Korrektheit
Angriffe durch einen Dritten	Wiederholen oder Verzögern von Protokollelementen	◆	◆
	Einfügen oder Löschen von Daten in den Protokollelementen	◆	◆
	Modifikation der Daten in den Protokollelementen	◆	◆
	Boykott des Receivers	◆	◆
	Trittbrettfahrer	◆	◆
	Senden von Malware (Viren, Würmer, Trojanische Pferde,...)	◆	◆
Angriffe durch den Transmitter	Aufbau u. Nutzung von Kommunikationsverbindungen	◆	◆
	Nutzung von Kommunikationsprotokollen und -diensten	◆	◆
	Vortäuschen einer falschen Identität (Maskerade-Angriff)	◆	◆
	Java, ActiveX, ... Angriffe	◆	◆
	falsche Konfiguration/Implementierungsfehler	◆	◆
	Leugnen der Kommunikationsbeziehung	◆	◆
Vorbereitung für Angriffe	Social Engineering	○	○
Angriffe auf das Firewall-System	Analyse mithilfe von Scannerprogrammen	◆	◆
	Manipulation des Firewall-Systems	◆	◆
	Einbau einer Trap-Door	○	●
	Nutzung einer falschen Konfiguration des Firewall-Systems	○	○
	Nutzung von Implementierungsfehlern des Firewall-Systems	○	◆
	interne Angriffe	○	○

● sehr große Wirkung ◕ große Wirkung ◑ Wirkung
◔ wenig Wirkung ○ keine Wirkung ◆ Grundlage für die Wirkung

Abb. 14.10: Die Wirkung der vertrauenswürdigen Realisierung

neuKap14.fm Seite 493 Freitag, 18. Oktober 2002 5:12 17

Beurteilung der Wirkung gegen die verschiedenen Angriffsarten:

Die Vertrauenswürdigkeit eines Firewall-Systems stellt eine Randbedingung der Sicherheit sowie die Grundlage für die Wirkung gegen die entsprechenden Angriffsarten da (siehe Tabelle). Die Überprüfung der Korrektheit stellt als einziger Einflussfaktor eine sehr große Wirkung gegen eingebaute Trap-Doors dar.

14.5.10 Die Wirkung der Einflussfaktoren der eigenen Organisation

In der folgenden Tabelle wird die Wirkung der Einfussfaktoren der eigenen Organisation auf die Angriffe dargestellt.

Angriffsart	Einflußfaktoren der eigenen Organisation	Infrastruktur	Organisation	Personal	Notfall	Sicherheitspolitik	sicherer Betrieb
Angriffe durch einen Dritten	Wiederholen oder Verzögern von Protokollelementen	○	○	○	○	◆	◆
	Einfügen oder Löschen von Daten in den Protokollelementen	○	○	○	○	◆	◆
	Modifikation der Daten in den Protokollelementen	○	○	○	○	◆	◆
	Boykott des Receivers	◕	○	○	◕	◆	◆
	Trittbrettfahrer	○	○	○	○	◆	◆
	Senden von Malware (Viren, Würmer, Trojanische Pferde,...)		○	◕	○	◆	◆
Angriffe durch den Transmitter	Aufbau u. Nutzung von Kommunikationsverbindungen	○	○	○	○	◆	◆
	Nutzung von Kommunikationsprotokollen und -diensten	○	○	○	○	◆	◆
	Vortäuschen einer falschen Identität (Maskerade-Angriff)	○	○	○	○	◆	◆
	Java, ActiveX, ... Angriffe	○	○	◕	○	◆	◆
	falsche Konfiguration/Implementierungsfehler	○	○	○	○	◆	◆
	Leugnen der Kommunikationsbeziehung	○	○	◕	○	◆	◆
Vorbereitung für Angriffe	Social Engineering	○	◕	●	○	◆	◆
	Analyse mithilfe von Scannerprogrammen	○	○	○	○	◆	◆
Angriffe auf das Firewall-System	Manipulation des Firewall-Systems	◕	◕	◕	○	◆	◆
	Einbau einer Trap-Door	○	○	○	○	○	○
	Nutzung einer falschen Konfiguration des Firewall-Systems	○	◕	○	○	◆	◆
	Nutzung von Implementierungsfehlern des Firewall-Systems	○	◕	○	○	◆	◆
	interne Angriffe	○	◕	◕	○	◆	◆

● sehr große Wirkung ◕ große Wirkung ◑ Wirkung
◔ wenig Wirkung ○ keine Wirkung ◆ Grundlage für die Wirkung

Abb. 14.11: Die Wirkung der Einfussfaktoren der eigenen Organisation

14.5.10.1 Bewertung der Einfussfaktoren der eigenen Organisation

In diesem Abschnitt werden die Einflussfaktoren aufgezeigt, die der Betreiber des Firewall-Systems selbst initiieren und verantworten muss.

neuKap14.fm Seite 494 Freitag, 18. Oktober 2002 5:12 17

Nicht-technische Sicherheitsmaßnahmen für Firewall-Systemen

Das eigentliche Firewall-Produkt besteht aus Software und Hardware. Neben dieser technischen Sicherheitsmaßnahme müssen weitere Sicherheitsmaßnahmen berücksichtigt werden, damit der sichere Betrieb eines Firewall-Systems garantiert werden kann. Die zusätzlichen Sicherheitsmaßnahmen gliedern sich in die folgenden Unterpunkte /Pohl2000a/, /KSG98/:

14.5.10.2 Infrastruktur

Folgende infrastrukturelle Sicherheitsmaßnahmen tragen zur Erhöhung der Sicherheit des Firewall-Betriebs bei:

- zugangsgesicherter Raum
- unterbrechungsfreie Stromversorgung
- geschützte Leitungsführung
- eindeutige Kennzeichnung und Dokumentation aller Leitungen
- Ankopplung an ein Netzwerkmanagement-System

Durch diese Sicherheitsmaßnahmen wird verhindert, dass das Firewall-System physikalisch manipuliert werden kann, und die Verfügbarkeit des Firewall-Systems wird erhöht.

Beurteilung der Wirkung gegen die verschiedenen Angriffsarten:

Durch infrastrukturelle Sicherheitsmaßnahmen ist eine große Wirkung gegen den Boykott des Receivers und gegen die Manipulation des Firewall-Systems zu erzielen (siehe Tabelle).

14.5.10.3 Organisation

Diese Sicherheitsmaßnahmen betreffen die technische Realisierung, das Security Management, die Benutzer und die allgemeine Organisation.

- keine weiteren externen Zugänge (backdoors)
- Festlegung der Verantwortung für das Firewall-System
- Festlegung der Zugriffsrechte für das Security Management
- Kontrolle der Protokolldaten
- Informationsbeschaffung über Sicherheitslücken des Firewall-Systems
- Festlegung der Reaktion auf Verletzungen der Sicherheitspolitik
- Verpflichtung des Security-Administrators zur Datensicherung
- keine Weitergabe von Security Token und Passworten durch den Benutzer
- Betreuung und Beratung der Benutzer, die über das Firewall-System kommunizieren
- Regelung für Wartungs- und Reparaturarbeiten am Firewall-System
- Beteiligung des Personal-/Betriebsrats

Hier werden die Verantwortungen für den sicheren Betrieb des Firewall-Systems festgelegt.

neuKap14.fm Seite 495 Freitag, 18. Oktober 2002 5:12 17

Beurteilung der Wirkung gegen die verschiedenen Angriffsarten:

Durch organisatorische Sicherheitsmaßnahmen ist eine große Wirkung gegen Angriffe auf das Firewall-System zu erzielen (siehe Tabelle), weil hier die Verantwortungen für die unterschiedlichen Rollen klar geregelt sind und überprüft werden.

14.5.10.4 Personal

Diese Sicherheitsmaßnahmen betreffen das Security Management und die Benutzer.

- Festlegung des Administrators und Vertreters
- Vertretungsregelung festlegen
- geregelte Verfahrenweise beim Ausscheiden von Benutzern
- Anweisung an die Benutzer bezüglich der Nutzung von Internetdiensten
- Aufklärung der Benutzer über die Protokollierung von Firewall-Daten
- Sensibilisierung der Benutzer für die möglichen Gefahren bei der Nutzung des Internet
- Schulung zum Thema Sicherheit

Die personellen Sicherheitsmaßnahmen wirken besonders gegen Social Engineering, wobei personelle Sicherheitsmaßnahmen für die Aufklärung und Unterstützung der Benutzer eine besondere Rolle spielen.

Beurteilung der Wirkung gegen die verschiedenen Angriffsarten:

Durch personelle Sicherheitsmaßnahmen ist eine große bis sehr große Wirkung auf die entsprechenden Angriffe zu erzielen (siehe Tabelle). Besonders gegen Social Engineering hilft die Aufklärung und Schulung ernorm. Auch beim Umgang mit Java und Viren kann mithilfe von personellen Sicherheitsmaßnahmen eine große Wirkung erlangt werden.

14.5.10.5 Notfall

- Festlegung der Verfügbarkeitsanforderungen
- Schaffen und Testen von Backup-Möglichkeiten

Beurteilung der Wirkung gegen die verschiedenen Angriffsarten:

Durch Notfall-Sicherheitsmaßnahmen ist eine große Wirkung gegen den Boykott des Receivers zu erzielen (siehe Tabelle).

14.5.10.6 Sicherheitspolitik

Eine Firewall-Sicherheitpolitik ist die Voraussetzung für den sicheren Betrieb eines Firewall-Systems. Ein Firewall-System macht nicht automatisch sicher, sondern mit einem Firewall-System *kann* der Übergang zwischen einem unsicheren und einem zu schützenden Netz sicher gemacht werden.

neuKap14.fm Seite 496 Freitag, 18. Oktober 2002 5:12 17

Die richtige Sicherheitspolitik ist die Grundlage für die Wirkung aller Sicherheitsfunktionen eines Firewall-Systems. Die folgenden Aspekte müssen sorgsam definiert werden:

- die Sicherheitsziele der eigenen Organisation
- die zu schützenden Ressourcen
- die zu schützenden Werte
- die Einschätzung des Schutzbedarf und des Angriffspotenzials
- die Kommunikationsanforderungen
- die Verfügbarkeit
- die Dienste und Anwendungen, die erlaubt werden sollen
- die Benutzer, die über das Firewall-System kommunizieren sollen, und deren Kommunikationsprofil
- Maßnahmen beim Auftauchen von Sicherheitsproblemen
- usw.

Weitere Fragen für die Erarbeitung der Sicherheitspolitik sind z. B.:

- Wer ist für die Festlegung der Kommunikationsprofile verantwortlich, wer für die Vergabe der Kommunikationsprofile oder der einzelnen Dienste an die Benutzer, wer für die Administration und damit auch für die Umsetzung der Filterregeln?
- Welche Informationen werden im Firewall-System protokolliert?
- Wer analysiert wann die Protokolldaten?
- Was soll passieren, wenn ein Angriff erkannt wird?

Die Sicherheitspolitik ist die Grundlage für die Sicherheitsrichtlinien.

Beurteilung der Wirkung gegen die verschiedenen Angriffsarten:

Die richtige Sicherheitspolitik eines Firewall-Systems stellt die Grundlage für die Wirkung gegen die entprechenden Angriffsarten dar (siehe Tabelle). Nur wenn eine Organisation definiert, was wann gegen welche Angriffe geschützt werden soll, kann eine nachvollziehbare Sicherheit erreicht werden. Die Sicherheitspolitik ist Grundlage für eine restriktive, d.h. sichere Konfiguration.

14.5.10.7 Sicherer Betrieb von aktiven Firewall-Elementen

Damit mithilfe eines Firewall-Systems ein effektiver Schutz für die Kommunikation zwischen dem unsicheren Netz und dem zu schützenden Netz gewährleistet werden kann, müssen die folgenden Bedingungen erfüllt werden:

- Das Firewall-Konzept muss in das IT-Konzept der Organisation eingebunden werden.
- Der Betrieb des Firewall-Systems muss auf eine umfassende Sicherheitspolitik aufbauen.
- Das Firewall-System muss korrekt installiert sein.
- Das Firewall-System muss korrekt administriert werden.

neuKap14.fm Seite 497 Freitag, 18. Oktober 2002 5:12 17

Aus diesem Grund ist eine regelmäßige Überprüfung der umgesetzten Sicherheitsmaßnahmen notwendig. Hierbei soll festgestellt werden, ob die unterschiedlichen Sicherheitsmaßnahmen richtig eingehalten werden.

Außerdem kann der sichere Betrieb von Firewall-Systemen in den folgenden Phasen betrachtet werden:

- Installation
- Probebetrieb
- Wirkbetrieb
- Updatevorgang

Installationsphase

In der Installationsphase ist die Authenzität des Firewall-Systems selbst von überragender Bedeutung. Durch den Versand- und Installationsweg der Hard- und Software ist sicherzustellen, dass weder Funktionen der Software entfernt noch Trapdoors hinzugefügt werden können. Dies ist z. B. durch kryptographische Verfahren wie MAC oder elektronische Unterschriften zu bewerkstelligen.

Probebetrieb

In einem Probebetrieb ist die Funktionalität des Firewall-Systems unter Beweis zu stellen. Dies geschieht am besten während vorhandener Wartungsfenster oder in exemplarischen Teilnetzen. So ist die Verfügbarkeit der Kommunikation nur begrenzt gefährdet. Ferner können so alternative Installationen gezielt getestet werden.

Wirkbetrieb

Im Wirkbetrieb ist es aus unterschiedlichen Gründen notwendig, das Regelwerk in kleinen oder größeren Teilen außer Betrieb zu nehmen. So kann die Installation oder das Update neuer Software-Komponenten den externen Zugriff auf speziell abgesicherte Rechnersysteme erfordern. Hierbei ist ein ausgewogenes Verhältnis zwischen Ergonomie und Sicherheit zu finden. Ferner ist es unabdingbar, solche Ausnahmeregelungen auf ein zeitliches Minimalmaß zu beschränken.

Ein regelmäßiges Audit über die beabsichtigte Sicherheitsfunktionalität stellt sicher, dass zwischenzeitliche und irrtümlich nicht zurückgesetzte Veränderungen im Regelwerk aufgedeckt und behoben werden können. Solche Audits können manuell oder besser semi-automatisch, unterstützt durch Testtools, durchgeführt werden. Die Verantwortung für diese Audits sollte nicht beim Betreiber des Firewall-Systems liegen. Hier bietet sich Outsourcing oder die Einbeziehung von Revisionsabteilungen an.

Updatephase

In der Updatephase ist analog zur Installationsphase die Authentizität des Firewall-Systems von besonderer Bedeutung. Genauso wichtig ist eine gesicherte Migra-

neuKap14.fm Seite 498 Freitag, 18. Oktober 2002 5:12 17

tionsstrategie vom Alt- zum Neusystem. Hierbei ist eine kontinuierliche Sicherheit und Verfügbarkeit der Kommunikationsdienste sicherzustellen. Dies lässt sich beim Vorhandensein getrennter Testkomponenten in effizienter Weise durchführen, ohne den Ausfall eines Produktionssystems zu provozieren.

Beurteilung der Wirkung gegen die verschiedenen Angriffsarten:

Der sichere Betrieb eines Firewall-Systems stellt die Grundlage für die kontinuierliche Wirkung gegen die entsprechenden Angriffsarten da (siehe Tabelle).

14.5.11 Die Wirkung der unterschiedlichen Firewall-Konzepte

In der folgenden Tabelle wird die Wirkung der unterschiedlichen Firewall-Konzepte gegen Angriffe dargestellt. Es wird davon ausgegangen, dass das High-level Security Firewall-System über ein sicheres Betriebssystem, ein sicheres Security Management und Firewall-Schutzmechanismen verfügt.

Angriffsart	Firewall-Konzepte	Packet Filter	dual-homed Application Gateway	Packet Filter und single-homed Application Gateway	Packet Filter und dual-homed Application Gateway	zwei Packet Filter als Screened Subnet und ein single-homed Application Gateway	High-level Security Firewall-System
Angriffe durch einen Dritten	Wiederholen oder Verzögern von Protokollelementen	◔	◕	◔	◕	◔	◕
	Einfügen oder Löschen von Daten in den Protokollelementen	◔	◕	◑	◕	◑	◕
	Modifikation der Daten in den Protokollelementen	○	◕	◑	◕	◑	◕
	Boykott des Receivers	◔	◑	◔	◑	◔	◕
	Trittbrettfahrer	◔	◑	◔	◑	◔	◑
	Senden von Malware (Viren, Würmer, Trojanische Pferde,...)	◔	◕	◑	◕	◑	◕
Angriffe durch den Transmitter	Aufbau u. Nutzung von Kommunikationsverbindungen	◔	◕	◕	◕	◕	●
	Nutzung von Kommunikationsprotokollen und -diensten	◔	◕	◑	◕	◑	●
	Vortäuschen einer falschen Identität (Maskerade-Angriff)	◔	●	◕	●	◕	●
	Java, ActiveX, ... Angriffe	○	◕	◑	◕	◑	◕
	falsche Konfiguration/Implementierungsfehler	◔	◕	◑	◕	◑	●
	Leugnen der Kommunikationsbeziehung	○	◑	◔	◑	◔	◑
Vorbereitung für Angriffe	Social Engineering	○	○	○	○	○	○
	Analyse mit Hilfe von Scannerprogrammen	○	●	◑	●	◑	●
Angriffe auf das Firewall-System	Manipulation des Firewall-Systems	○	○	◔	◕	◑	●
	Einbau einer Trap-Door	○	○	○	○	○	○
	Nutzung einer falschen Konfiguration des Firewall-Systems	○	◔	◔	◕	◑	●
	Nutzung von Implementierungsfehlern des Firewall Systems	○	◔	◔	◕	◑	●
	interne Angriffe	○	○	○	○	○	○

● sehr große Wirkung ◕ große Wirkung ◑ Wirkung
◔ wenig Wirkung ○ keine Wirkung ✦ Grundlage für die Wirkung

Abb. 14.12: Die Wirkung von Firewall-Konzepten

neuKap14.fm Seite 499 Freitag, 18. Oktober 2002 5:12 17

Beurteilung der Wirkung unterschiedlicher Firewall-Konzepte gegen die verschiedenen Angriffsarten:

Im Folgenden werden die einzelnen Firewall-Konzepte bewertet, die in Kapitel 6 *»Konzepte für Firewall-Systeme«* beschrieben sind.

Packet Filters

Durch den ausschließlichen Einsatz eines Packet Filters kann eine geringe Wirkung gegen die entsprechenden Angriffe erzielt werden (siehe Tabelle).

Application Gateway

Durch den ausschließlichen Einsatz eines Application Gateways kann eine bis zu sehr große Wirkung gegen die entsprechenden Angriffe erzielt werden (siehe Tabelle).

Packet Filter und single-homed Application Gateway

Durch den Einsatz eines Packet Filters und eines single-homed Application Gateways kann eine geringe bis große Wirkung gegen die entsprechenden Angriffe erzielt werden (siehe Tabelle).

Packet Filter und dual-homed Application Gateway

Durch den Einsatz eines Packet Filters und eines dual-homed Application Gateways kann eine bis zu sehr große Wirkung gegen die entsprechenden Angriffe erzielt werden (siehe Tabelle). Die Wirkung gegen Angriffe auf das Firewall-System selbst ist aufgrund des vorgeschalteten Packet Filters groß im Vergleich zur ausschließlichen Verwendung eines Application Gateways.

Zwei Packet Filter als Screened Subnet und einem single-homed Application Gateway

Durch den Einsatz von zwei Packet Filters als Screened Subnet und eines single-homed Application Gateway kann eine geringe bis große Wirkung gegen die entsprechenden Angriffe erzielt werden (siehe Tabelle).

High-level Security Firewall-System

Durch den Einsatz eines High-level Security Firewall-Systems kann eine bis zu sehr große Wirkung gegen die entsprechenden Angriffe erzielt werden (siehe Tabelle). Das High-level Security Firewall-System hat insgesamt die beste Wirkung gegen die definierten Angriffe.

neuKap14.fm Seite 500 Freitag, 18. Oktober 2002 5:12 17

14.5.12 Die Wirkung weiterer Sicherheitsmechanismen

In der folgenden Tabelle wird die Wirkung weiterer Sicherheitsmechanismen, die ein umfassendes Firewall-System ergänzen, gegen Angriffe dargestellt.

Angriffsart	weitere Sicherheitsmechanismen	Verschlüsselung	Anti-Malware-System	Intrusion Detection	Personal Firewall	Audits
Angriffe durch einen Dritten	Wiederholen oder Verzögern von Protokollelementen	◕	○	○	◔	✦
	Einfügen oder Löschen von Daten in den Protokollelementen	●	○	○	◔	✦
	Modifikation der Daten in den Protokollelementen	●	○	○	○	✦
	Boykott des Receivers	○	○	◑	◔	✦
	Trittbrettfahrer	●	○	○	◔	✦
	Senden von Malware (Viren, Würmer, Trojanische Pferde,...)	○	●	○	●	✦
Angriffe durch den Transmitter	Aufbau u. Nutzung von Kommunikationsverbindungen	○	○	◑	◔	✦
	Nutzung von Kommunikationsprotokollen und -diensten	○	○	◑	◔	✦
	Vortäuschen einer falschen Identität (Maskerade-Angriff)	○	○	◑	◔	✦
	Java, ActiveX, ... Angriffe	○	○	◑	●	✦
	falsche Konfiguration/Implementierungsfehler	○	○	○	◔	✦
	Leugnen der Kommunikationsbeziehung	○	○	○	○	✦
Vorbereitung für Angriffe	Social Engineering	○	○	○	○	✦
	Analyse mit Hilfe von Scannerprogrammen	○	○	◑	○	✦
Angriffe auf das Firewall-System	Manipulation des Firewall-Systems	○	○	◑	○	●
	Einbau einer Trap-Door	○	○	◔	○	○
	Nutzung einer falschen Konfiguration des Firewall-Systems	○	○	◑	○	●
	Nutzung von Implementierungsfehlern des Firewall Systems	○	○	◑	○	●
	interne Angriffe	○	○	◕	●	◔

● sehr große Wirkung ◕ große Wirkung ◑ Wirkung
◔ wenig Wirkung ○ keine Wirkung ✦ Grundlage für die Wirkung

Abb. 14.13: Die Wirkung weiterer Sicherheitsmechanismen

neuKap14.fm Seite 501 Freitag, 18. Oktober 2002 5:12 17

14.5.13 Zusammenfassung der Wirkung eines umfassenden Firewall-Systems

Als Resultat der gewonnenen Ergebnisse wird in der folgenden Tabelle und in den Zusammenfassungen die Wirkung eines umfassenden Firewall-Systems gegen definierte Angriffe in ihrer Gesamtheit dargestellt.

Angriffsart	Sicherheitsaspekte eines umfassenden Firewall-Systems	High-level Security Firewall-System	Verschlüsselung	Anti-Malware-System	Intrusion Detection Systeme	Personal Firewall	nichttechnische Sicherheitsmaßnahmen	Vertrauenswürdigkeit	Audits	Sicherheitspolitik	sicherer Betrieb
Angriffe durch einen Dritten	Wiederholen oder Verzögern von Protokollelementen	◕	◕	○	○	◔	○	✦	✦	✦	✦
	Einfügen oder Löschen von Daten in den Protokollelementen	◕	●	○	○	◔	○	✦	✦	✦	✦
	Modifikation der Daten in den Protokollelementen	◕	●	○	○	○	○	✦	✦	✦	✦
	Boykott des Receivers	◕	○	○	◑	◔	◕	✦	✦	✦	✦
	Trittbrettfahrer	◑	●	○	○	◔	○	✦	✦	✦	✦
	Senden von Malware (Viren, Würmer, Trojanische Pferde,...)	◕	○	◕	○	●	◕	✦	✦	✦	✦
Angriffe durch den Transmitter	Aufbau und Nutzung von Kommunikationsverbindungen	●	○	○	◑	◔	○	✦	✦	✦	✦
	Nutzung von Kommunikationsprotokollen und -diensten	●	○	○	◑	◔	○	✦	✦	✦	✦
	Vortäuschen einer falschen Identität (Maskerade-Angriff)	●	○	○	◑	◔	○	✦	✦	✦	✦
	Java, ActiveX, ... Angriffe	◕	○	○	◑	●	◕	✦	✦	✦	✦
	falsche Konfiguration/Implementierungsfehler	●	○	○	○	◔	○	✦	✦	✦	✦
	Leugnen der Kommunikationsbeziehung	◑	○	○	○	○	◕	✦	✦	✦	✦
Vorbereitung für Angriffe	Social Engineering	○	○	○	○	○	●	○	✦	✦	✦
	Analyse mit Hilfe von Scannerprogrammen	●	○	○	◑	○	○	✦	✦	✦	✦
Angriffe auf das Firewall-System	Manipulation des Firewall-Systems	●	○	○	◑	○	◕	✦	●	✦	✦
	Einbau einer Trap-Door	○	○	○	◔	○	○	●	○	○	○
	Nutzung einer falschen Konfiguration des Firewall Systems	●	○	○	◑	○	◕	○	●	✦	✦
	Nutzung von Implementierungsfehlern des Firewall Systems	●	○	○	◑	○	◕	✦	●	✦	✦
	interne Angriffe	○	○	○	◕	●	◕	○	◔	✦	✦

● sehr große Wirkung ◕ große Wirkung ◑ Wirkung
◔ wenig Wirkung ○ keine Wirkung ✦ Grundlage für die Wirkung

Abb. 14.14: Zusammenfassung der Wirkung eines umfassenden Firewall-Systems

14.6 Sicherheitsmechanismen und deren Wirkung

Hier werden die in den vorherigen Abschnitten bewerteten Sicherheitsmechanismen zusammenfassend betrachtet und dargestellt, wie sie qualitativ gegen die definierten Angriffe wirken.

neuKap14.fm Seite 502 Freitag, 18. Oktober 2002 5:12 17

High-level Security Firewall-System

Ein zentrales High-level Security Firewall-System (Analogie zum Pförtner) analysiert, kontrolliert und reglementiert die Kommunikation entsprechend einer Sicherheitspolitik. Außerdem protokolliert es sicherheitsrelevante Ereignisse und alarmiert bei erheblichen Verstößen. Im folgenden Bild ist die Wirkungsweise eines zentralen High-level Security Firewall-Systems in Bezug auf das Kommunikationsmodell schematisch dargestellt.

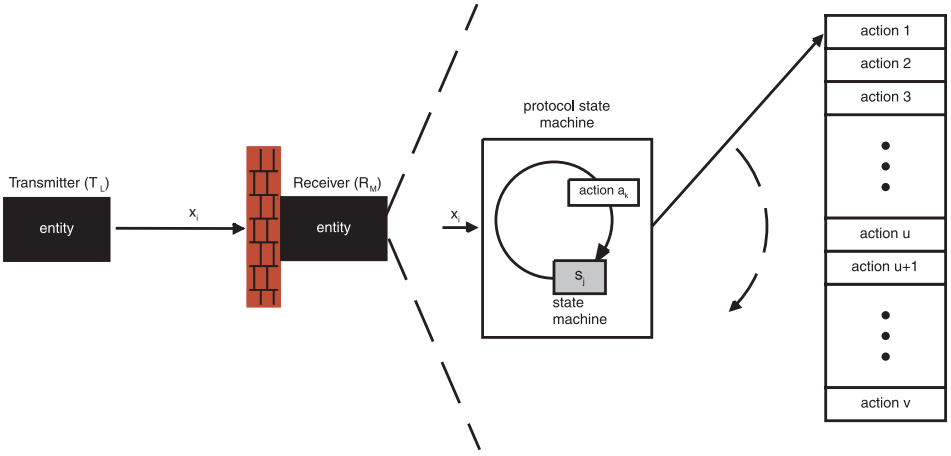


Abb. 14.15: Zentrales High-level Security Firewall-System

Die Wirkung von High-level Security Firewall-Systemen auf die meisten Angriffe ist groß bis sehr groß. Falls andere Firewall-Konzepte verwendet werden, fallen entsprechend die Wirkungen einzelner Sicherheitsfunktionen weg (siehe Kapitel 14.5.10 *»Die Wirkung von unterschiedlichen Firewall-Konzepten«*). Ein besonderer Aspekt von zentralen Firewall-Systemen ist der, dass alle »dahinter« liegenden Rechnersysteme geschützt werden, d.h. alle Clients (Microsoft Windows 95/98/2000/NT/ME ,..., Mac, LINUX, ...), alle Server (Lotus Notes, Novell, UNIX, ...), alle Host-Systeme und sonstige IT-Komponenten (Drucker, MTAs, ...).

Verschlüsselung

Die Verschlüsselung (Analogie zum Sicherheitstransporter) sorgt für die Vertraulichkeit der Protokollelemente während der Kommunikation zwischen Transmitter und Receiver. Außerdem verhindert die Verschlüsselung Trittbrettfahrer und eine gezielte Manipulation von Protokollelementen. Im folgenden Bild ist die Wirkungsweise der Verschlüsselung in Bezug auf das Kommunikationsmodell schematisch dargestellt.

Die Verschlüsselung erhöht die Schutzwirkung gegen Angriffe durch Dritte deutlich. Zusätzlich zu den definierten Angriffen erbringt die Verschlüsselung den

neuKap14.fm Seite 503 Freitag, 18. Oktober 2002 5:12 17

Sicherheitsdienst »Vertraulichkeit«. Besonders wichtig ist die sehr hohe Wirkung gegen Trittbrettfahrer und gezielte Manipulation.

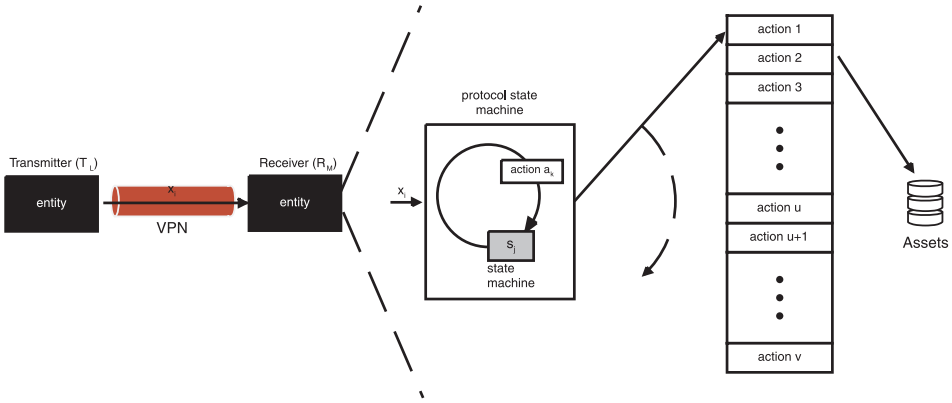


Abb. 14.16: Verschlüsselung

Anti-Malware-Systeme

Ein zentraler Virenscanner (Analogie zur zentralen Poststelle) sucht und erkennt Viren an zentraler Stelle und verhindert damit, dass Viren in die Organisation übertragen werden. Außerdem protokolliert er gefundene Viren und löst gegebenenfalls Alarm aus. Im folgenden Bild ist die Wirkungsweise eines zentralen Virenscanners in Bezug auf das Kommunikationsmodell schematisch dargestellt.

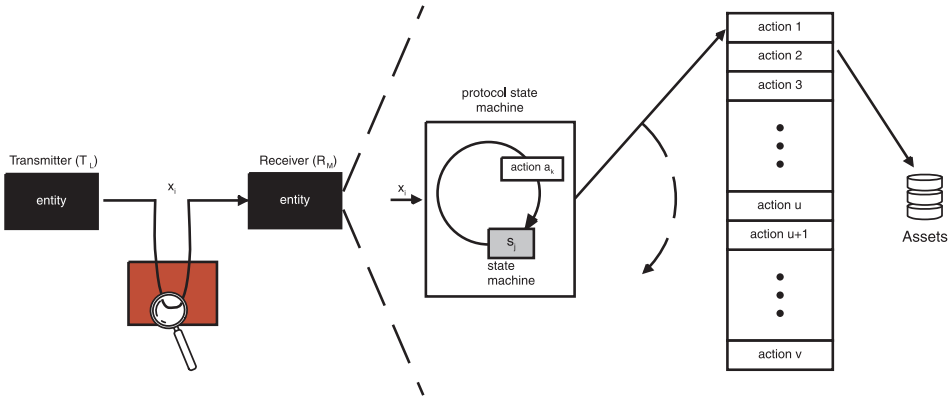


Abb. 14.17: Zentraler Virenscanner

Anti-Malware-Systeme sind notwendig, um mit einer großen Wirkung Schäden durch Viren, Würmer und Trojanische Pferde verhindern zu können. Die Installation eines zentralen Anti-Malware-Systems ist besonders wichtig, damit alle Rechnersysteme, vom Host über UNIX-Systeme bis zum Windows-PC geschützt werden können.

neuKap14.fm Seite 504 Freitag, 18. Oktober 2002 5:12 17

Intrusion-Detection-Systeme

Ein Intrusion-Detection-System (Analogie zur Videoüberwachung) sorgt für die frühzeitige Erkennung von Angriffen im Sinne der Schadensverhinderung. Dies geschieht durch Missbrauchserkennung (Fehler-Signaturen), Erkennung von Anomalien sowie eine entsprechende Protokollierung und Berichterstattung. Im folgenden Bild ist die Wirkungsweise eines Intrusion-Detection-Systems in Bezug auf das Kommunikationsmodell schematisch dargestellt.

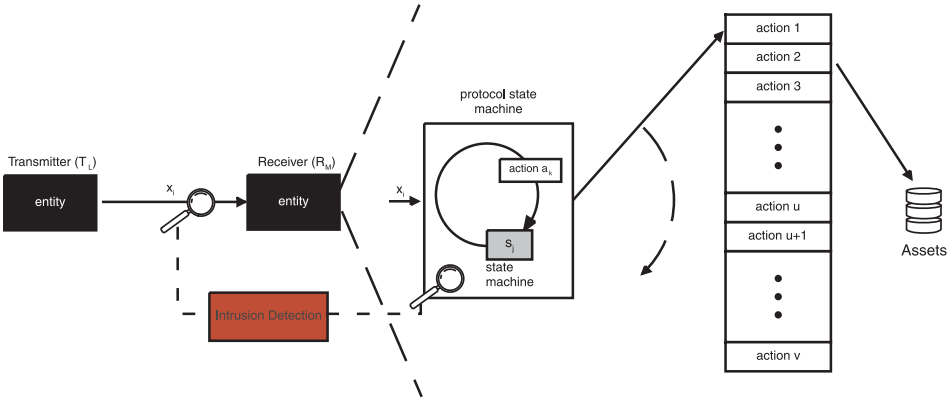


Abb. 14.18: Intrusion-Detection-System

Intrusion-Detection-Systeme haben eine große Wirkung gegen interne Angriffe. Sie lassen Unregelmäßigkeiten erkennen, sodass rechtzeitig und gezielt darauf reagiert werden kann. Hier spielen die Aspekte der frühzeitigen Erkennung im Sinne der Schadensverhinderung (z. B. das Erkennen von DDoS Angriffen) und der richtigen Nachbereitung im Sinne der Schadensminimierung nach einem Schadensfall eine besondere Rolle. Mithilfe der Ergebnisse von Intrution Detection-Systemen können umfassende Firewall-Systeme optimal konfiguriert und das reale Angriffspotenzial analysiert werden.

Personal Firewall

Eine Personal Firewall (Analogie zu einem Pförtner in einer Abteilung und einem Besucherraum, in dem kein Schaden angerichtet werden kann) analysiert, kontrolliert und reglementiert die Kommunikation entsprechend einer Sicherheitspolitik auf dem Rechnersystem. Außerdem wird mithilfe des »Advanced Sandboxing«-Mechanismus ein Schaden durch Malware verhindert. Im folgenden Bild ist die Wirkungsweise einer Personal Firewall in Bezug auf das Kommunikationsmodell schematisch dargestellt.

neuKap14.fm Seite 505 Freitag, 18. Oktober 2002 5:12 17

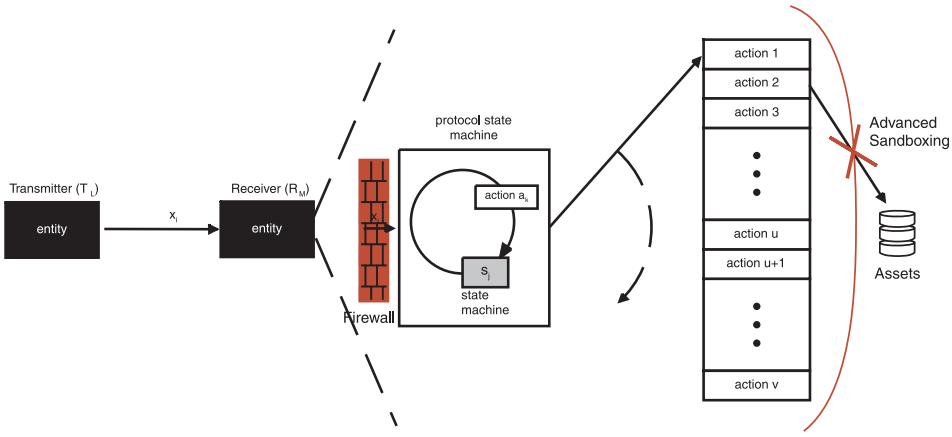


Abb. 14.19: Personal Firewall

Schützenswerte Systemressourcen und Dateien können gegen unerwünschte Zugriffe durch lokale Applikationen oder Malware, die in das System eindringen, dezentral abgeschirmt werden. Hierdurch wird eine sehr große Wirkung gegen das Empfangen von Malware sowie gegen Angriffe mit aktiven Inhalten (Java, ActiveX, Viren, ...) erzielt. Außerdem kann auch eine sehr große Wirkung gegen interne Angriffe erreicht werden. Eine Personal Firewall kann gegenwärtig aus Produktverfügbarkeitsgründen nicht auf allen Rechnersystemen, z. B. Host-Systemen, UNIX-Systemen, Mac-Systemen usw., verwendet werden. Neben den zuvor erwähnten Wirkungen bietet eine Personal Firewall bei Tele- und Mobil-Arbeitsplätzen auch die eigentliche Firewall-Funktionalität. Die Güte der Firewall-Funktionalität hängt von der Qualität der Realisierung, der Einbindung in das Betriebssystem und der Konfiguration des Betriebssystems ab. In dieser Betrachtung ist die Firewall-Funktionalität mit einer mindestens geringen Wirkung bewertet worden.

Nichttechnische Sicherheitsmaßnahmen

Durch nichttechnische Sicherheitsmaßnahmen wie Sicherheitspolitik, sicherer Betrieb usw. kann eine höhere Sicherheit erzielt werden. Dazu ist die Definition von infrastruktuellen, organisatorischen, personellen sowie Notfall-Sicherheitsmaßnahmen notwendig. Im folgenden Bild ist die Wirkungsweise von nichttechnischen Sicherheitsmaßnahmen in Bezug auf das Kommunikationsmodell schematisch dargestellt.

Nichttechnische Sicherheitsmaßnahmen haben eine große Wirkung gegen einige Angriffe und sind besonders wichtig, um »Social Engeneering« etwas entgegenzusetzen.

neuKap14.fm Seite 506 Freitag, 18. Oktober 2002 5:12 17

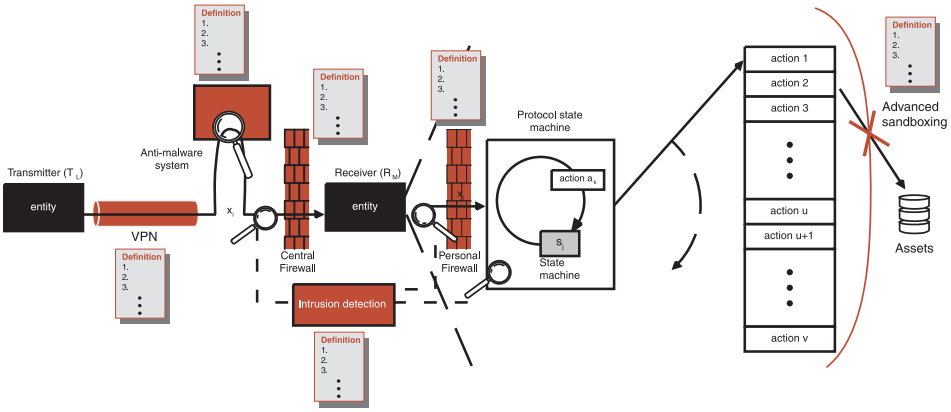


Abb. 14.20: Nichttechnische Sicherheitsmaßnahmen

Audits, Vertrauenswürdigkeit, Sicherheitspolitik und sicherer Betrieb

Durch Audits wird überprüft, ob die gewünschten Sicherheitsmaßnahmen tatsächlich so realisiert sind, wie sie in der Sicherheitspolitik definiert wurden. Im folgenden Bild ist die Wirkungsweise von Audits im Bezug auf das Kommunikationsmodell schematisch dargestellt.

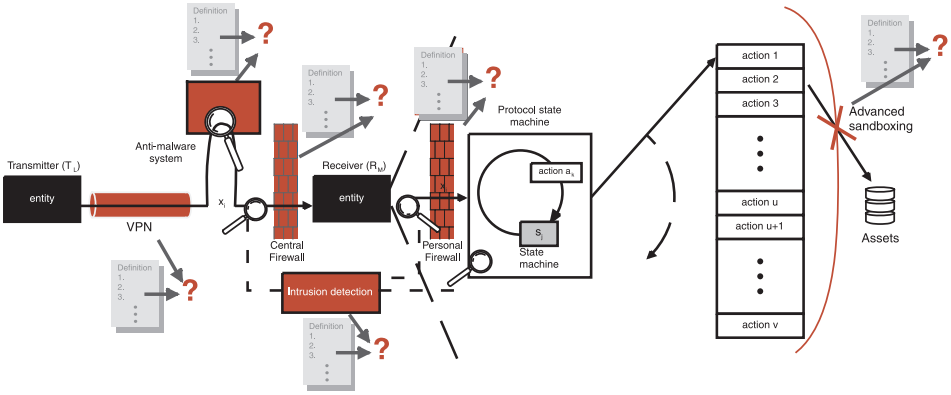


Abb. 14.21: Audits

Die Vertrauenswürdigkeit durch Evaluierung und Zertifizierung, die Durchführung von Audits, die Erarbeitung einer richtigen Sicherheitspolitik und der sichere Betrieb eines umfassenden Firewall-Systems stellen Randbedingungen der Sicherheit bei der Nutzung eines Firewall-Systems dar und sind somit Grundlage für die Wirkung gegen die entsprechenden Angriffsarten.

Die Vertrauenswürdigkeit ist der einzige Sicherheitsaspekt, der eine angemessene Wirkung gegen eine eingebaute Trap-Door hat.

neuKap14.fm Seite 507 Freitag, 18. Oktober 2002 5:12 17

14.7 Angriffe und die Wirkung von unterschiedlichen Sicherheitsmechanismen

Hier werden zusammenfassend die definierten Angriffe betrachtet und aufgezeigt, welche Sicherheitsmechanismen wie qualitativ wirken.

Generell

Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis, damit die Wirkung der einzelnen Sicherheitsmechanismen gegen die definierten Angriffe zur Entfaltung kommen.

Wiederholen oder Verzögern von Protokollelementen

- Die Nutzung der Rechteverwaltung in High-level Security Firewall-Systemen und Verschlüsselung helfen hier eine große Wirkung zu erzielen.
- Die Personal Firewall bietet hier einen Grundschutz für die Rechnersysteme.
- Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.

Einfügen oder Löschen von Daten in den Protokollelementen

- Die Nutzung der Rechteverwaltung in High-level Security Firewall-Systemen hat eine große Wirkung gegen diesen Angriff.
- Die Verschlüsselung hat eine sehr große Wirkung gegen diesen Angriff.
- Die Personal Firewall bietet einen Grundschutz für die Rechnersysteme.
- Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.

Modifikation der Daten in den Protokollelementen

- Die Nutzung der Rechteverwaltung in High-level Security Firewall-Systemen hat eine große Wirkung gegen diesen Angriff.
- Die Verschlüsselung hat eine sehr große Wirkung gegen diesen Angriff.
- Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.

Boykott des Receivers

- Der Mechanismus »dual-homed Application Gateway« im High-level Security Firewall-System hat eine große Wirkung.
- Durch die Verwendung von Intrusion-Detection-Systemen kann ein solcher Angriff schnell erkannt werden und damit eine schnelle Reaktion auch mithilfe weiterer Organisationen (CERT, Behörden, ...) eingeleitet werden.
- Die Personal Firewall bietet hier einen Grundschutz für die Rechnersysteme.

neuKap14.fm Seite 508 Freitag, 18. Oktober 2002 5:12 17

- Die Diskussion über DDoS-Angriffe hat gezeigt, dass hier eine weltweite Zusammenarbeit sinnvoll und erfolgreich ist. Dies ist aus Sicht des Betreibers eine organisatorische Sicherheitsmaßnahme, die z. B. durch Organisationen wie CERT unterstützt werden kann.
- Notfall-Sicherheitsmaßnahmen, wie z. B. das Schaffen von Backup-Möglichkeiten und infrastrukturelle Sicherheitsmaßnahmen wie z. B. eine »unterbrechungsfreie Stromversorgung« erzielen eine große Wirkung.
- Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.

Trittbrettfahrer (Man in the middle)

- Dieser Angriff muss in Zusammenhang mit dem Angriff »Vortäuschen einer falschen Identität (Maskerade-Angriff)« betrachtet werden, wogegen die starke Authentikation eine wichtige Rolle spielt (high-level Security Firewall).
- Hier hilft der Sicherheitsmechanismus Verschlüsselung besonders gut.
- Die Personal Firewall bietet hier einen Grundschutz für die Rechnersysteme.
- Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.

Senden von Malware (Viren, Würmer, Trojanische Pferde, ...)

- Gegen diese Angriffe empfiehlt sich ein zentraler Virenscanner, der separat in das umfassende Firewall-System oder in das Firewall-System selbst integriert ist. Damit kann zentral für alle Rechnersysteme eine große Wirkung erreicht werden.
- Durch die Verwendung Personal Firewalls kann dezentral ein möglicher Schaden verhindert werden, was eine sehr große Wirkung gegen diesen Angriff darstellt.
- Die personellen Sicherheitsmaßnahmen Sensibilisierung, Aufklärung und Schulung haben eine große Wirkung.
- Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.

Aufbau und Nutzung von Kommunikationsverbindungen

- Bei diesem Angriff hat die Nutzung der Rechteverwaltung mit starker Reglementierung der Kommunikationsmöglichkeit in einem High-level Security Firewall-Systemen eine sehr große Wirkung.
- Das Intrusion-Detection-System kann Unregelmäßigkeiten erkennen und somit möglicherweise im Vorfeld Schäden reduzieren.
- Die Personal Firewall bietet hier einen Grundschutz für die Rechnersysteme.
- Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.

neuKap14.fm Seite 509 Freitag, 18. Oktober 2002 5:12 17

Nutzung von Kommunikationsprotokollen und -diensten

- Bei diesem Angriff hat die Nutzung der Rechteverwaltung in einem High-level Security Firewall-System eine sehr große Wirkung.
- Das Intrusion-Detection-System kann Unregelmäßigkeiten erkennen und somit möglicherweise im Vorfeld Schäden reduzieren.
- Die Personal Firewall bietet hier einen Grundschutz für die Rechnersysteme.
- Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.

Vortäuschen einer falschen Identität (Maskerade-Angriff)

- Der starke Authentikationsmechanismus in einem High-level Security Firewall-System hat eine sehr große Wirkung. Dieser Angriff muss in Zusammenhang mit dem Angriff »Trittbrettfahrer« betrachtet werden, wogegen die Verschlüsselung eine wichtige Rolle spielt.
- Das Intrusion-Detection-System kann Unregelmäßigkeiten erkennen und somit möglicherweise im Vorfeld Schäden reduzieren.
- Die Personal Firewall bietet hier einen Grundschutz für die Rechnersysteme.
- Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.

Java, ActiveX, ... Angriffe

- Bei diesem Angriff kann mithilfe entsprechender Sicherheitsmechanismen, z. B. Applet-Filter oder Java Proxy, in einem High-level Security Firewall-System eine große Wirkung zentral erzielt werden.
- Das Intrusion-Detection-System kann Unregelmäßigkeiten erkennen und somit möglicherweise im Vorfeld Schäden reduzieren.
- Durch die Verwendung von Personal Firewalls kann auf den Rechnersystemen dezentral ein möglicher Schaden verhindert werden, was eine sehr große Wirkung gegen diesen Angriff erzielt.
- Die personellen Sicherheitsmaßnahmen Sensibilisierung, Aufklärung und Schulung haben eine große Wirkung.
- Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.

Falsche Konfiguration/Implementierungsfehler

- Durch die Nutzung eines High-level Security Firewall-Systems, insbesondere die Einbindung mehrerer unterschiedlicher Firewall-Elemente wie Packet Filter und dual-homed Application Gateways, kann eine sehr große Wirkung erzielt werden.
- Die Personal Firewall bietet hier einen Grundschutz für die Rechnersysteme.
- Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.

neuKap14.fm Seite 510 Freitag, 18. Oktober 2002 5:12 17

Leugnen der Kommunikationsbeziehung

- Hier spielt die Protokollierung eine wichtige Rolle. Für die Kommunikation mit bekannten Kommunikationspartnern kann hier eine Wirkung erzielt werden.
- Im Bereich externer Services kann die Beweissicherung durch Protokollierung sogar als organisatorische Sicherheitsmaßnahme in den Servicevertrag aufgenommen werden.
- Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.

Social Engineering

- Bei diesem Angriff haben die nichttechnischen Sicherheitsmechanismen wie Aufklärung und Schulung eine sehr hohe Wirkung.
- Die personellen Sicherheitsmaßnahmen Sensibilisierung, Aufklärung und Schulung haben eine große Wirkung.
- Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.

Analyse mithilfe von Scannerprogrammen

- Dieser Angriff kann durch die Nutzung des dual-homed Application Gateways in einem High-level Security Firewall-Systems mit sehr großer Wirkung verhindert werden.
- Durch die Verwendung von Intrusion-Detection-Systemen kann dieser Angriff erkannt und entsprechende Gegenmaßnahmen eingeleitet werden.
- Vertrauenswürdigkeit, Audits, Sicherheitspolitik und sicherer Betrieb sind die Basis.

Manipulation des Firewall-Systems

- Dieser Angriff kann durch die Nutzung eines sicheren Designkonzepts, eigener Schutzmechanismen, eines separaten und zentralen Security Managements und verschiedener Firewall-Elemente in einem High-level Security Firewall-System mit sehr großer Wirkung verhindert werden.
- Durch die Verwendung von Intrusion-Detection-Systemen kann dieser Angriff erkannt werden.
- Durch infrastrukturelle Sicherheitsmaßnahmen wie z.B. einen zugangsgesicherten Raum und organisatorische Sicherheitsmaßnahmen wie z.B. die Festlegung der Zugriffsrechte für das Security Management ist eine große Wirkung zu erzielen.
- Durch regelmäßige Audits kann ein Schaden verhindert werden.

neuKap14.fm Seite 511 Freitag, 18. Oktober 2002 5:12 17

Einbau einer Trap-Door

- Durch die Verwendung von Intrusion-Detection-Systeme kann dieser Angriff möglicherweise entdeckt werden.
- Diesem Angriff kann nur mithilfe einer ausreichenden Evaluierung und Zertifizierung sicher entgegengewirkt werden.

Nutzung einer falschen Konfiguration des Firewall-Systems

- Dieser Angriff kann durch die Nutzung eines sicheren Designkonzepts, eigener Schutzmechanismen, eines separaten und zentralen Security Managements und verschiedener Firewall-Elemente in einem High-level Security Firewall-System mit sehr großer Wirkung verhindert werden.
- Durch die Verwendung von Intrusion-Detection-Systemen kann dieser Angriff möglicherweise entdeckt werden.
- Durch organisatorische Sicherheitsmaßnahmen, wie z. B. »klar geregelte Verantwortung« kann hier eine große Wirkung erzielt werden.
- Durch regelmäßige Audits kann dieser Angriff verhindert werden.

Nutzung von Implementierungsfehlern des Firewall-Systems

- Dieser Angriff kann durch die Nutzung eines sicheren Designkonzepts, eigenen Schutzmechanismen, einem separaten und zentralen Security Management und verschiedenen Firewall-Elementen in einem High-level Security Firewall-System mit sehr großer Wirkung verhindert werden.
- Durch die Verwendung von Intrusion-Detection-Systeme kann dieser Angriff möglicherweise entdeckt werden.
- Durch organisatorische Sicherheitsmaßnahmen, wie z. B. »Klar geregelte Verantwortung« kann hier eine große Wirkung erzielt werden.
- Durch regelmäßige Audits kann dieser Angriff verhindert werden.

Interne Angriffe

- Mithilfe von Intrusion-Detection-Systemen kann durch die Erkennung solcher Angriffe auch im Voraus, bevor ein Schaden aufgetreten ist, eine große Wirkung erzielt werden.
- Diesem Angriff kann mit einer sehr großen Wirkung mithilfe von Personal Firewalls entgegengewirkt werden, da sie in das System (z. B. in Microsoft Windows Betriebssysteme) integriert werden können.
- Die personellen Sicherheitsmaßnahmen Sensibilisierung, Aufklärung und Schulung haben eine große Wirkung.
- Durch Audits können interne Angriffe erkannt/nachgewiesen werden.

neuKap14.fm Seite 512 Freitag, 18. Oktober 2002 5:12 17

14.8 Zusammenfassung

Um dem internationalen Wettbewerb standzuhalten und die enormen Chancen zu nutzen, müssen sich Organisationen an öffentliche Kommunikationssysteme wie das Internet ankoppeln.

Die Organisationen haben dabei meist einen hohen bis sehr hohen Bedarf, ihre Rechnersysteme und Informationen gegen den Verlust von Vertraulichkeit, Integrität, Verfügbarkeit, Verbindlichkeit und Authentizität zu schützen. Sie benötigen deshalb Sicherheitssysteme, um sich gegen Angriffe aus dem Internet zu schützen, z. B. umfassende Firewall-Systeme.

Die Entwicklung und Diskussion des Kommunikationsmodells mit integriertem Firewall-System zeigt die grundsätzlichen Einflussfaktoren auf die Sicherheit und Vertrauenswürdigkeit von Firewall-Systemen.

Hierzu wurden Angriffe aus dem Netz der Kategorien »Angriffe durch Dritte«, »Angriffe durch den Kommunikationspartner«, »Vorbereitung für Angriffe«, »interne Angriffe« und »Angriffe auf das Firewall-System« definiert.

Mit den grundsätzlichen Definitionen und Ergebnissen wurden die strukturellen Zusammenhänge über definierte Angriffe und die Wirkung der verschiedenen Einflussfaktoren auf ein Firewall-System analysiert, beschrieben und in Form von Tabellen umfassend bewertet und dargestellt.

Außerdem wurde im Kapitel *»Theoretische Grundlagen von Firewall-Systemen«* aufgezeigt, dass neben den eigentlichen Sicherheitsdiensten eines Firewall-Systems die Einsatzumgebung, die Evaluierung und Zertifizierung sowie Einflussfaktoren der eigenen Organisation eine große Wirkung auf die Sicherheit und Vertrauenswürdigkeit von Firewall-Systemen haben und entsprechend berücksichtigt werden müssen.

Es wurde grundsätzlich erklärt, wie mit diesem Wissen sichere Netzübergänge zu unsicheren Netzen wie dem Internet sicher und vertrauenswürdig gestaltet werden können.

Durch die richtige Gestaltung der Firewall-Elemente kann eine nachvollziehbar höhere Sicherheit erreicht werden. Eine geeignete Kombination von Firewall-Elementen zu einem Firewall-System in Abhängigkeit vom Schutzbedarf und dem Einsatzfall kann garantiert ein höheres Maß an Sicherheit als jedes Firewall-Element für sich allein.

Eine Erweiterung durch Sicherheitsmechanismen wie Intrusion-Detection-Systeme, Anti-Malware-Systeme, Personal Firewalls, Verschlüsselung und Audits sorgt dafür, dass weitere Unsicherheiten ausgeräumt werden und damit das Restrisiko minimiert wird.

neuKap15.fm Seite 513 Freitag, 18. Oktober 2002 3:53 15

Recht im Internet

Das Vordringen der Informations- und Kommunikationstechnik in fast alle Lebensbereiche hat neue IT-Delikte hervorgebracht und die Computerkriminalität insgesamt vielfältiger und gefährlicher gemacht. Mit der Verbreitung der weltweiten Netze sind Veränderungen der Täter- und Opferprofile einhergegangen: Computerdelikte können heute von jedermann vom Wohnzimmersessel aus begangen werden, und jeder kann Opfer werden. Die elektronische Datenverarbeitung ist mit der Telekommunikation zusammengewachsen, sodass die Delikte zunehmend über Telekommunikationsnetze und auch vom Ausland aus begangen werden und neue Formen angenommen haben. /Pohl 2000/

In kaum einem anderen Bereich zwischenmenschlicher Kommunikation gibt es so viele Verstöße gegen geltendes Recht wie im Internet: Beleidigungen, Verleumdungen, Boykotte, Namens- und Markenrechtsverletzungen, Verstöße gegen das Urheberrecht usw. sind an der Tagesordnung. Mit der wachsenden Bedeutung der Kommunikation in und über Netze wird offensichtlich, dass rechtliche Regelungen unumgänglich sind. Wo immer mehr Menschen im und mit dem Netz Geld verdienen wollen, verstärkt sich der Handlungsbedarf, im zwar nicht »rechtsfreien«, aber bisher fast »rechtsfolgenfreien« Raum rechtsverbindliche und auch in der Praxis durchführbare Orientierungshilfen zur Verfügung zu stellen.

Die neuen Kommunikationsmöglichkeiten bringen dabei eine ganz neue Dimension von Rechtsverstößen mit sich. Das hängt zum einen mit der nie dagewesenen weltweiten Relevanz von Handlungen zusammen, die es jedem einfachen Benutzer einer Mailbox ermöglicht, in einem anderen Teil der Welt für Unruhe zu sorgen, ohne dass er sich der Verantwortung bewusst ist, die mit solchen Möglichkeiten verbunden ist.

15.1 Aktuelle Formen des Delikts »Computerkriminalität«

Bei den neuen Rechtsverstößen im Internet handelt es sich nicht um Delikte, die vor der Vernetzung unbekannt waren, sondern um altbekannte Rechtsverletzungen, die sich in neuem Gewand präsentieren. Gesetzgeber und Justiz stehen ihnen daher nicht hilflos gegenüber, sondern sie müssen altbewährtes Recht den neuen Dimensionen anpassen. Die häufigsten Missbräuche wie Persönlichkeitsrechtsverletzungen und vor allem Wirtschaftsdelikte sind ja keine gänzlich neuen Delikte, sondern aktuelle Formen von Verstößen, die seit jeher geahndet werden und spätestens seit Erfindung der EDV die Rechtsprechung beschäftigt haben.

neuKap15.fm Seite 514 Freitag, 18. Oktober 2002 3:53 15

15.1.1 Persönlichkeitsrechtsverletzungen

Das Persönlichkeitsrecht des Bürgers ist gesetzlich geschützt und kann durch Sammlung, Speicherung, Weitergabe oder Verknüpfung personenbezogener Daten verletzt werden. In heutigen Statistiken spielen Persönlichkeitsrechtsverletzungen nur eine geringe Rolle. Allerdings kann sich dies durch die neuen Möglichkeiten im Internet schnell ändern: Delikte wie die Benutzung unrichtiger Daten (z. B. falsche Adressangabe bei E-Mail), die unbefugte Einsicht in Datenbestände, die unbefugte Sammlung, Speicherung, Weitergabe oder Verwendung personenbezogener Daten und der Verstoß gegen die Formalvorschriften des Datenschutzrechts finden hier einen neuen, fruchtbaren Nährboden.

Elektronischen Nachrichten fehlt so etwas wie ein »digitaler Briefumschlag«. Mit entsprechendem technischem Know-how können Filter in die Transport-Server (MTAs) eingebaut werden, die den Datenfluss analysieren und bestimmte E-Mails herausfiltern können. Auf diese Weise können z. B. E-Mails an einen bestimmten Empfänger abgefangen, auf ein anderes Rechnersystem umgeleitet und dort eingesehen werden.

Ein Beispiel besonders unverfrorener und vor allem professioneller Beschaffung von Daten lieferte 1996 ein Unbekannter beim US Internet Provider Prodigy: Eingeloggten Mitgliedern wurde während des Surfens die Aufforderung zugestellt, sich umgehend bei ihrem Provider zu melden. Unter der angegebenen Telefonnummer meldete sich eine Voicebox, die mit dem Hinweis auf Probleme bei der letzten Beitragsrechnung um den Namen, die Adresse, die Kreditkartennummer, Telefonnummer und den Geburtstag bat. Diese Auskünfte wurden von etlichen Benutzern geliefert, die erst Wochen später bei der nächsten Abrechnung merkten, dass man sie hereingelegt hatte.

15.1.2 Wirtschaftsdelikte

Das Internet hat mit seinem rasanten Wachstum auch die Möglichkeiten von Wirtschaftsdelikten aller Art enorm gesteigert. Computermanipulationen, Sabotage und Erpressung, Hacking, Spionage, Software-Diebstahl und andere Formen der Produktpiraterie breiten sich schneller aus, als Politik und Gesetzgebung ihnen mit entsprechenden Gesetzen, Verboten oder Strafen Einhalt gebieten könnten, siehe dazu auch Kapitel 16.

Computermanipulationen

Zu den klassischen Computermanipulationen zählen Abrechnungsmanipulationen wie Gehalts- und Rechnungszahlungen von Industrieunternehmen, Bilanzmanipulationen und Kontostandsmanipulationen bei Banken. Die derzeit noch vorherrschende Sorglosigkeit der Organisationen lädt Hacker geradezu ein, sich an ihren Rechnersystemen zu versuchen.

neuKap15.fm Seite 515 Freitag, 18. Oktober 2002 3:53 15

Seit einigen Jahren sind Kartenmissbräuche das häufigste Computerdelikt. Geschichten von findigen Tüftlern, die wiederaufladbare Telefonkarten konstruiert oder Kreditkarten gefälscht haben, liest man immer wieder in der Presse. Neue Möglichkeiten des Missbrauchs bieten elektronische Zahlungsmittel. Für diese Systeme gewinnt die Sicherung durch Chipkarten-Technologie an Bedeutung.

Im Internet soll sich jetzt der elektronische Geldverkehr bewähren, der mit Electronic Sales, Cybermoney und Electronic Banking auf dem Vormarsch ist und nicht nur für Banken und Geschäfte im Internet, sondern auch für kriminelle Aktivitäten reichlich neue Perspektiven bietet.

Während das Telefonnetz früher allenfalls manipuliert wurde, um die eigene Telefonrechnung zu verfälschen, hat inzwischen eine qualitative Veränderung der Manipulationen im Telefonnetz stattgefunden. Seit unzureichend geschützte und nicht zu diesem Zweck entwickelte Telefonnetze in unvorsichtiger Weise zur Abrechnung von Dienstleistungen eingesetzt werden, finden auch zunehmend finanzielle Manipulationen mit dem Ergebnis der Überweisung von Geldern statt.

Computersabotage und -erpressung

Viren- und Wurmprogramme verursachen massenhaft Schädigungen, die vor allem über raubkopierte Software oder in Netzwerken verbreitet werden. Im Internet bietet sich die neue Möglichkeit, im Hintergrund von Programmen, vom Benutzer unbemerkt, eine Art Zeitbombe zu installieren, die nach einer bestimmten Zeit Programme zerstört oder die Festplatte gründlich »aufräumt«.

Die Abhängigkeit der Informationsgesellschaft von Rechnersystemen macht Computererpressung zu einer gefährlichen Angriffsform. Mit der Drohung, Rechnersysteme und Datenbestände zu zerstören oder unbrauchbar zu machen, lassen sich Organisationen erpressen, die sich nicht gründlich abgesichert haben.

Hacker

Beim klassischen Computerhacking stand vor allem die Freude an der Überwindung technischer Sicherheitsmaßnahmen im Vordergrund, die das angegriffene Unternehmen schädigte und bei der Spätschäden drohten, wenn die erlangten Kenntnisse zur Begehung von Spionage- und Sabotagehandlungen genutzt wurden. Rechtlich waren die Geheimnissphäre und die Integrität des betroffenen Rechnersystems beeinträchtigt.

Im Telefonnetz gibt es massenhaft Missbräuche durch Phreaker in Telefonleitungen, Anrufbeantwortern und Voice-Boxen, z. B. das Mithören von Gesprächen und die Nummern von Telefonberechtigungskarten. Durch digitales ISDN-Netz und die Verbindung von Telefon- und Computertechnik sind neue Möglichkeiten des Missbrauchs entstanden.

neuKap15.fm Seite 516 Freitag, 18. Oktober 2002 3:53 15

So erlaubt der neue Dienst »leistungsfähiger Messaging Service für Netware-LANs« computergenerierte Telefonanrufe, die dazu missbraucht werden können, gezielt Telefonterror zu betreiben: mit entsprechender Botschaft und per Knopfdruck eingestellter Stimme (z. B. Flüstern) kann man ein Telefon zu einer beliebigen Uhrzeit klingeln lassen und am anderen Ende der Leitung Angst und Schrecken verbreiten.

Wirtschaftsspionage

Schon die klassische Wirtschaftsspionage versprach hohe Gewinne, die heute durch den Reiz großer Datenmengen auf kleinstem Raum, schnell und einfach zu kopieren, um ein Vielfaches gewachsen sind. Tatobjekte sind Programme, Forschungs- und Rüstungsdaten, Daten des kaufmännischen Rechnungswesens sowie Kundenadressen. Die Täter sind meist jugendliche Hacker, konkurrierende Organisationen und zunehmend Geheim- bzw. Nachrichtendienste.

Zur Spionage zählt auch das Abhören von Telefongesprächen. Autotelefone, Richtfunksender und Satellitenverbindungen sind bei unverschlüsselter Kommunikation leichte Angriffsziele.

Software-Diebstahl und andere Formen der Produktpiraterie

Die unbefugte Kopie und Nutzung fremder Computerprogramme betraf früher vor allem Individual-Software, während heute die rechtswidrige Kopie von massenhaft vertriebener Standard-Software dominiert. Datenbanken und andere Datensammlungen sowie die unbefugte Nutzung von Multimedia-Produkten und Ähnlichem erfreuen sich zunehmender Beliebtheit. Wenn Pay-TV-Sender die Verschlüsselung ihres Bildsignals ändern, vergehen immer nur wenige Tage, bis der elektronische Nachschlüssel auf einschlägigen Internetseiten auftaucht. Software-, Musik-, Video-, und Multimediapiraterie werden durch die Verbreitung von Geräten zum Abspielen und Herstellen von CDs und DVDs erleichtert.

15.1.3 Sonstige Delikte

Die Verbreitung von gewaltverherrlichenden, rassistischen oder pornographischen Informationen sowie der zunehmende Einsatz von Rechnersystemen bei der organisierten Kriminalität und die Gefahr möglicher Manipulationen in Kernkraftwerken, Rüstungssystemen usw. sind die stärksten Argumente von Befürwortern einer »Cyberpolizei«. Computermissbrauch ist zu einer globalen Bedrohung geworden und die Sicherheit moderner Rechnersysteme hat für die heutige Informationsgesellschaft zentrale Bedeutung gewonnen.

neuKap15.fm Seite 517 Freitag, 18. Oktober 2002 3:53 15

15.2 Rechtsfragen

Der Gesetzgeber in Deutschland hat auf die neuen Kriminalitätsformen in vier Wellen computerspezifischer Reformen reagiert: Persönlichkeitsschutz, Wirtschaftsstrafrecht und der Schutz des geistigen Eigentums wurden in verschiedenen Reformwellen in den 70er- und 80er-Jahren erfasst, wobei u.a. der zivilrechtliche Urheberrechtsschutz, das Urheberstrafrecht und der Rechtsschutz von Topographien sowie die allgemeine Produktpiraterie den neuen Anforderungen angepasst wurden. Die entsprechenden Reformgesetze umfassen öffentlich-rechtliche und zivilrechtliche Maßnahmen mit Schwerpunkt im Strafrecht.

In Deutschland bereits gültige Bestimmungen, die im Internet den gesetzlichen Rahmen bilden, sind im Einzelnen: das Gesetz über das Urheberrecht und verwandte Schutzrechte, der Staatsvertrag über Bildschirmtext, das Gesetz über Fernmeldeanlagen (FAG), das Telekommunikationsgesetz (TKG), die Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen, die Verordnung über den Datenschutz bei Dienstleistungen der Deutschen Bundespost/Telekom, das Gesetz über die Verbreitung jugendgefährdender Schriften (GjS), das Strafgesetzbuch (StBG) und das Grundgesetz (GG).

In den meisten westlichen Staaten war die Reaktion ähnlich. Internationale Organisationen wie OECD, Europarat, EU, WIPO, WTO und AIDP begleiteten die nationalen Reformmaßnahmen. Der Druck der Industrie förderte die Rechtsvereinheitlichung, wodurch es zu raschen Lösungen kam, die aber ad hoc und isoliert waren und denen keine grundsätzlichen Überlegungen zur Rolle des Strafrechts in der Informationsgesellschaft zugrunde lagen.

15.3 Paradigmenwechsel und Perspektiven

Der Wandel von der Industrie- zur Informationsgesellschaft hat Folgen für das Rechtssystem und die aus der entstehenden Risikogesellschaft resultierenden Veränderungen des Strafrechts.

Dieser Wandel (»zweite industrielle Revolution«) bedeutet vor allem eine Verlagerung menschlicher Geistestätigkeit auf Maschinen. Neben körperlichen Dingen nehmen zunehmend unkörperliche Werte an Bedeutung zu wie elektronisches Geld, Urheberrechte, Geschäftsgeheimnisse und sonstiges Know-how. Information ist ein neuer Wert, der auch Machtfaktor und Gefährdungspotenzial bedeutet.

Der gesellschaftliche Paradigmenwechsel hat das Strafrecht bereits erreicht, aber es fehlt eine allgemeine Theorie für den Schutz von Informationen, die zu der dritten Grundgröße neben Materie und Energie geworden ist. Information ist ein neues wirtschaftliches, kulturelles und politisches Gut, das aber auch neue Probleme schafft. Die moderne Informationstechnik steigert den Wert von Information: Information wird zu einem aktiven Faktor, der in automatischen Datenverar-

neuKap15.fm Seite 518 Freitag, 18. Oktober 2002 3:53 15

beitungssystemen ohne weiteres menschliches Zutun Veränderungen vornimmt, und in manchen Bereichen ersetzen informationstechnische Systeme menschliche Entscheidungen.

Bei der rechtlichen Beurteilung materieller und immaterieller Güter gibt es einige Unterschiede zu beachten: Während Eigentum oder Besitz an materiellen Gütern geschützt werden können, handelt es sich beim immateriellen Gut Information um ein öffentliches Gut, das nicht durch Ausschließlichkeitskriterien geschützt werden kann. Das grundlegende Prinzip der Informationsfreiheit und des freien Informationsflusses ist eine wesentliche Voraussetzung für ein freies wirtschaftliches und politisches System.

Außerdem betrifft der Schutz von Information nicht nur die wirtschaftlichen Interessen ihres Besitzers, sondern auch die Interessen derjenigen, die vom Inhalt betroffen sind. Das bedeutet rechtlich eine neue Anforderung an den Persönlichkeitsrechtsschutz im IT-Bereich.

Zum dritten gewinnen die Zugangsrechte zu Informationen für den privaten und den öffentlichen Bereich an Bedeutung (access to information rights), z. B. bezüglich des Datenschutzrechtes und für Strafverfolgungsbehörden. Aus diesen Unterschieden ergibt sich, dass Rechtsregeln für Informationen nicht im Wege einer Analogie aus Vorschriften über materielle Gegenstände entwickelt werden können, sondern einer eigenständigen Grundlage und Theorie bedürfen.

Die Entwicklung der Technikgesellschaft und des Technikrechts in der postindustriellen Informationsgesellschaft werden auch unter dem Stichwort »Risikogesellschaft« diskutiert. Damit sind insbesondere die Technikgefahren der Chemie, der Kernenergie, der Gentechnik und anderer Anlagen mit schädlichem Einwirkungspotenzial auf den Menschen und die Umwelt gemeint. Bei Betrachtung der neuen Risiken muss berücksichtigt werden, dass sie oft vergesellschaftet sind und nicht mehr auf einen Urheber zurückgeführt werden können, vor allem aber, dass sie schwerwiegende Folgen haben können, die nach Ort, Zeit und Kreis der Betroffenen nicht eingrenzbar sind. Gleichzeitig werden Komplexität und Entwicklungsgeschwindigkeit der gesellschaftlichen und technischen Veränderungen immer größer.

Rechtlich ergibt sich aus der Betrachtung der Risiken die Forderung nach einer besseren gesellschaftlichen Kriminalitätsprophylaxe, von der die Informationstechnik als Teil der Risikogesellschaft ebenfalls betroffen ist. Zur Bekämpfung der Computerkriminalität sind vor allem außerstrafrechtliche Maßnahmen gefordert: technische Sicherheitsstandards mit Zugriffskontrollsystemen, Aufklärung der betroffenen Benutzer und geeignete zivilrechtliche und öffentlich-rechtliche Rahmenbedingungen. Das Strafrecht muss an die neuen Risiken angepasst werden. Eine Voraussetzung für rechtliche Regelungen in diesem Bereich ist ein strukturelles Denken: Statt bei zufälligen technischen Veränderungen anzusetzen, müssen

neuKap15.fm Seite 519 Freitag, 18. Oktober 2002 3:53 15

Funktionen beschrieben werden, die auch in Zukunft der veränderten Technik standhalten können.

Das bedeutet vor allem, dass nationale Grenzen ihre Bedeutung verlieren und eine internationale Harmonisierung des Rechts stattfinden muss. Bei der Nutzung internationaler Telekommunikationsnetze wie dem Internet können Daten in Sekundenbruchteilen über internationale Netze übertragen werden, ohne dass eine Kontrolle möglich ist. Mithilfe von Rechnersystemen können Straftaten begangen werden, deren Konsequenzen im Ausland eintreten.

Unterschiedliche nationale Gesetze würden dagegen zu »data havens« oder »computer crime havens« führen, die nationale Beschränkungen des freien Informationsflusses zur Folge hätten. Zudem wären nationale Barrieren wirkungslos, da Informationen über internationale Netze auch in verschlüsselter Form ins Ausland übertragen werden könnten. Nationale Beschränkungen und Überwachungsmaßnahmen würden Persönlichkeitsrechte der Bürger und Geschäftsgeheimnisse von Organisationen gefährden, sowie die wirtschaftliche Entwicklung eines internationalen Informationsmarktes behindern. Daher ist die internationale Harmonisierung des Informationsrechts durch EU, Europarat, OECD, UN, WIPO, TWTO und AIDP zu begrüßen, wenngleich noch eine Verstärkung von Kontakten und verbesserte Zusammenarbeit zwischen den einzelnen Staaten erforderlich ist.

1997 haben die Justiz- und Innenminister der G8-Länder einen Plan ausgearbeitet, um mit internationaler Kooperation die wachsende IT-Kriminalität zu bekämpfen. US-Generalstaatsanwältin Janet Reno äußerte, Informationstechnologie habe eine neue grenzüberschreitende »Frontier« der Kriminalität eröffnet. Nötig sei, den Cyberkriminellen nicht länger hinterherzuhinken, sondern ihnen einen Schritt voraus zu sein. Der Plan sieht unter anderem vor, dass in jedem Land eine ausreichende Zahl von Spezialisten zur Bekämpfung der IT-Kriminalität angestellt werden, dass die Staaten enger zusammenarbeiten und Angriffe auf Netzwerke sowie die Identifizierung der Täter schneller erfolgen sollen, dass ein Straftäter auch in dem Land zur Rechenschaft gezogen werden kann, in das er geflohen ist, wenn eine Auslieferung nicht möglich ist, und dass entsprechende Gesetze für eine leichtere Strafverfolgung geschaffen werden müssen.

15.4 Zusammenfassung

Das Zusammenwachsen von Datenverarbeitungs- und Datenübertragungstechnik hat die Computerkriminalität vielfältiger und gefährlicher gemacht. Die Möglichkeiten und Gefahren, die sich heute schon und in Zukunft verstärkt im Internet ergeben, sind noch kaum abzuschätzen. Zentralen Einfluss auf die Zukunft haben aus rechtlicher Sicht vor allem drei grundsätzliche soziale Veränderungen in unserer Gesellschaft: Die Entstehung der Informationsgesellschaft mit ihren neuen strafrechtlichen Rechtsgütern, die Veränderung der Risikogesellschaft, in der

neuKap15.fm Seite 520 Freitag, 18. Oktober 2002 3:53 15

außerstrafrechtlichen Maßnahmen größere Bedeutung zukommt als strafrechtlichen und strafprozessualen Maßnahmen, und das Zusammenwachsen der Bürger in einer Informationsgesellschaft, in der sich die neuen Herausforderungen nur durch gemeinsame internationale Anstrengungen bewältigen lassen.

neuKap16.fm Seite 521 Freitag, 18. Oktober 2002 3:53 15

Kapitel 16

Computerkriminalität – Fakten und Zahlen

Vorbemerkung

Der etablierte Fachbegriff »Computerkriminalität« umfasst die Kriminalität im gesamten Bereich der Informationstechnologie. Von IT-Kriminalität zu sprechen, ist noch nicht üblich.

Auch beim Deliktsbereich Informations-»Diebstahl« ist die Terminologie unscharf: Meist wird Information zwar unerlaubt kopiert, aber an der Quelle selbst nicht gelöscht. Nach klassischer Definition ist aber Diebstahl »Entwenden einer fremden, beweglichen Sache«. Treffender ist daher der Begriff »Ausspähen von Daten«.

16.1 Kriminalitätsstatistik des BKA

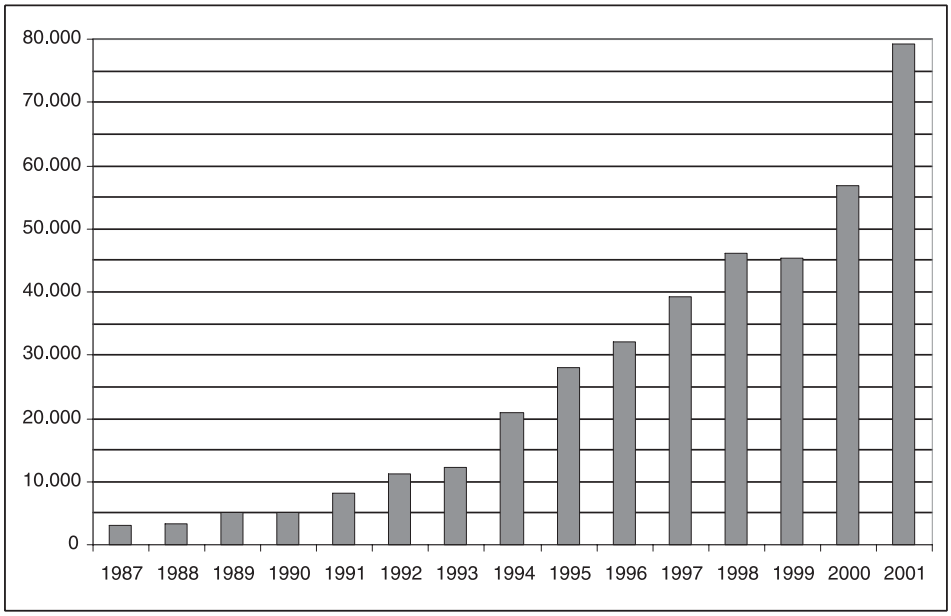


Abb. 16.1: Erfasste Fälle von Computerkriminalität in Deutschland

neuKap16.fm Seite 522 Freitag, 18. Oktober 2002 3:53 15

Erfassung der Computerkriminalität in Deutschland

Seit 1987 werden in Deutschland Computerstraftaten in der Polizeilichen Kriminalitätsstatistik des Bundeskriminalamts (BKA) erfasst und vom Innenministerium im Mai des Folgejahrs als Bulletin und im Internet unter `www.bka.de` publiziert.

Die nachfolgende Auswertung der für den Teilbereich Computerkriminalität relevanten Daten aus dem Jahr 2001 basiert auf dem im Mai 2002 veröffentlichten Bericht.

Dunkelziffer

In der BKA-Statistik fehlen allerdings alle Fälle, die nicht angezeigt bzw. den Ermittlungsbehörden nicht bekannt wurden – wie bei jeder Form von Kriminalität. Über die Höhe dieser so genannten Dunkelziffer ist keine seriöse Schätzung möglich. Sie ist im Bereich Computerkriminalität sicherlich hoch, denn viele betroffene Organisationen und Unternehmen schweigen, um ihr Renommee nicht zu gefährden. Außerdem bleiben Manipulationen und »IT-Einbrüche« durch hochqualifizierte Industrie- und Wirtschaftsspione oder durch Mitarbeiter (Innentäter) oft unbemerkt.

Bei einigen Deliktsbereichen – beispielsweise bei der Software-Piraterie, die nahezu ein »Massenphänomen« ist – lässt bereits die Zahl der erfassten Fälle und die angegebene Aufklärungsquote erkennen, dass zwischen Statistik und Realität erhebliche Differenzen bestehen können.

Auswertung der BKA-Kriminalitätsstatistik für das Jahr 2001

- 2001 wurden 79 286 Computerstraftaten bekannt, das sind 1,2% der registrierten Gesamtkriminalität.
- Während die erfasste Gesamtkriminalität in Deutschland seit 1993 stagniert bzw. leicht rückläufig ist, stieg die Computerkriminalität bis 1998 im zweistelligen Prozentbereich und war damit der bei weitem am stärksten wachsende Kriminalitätsbereich überhaupt. Nach einem Rückgang um 1,5% im Jahr 1999 setzte sich in den folgenden Jahren der Anstieg weiter fort. Im Jahr 2000 lag der Zuwachs im Mittel bei 25%, 2001 bei knapp 40%. Für die letzten zwei Jahre ergibt sich somit ein Anstieg der Computerkriminalität um insgesamt 75%.
- Auffallend ist die heterogene Entwicklung der einzelnen Deliktsbereiche, die im Jahr 2001 von einem Rückgang um 56% bei der »Software-Piraterie in Form gewerbsmäßigen Handelns« bis zu einem Anstieg um 266% beim »Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten« reichte (siehe nachfolgende Tabelle).
- Die Aufklärungsquote lag 2001 bei 57% und damit um knapp 4% über dem Durchschnitt der Gesamtkriminalität.

neuKap16.fm Seite 523 Freitag, 18. Oktober 2002 3:53 15

Deliktsbereiche, Fallentwicklung und Aufklärungsquoten

Bereiche der Computerkriminalität	Fälle 2001	Änderung zu 2000	Aufklärungs-quote
Betrug mittels rechtswidrig erlangter Karten für Geldausgabe- bzw. Kassenautomaten	48 610	+ 10 %	42 %
Computerbetrug (§ 263 a StGB)	17 310	+162 %	78 %
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	8 039	+266 %	84 %
Computer-Software-Piraterie			
– zur privaten Anwendung	1 672	+ 23 %	99 %
– in Form gewerbsmäßigen Handelns	410	- 56 %	96 %
Fälschung beweiserheblicher Daten oder Täuschung im Rechtsverkehr bei Datenverarbeitung	920	+243 %	96 %
Ausspähen von Daten	1 463	+172 %	83 %
Datenveränderung oder Computersabotage	862	+ 68 %	45 %

- Über 60% aller erfassten Computerstraftaten fielen 2001 in den Bereich **Kredit-, Bank- und Geldkartenbetrug**, das sind mehr als 48 000 Fälle. Betrug in diesem Bereich wird meistens angezeigt, sodass die Dunkelziffer als eher klein einzuschätzen ist. Die Aufklärungsquote betrug lediglich 42%.

  Zu diesem Deliktsbereich schreibt das BKA:

  »Bei weiter fortschreitender Technisierung (elektronische Geldbörse) und Expansion des Einsatzes neuer Techniken durch Straftäter wird dieses Deliktfeld in den nächsten Jahren weiter an Bedeutung gewinnen. Deshalb bedarf es weiterhin gemeinsamer Anstrengungen von Politik, Wirtschaft und Polizei, sowie der Förderung der fachlichen Spezialisierung. Gefordert sind insbesondere Präventionsleistungen der Industrie durch technische Sicherung ihrer Produkte. (...) Durch zwingende Benutzung einer PIN könnten in diesem Bereich durchgreifende Verbesserungen erzielt werden.«

- Mehr als jede fünfte Computerstraftat fiel 2001 in den Bereich **Computerbetrug**. Beispiele dafür sind Manipulationen von Programmen oder Daten im Abrechnungswesen und Veränderungen der Programme von Geldspielautomaten zur Erhöhung der Gewinnchancen.
- **Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten** umfasste über 8000 Fälle. Dazu gehört das Einloggen bei Internet-Providern mit fremden oder gefälschten Zugangsdaten, aber auch das unbefugte Entsperren von so genannten SIM-Locks bei Mobiltelefonen sowie »Zugangserschleichungen zu Telefonanschlüssen mit illegalem Anwählen von mit hohen Kosten verbundenen 0190er-Nummern«. Die Aufklärungsquote von 84% deutet darauf

neuKap16.fm Seite 524 Freitag, 18. Oktober 2002 3:53 15

hin, dass solche Fälle überwiegend dann angezeigt wurden, wenn es Hinweise auf den Täter gab. Die Dunkelziffer ist als beträchtlich höher einzuschätzen.

- Bei der **Software-Piraterie** (Raubkopieren) fällt auf, dass wesentlich mehr Delikte im privaten Bereich als im Rahmen »gewerbsmäßigen Handelns« registriert wurden. Zusammen mit dem Rückgang der Fallzahlen in der zweiten Kategorie um 56% und der sagenhaften Aufklärungsquote von im Mittel 98% deutet dies stark darauf hin, dass fast ausschließlich aufgeklärte Fälle erfasst wurden. Die Gesamtzahl von 2082 Fällen liegt mit Sicherheit weit unter den tatsächlichen Verhältnissen.
- Der Gesamtbereich **Fälschung/Täuschung/Ausspähung/Veränderung/Sabotage** umfasste insgesamt 3245 Fälle und damit ›nur‹ 4% aller Computerdelikte, allerdings ist je nach den Umständen von erheblichen Schadenshöhen pro Delikt auszugehen.

16.2 Schätzungen der Schadenshöhe

Das Bundeskriminalamt nennt keine Schadenshöhen durch Computerkriminalität. Für den Teilbereich Wirtschaftsspionage gibt es Schätzungen von verschiedenen Institutionen: Der Verlust, den deutsche Unternehmen durch Wirtschaftsspionage erleiden, wird zwischen 4,25 und 20 Milliarden EUR pro Jahr taxiert.

Die 1998er Studie vom US Computer Security Institute und FBI taxiert den Schaden durch IT-Kriminalität in den USA auf 10 Milliarden US-Dollar jährlich. Schätzungen für den Bereich Industriespionage allgemein in den USA reichen von 63 bis 300 Milliarden Dollar pro Jahr.

Weil der Schaden für Unternehmen existenzbedrohend sein kann, bietet Lloyds seit 1999 erstmals eine Versicherung an, die bis zu einer Höhe von 50 Millionen Dollar vor Risiken des Informationsverlustes durch Cracker, Viren, Computersabotage oder Datenverlust schützt.

16.3 Fallbeispiele

Zum Abschluss sollen einige Fallbeispiele belegen, dass IT-Kriminalität eine reale Bedrohung ist. Kaum ein Tag vergeht, ohne dass die Presse und Online-Informationsdienste, z. B. der Newsticker des Heise-Verlags *(*`www.heise.de/newsticker`*)*, entsprechende Delikte melden.

Betrug, Erpressung

Der Bereich Kreditkartenbetrug wird von den Geldinstituten verschleiert, um die Kundenakzeptanz nicht zu beeinträchtigen. Der Verlust, den die Banken stillschweigend ertragen, mindert die enormen Rationalisierungsgewinne durch

neuKap16.fm Seite 525 Freitag, 18. Oktober 2002 3:53 15

Informationstechnologie nicht wesentlich. Jedoch sind die geschädigten Kunden oft in Beweisnot.

Grundsätzlich sind alle Unternehmen im E-Commerce-Bereich durch IT-Kriminalität gefährdet, wie zwei Fallbeispiele zeigen sollen:

- Im Dezember 1999 erpresste ein zunächst »unbekannter Russe« ein Unternehmen mit gestohlenen Kreditkarteninformationen – 300 000 Kreditkartennummern – und publizierte diese teilweise im Web, um seiner Forderung Nachdruck zu verleihen. Schlagzeile der WELT vom 13.1.2000: »Der größte Datendiebstahl aller Zeiten«.
- Im Januar 2000 berichteten Zeitungen, dass britische Cracker in Systeme von mindestens zwölf internationalen Firmen – unter anderem des Kreditkartenunternehmens Visa – eindrangen, Quellcodes kopierten und Erpressungsgeld in Höhe von insgesamt 31 Millionen Mark forderten. Ein Scotland-Yard-Ermittler sprach von »der bisher schwersten systematischen Verletzung von Sicherheitssystemen«.

Site-Hacking

- Am 5.11.1999 meldeten die Tageszeitungen Site-Hacking beim rumänischen Finanzministerium. Auf dessen Internetseite wurden »Steuern auf Dummheit« angekündigt.
- Im Januar 2000 gelang es chinesischen Hackern, systematisch die Internetseiten verschiedener japanischer Behörden zu hacken und Protest gegen das Nanking-Massaker von 1937 anzubringen, was im »High-Tech-Land Japan« als große Blamage empfunden wurde (Quelle: FAZ vom 28.1.2000).
- Unbekannte veränderten vor einigen Jahren die Homepage des amerikanischen Justizministeriums in »U.S. Department of Injustice«. Schwedische Hacker änderten die CIA-Homepage in »Central Stupidity Agency« und legten »Hot«-Links zu Sex- und Musikangeboten. Eine weitere Blamage: Unbekannte änderten das CIA-Logo in »Central Idiots Agency«, und dieses Fake stand volle vier Tage im Web.
- Zunehmend werden auch politische Auseinandersetzungen zum Anlass für Hackerangriffe genommen. So kam es zu einem mehrwöchigen »Schlagabtausch« zwischen chinesischen und US-amerikanischen Hackern, nachdem am 1.4.2001 ein chinesischer Pilot beim Zusammenstoß seines Kampfjets mit einem US-Aufklärungsflugzeug über dem Pazifik getötet worden war.
  Auch nach den Terroranschlägen in New York und Washington am 11.9.2001 traten Hacker in Aktion; in diesem Fall waren Webseiten islamischer Organisationen Ziel diverser Attacken.

Mehr Informationen über solche zweifelhaften »Erfolge« finden Sie im Archiv von »2600 – The Hacker Quarterly« unter `www.2600.com/hacked_pages` und unter `www.ccc.de` (Chaos Computer Club Hamburg e.V.) sowie unter `www.alldas.de`, wo gezeigt wird, was Cracker und »Scriptkiddies« angerichtet haben.

neuKap16.fm Seite 526 Freitag, 18. Oktober 2002 3:53 15

Täuschung durch Manipulation von Information

- Im Dezember 1999 meldeten die Tageszeitungen ein Beispiel dafür, dass die Veränderung von Informationen auf der Site eines großen US-Wirtschaftsdienstes die Börse beeinflusste: »Pairgain Technologies wird übernommen«, lautete dort eine illegal plazierte Meldung.

Informationsbeschaffung

- Eine Milliarde Dollar Streitwert hat das Gerichtsverfahren eines Erdöl-Konzerns gegen einen IT-Dieb, der die Ergebnisse von Testbohrungen in einem neuen Ölfeld crackte (Quelle: Verbrauchermagazin DM 1/2000).
- 1993 wurde der General Motors Manager Lopez mit einem Teil seiner »Warriors« genannten Managerriege von VW abgeworben. Neben 23 000 Blatt vertraulicher Unterlagen brachten sie auch Informationen auf Datenträgern bei VW ein. Die IT-Spezialisten der Staatsanwaltschaft Darmstadt fanden bei einer – zuvor verratenen – Hausdurchsuchung trotz frisch formatierter Festplatten im IT-System von VW Hinweise auf den Informationsraub. Nach außergerichtlicher Einigung leistete VW an GM einen sehr hohen Schadensersatz.
- Jahrelang wurde das Rechnersystem der EU von US-Geheimdienststellen online angezapft und vor wichtigen internationalen Wirtschaftskonferenzen die jeweiligen nationalen Strategien ausspioniert.
- 1997 wurde die Entwicklungsdatenbank der BASF »geknackt und möglicherweise komplett ausgeräumt« (laut Verbrauchermagazin DM 1/2000).
- 1999 wurden im PDS-Parteibüro Laptops und Festplatten gestohlen. BILD-Schlagzeile am 30.7.1999: »Einbrecher stehlen Gysis Computerdaten«.
- Am 4.1.2000 meldete die Frankfurter Rundschau, das gesamte Nuklearwaffenprogramm der USA – ein virtueller Katalog, der 800 000 Seiten entspricht – sei von einem Innentäter auf Datenträger kopiert worden.
- Im Januar 2000 wurde bekannt, dass ein 16-jähriger aus Kalifornien 27 Internet Service Provider gehackt und dabei über 200 000 Passwörter erbeutet hatte .
- Ein ähnlicher Fall ereignete sich 2001 in Deutschland: Eine Gruppe von etwa 30 Personen hatte die Passwörter von mehreren tausend Internetnutzern ausspioniert und auf einschlägigen Webseiten veröffentlicht. Die Zugangsdaten wurden vermutlich in mehreren tausend Fällen von Dritten missbraucht, um auf fremde Kosten im Internet zu surfen oder falsche Online-Verträge mit Internet Providern abzuschließen (Quelle: Spiegel Online, 3.11.2001).

Industrie- und Wirtschaftsspionage

Nach Ende des Kalten Kriegs betreiben die Geheimdienste Wirtschaftsspionage als neuen Schwerpunkt. Sie verfügen über das Know-how und die beste verfügbare personelle und technische Ausstattung für »elektronische Raubzüge« ohne Spuren.

neuKap16.fm Seite 527 Freitag, 18. Oktober 2002 3:53 15

Aufschlussreich ist der Bericht des Scientific and Technological Options Assessment (STOA) des Europäischen Parlaments: »An Appraisal of the Technologies to Political Control«; Download und aktuelle Ergänzungen siehe
`www.europarl.eu.int/dg4/stoa/en` oder `http://cryptome.org/stoa-atpc.htm`

Durch den weltweit verschärften Wettbewerb wird Industriespionage für Unternehmen Gewinn bringend. Beauftragte High-Tech-Spione stehlen gezielt Knowhow und Strategiepläne der Konkurrenz. Forschungs- und Entwicklungskosten können so drastisch reduziert werden. Dabei existiert kein Unrechtsbewusstsein, Konkurrenten werden mit allen verfügbaren Mitteln ausgebootet:

- Siemens verlor den ICE-Auftrag in Korea, weil der französische Geheimdienst das endgültige Angebot ausspionierte. Siemens-Deutschland hatte unverschlüsselt an seine Niederlassung gefaxt, das Angebot wurde daraufhin vom TGV-Konsortium unterboten.
- Enercon konnte seine Windkraftanlagen nicht in die USA exportieren, weil die Technologie bereits durch gezielten Informationsdiebstahl von der Konkurrenz patentgeschützt war.
- Airbus verlor 1994 einen Großauftrag an Boeing, weil die staatlichen Lauscher des NSA über das Echelon-System – siehe `www.echelonwatch.org` – alle Faxe und Telefonate zum Verhandlungspartner in Saudi-Arabien abhörten.

Software-Piraterie

Der »Diebstahl« von Software (Raubkopieren, Software-Piraterie) ist inzwischen ein großer Bereich der Schattenwirtschaft:

- Im Januar 2000 meldeten die Zeitungen, dass eine Düsseldorfer Bande für geschätzte 1,5 Milliarde DM CD-Sets mit Raubkopien von begehrten Programmen in Auflagen von bis zu 20 000 Stück vertrieben hatte.

Virus-Schäden

- Selbst Viren ohne Schadensfunktionen können zu beträchtlichen finanziellen Schäden führen:
  Im November 1999 kam es laut Pressemeldungen beim PC-Hersteller DELL in Irland nach der Installation eines Updates der Anti-Viren-Software zur Meldung, dass Geräte mit dem Virus »FunLove«, einem harmlosen Windows-Virus, infiziert seien. Es wurden rund 12 000 Computer überprüft. Diese waren zum Teil schon ausgeliefert und mussten für diesen Zweck zurückgerufen werden. Der Gesamtschaden wird auf rund 22 Mio. US$ geschätzt.
- Seit dem Auftreten des »I love you«-Virus am 4.5.2000, der mithilfe eines »Viren-Baukastens« konstruiert worden war, vergeht kaum eine Woche ohne einen neuen oder »mutierten« Skriptvirus. Besonders dreist gingen Virenprogrammierer in zwei Fällen im Herbst 2001 vor, indem sie ihre Machwerke als Sicherheits-Patch für Microsoft-Produkte (»Redesi«-Wurm) bzw. als »neuen

neuKap16.fm Seite 528 Freitag, 18. Oktober 2002 3:53 15

kostenlosen Trojanerscanner« (»Ants«-Wurm) getarnt hatten. Viele Anwender ließen sich durch diese Spielart des Social Engineering täuschen und trugen mit einem Doppelklick auf das vermeintliche Sicherheitsprodukt zur Weiterverbreitung der Schädlinge bei.

- Gleich mehrere Verbreitungswege nutzte im September 2001 der Wurm »Nimda« aus und infizierte dadurch eine große Zahl von Rechnern: Er verbreitete sich als E-Mail-Attachment, über Web-Server, in deren Webseiten er JavaScript-Code einschleuste, sowie innerhalb von lokalen Windows-Netzwerken über freigegebene Laufwerke und Ordner. Zu seinen Schadensfunktionen gehörte neben der Manipulation von System- und Programmdateien die Einrichtung eines Gast-Accounts mit Administrator-Rechten auf Windows-NT/2000-Systemen, der als Hintertür für andere Angreifer aus dem Internet dienen kann.
  Verbreitung und Schadenshöhe lassen sich nur schwer erfassen, US-amerikanische Medien schätzen jedoch, dass allein 2,2 Millionen Server infiziert wurden, wodurch ein Schaden von über 500 Millionen Dollar entstand.

neuKap17_a.fm Seite 529 Freitag, 18. Oktober 2002 3:53 15

Sicherheitsstandards

Zurzeit gibt es mehrere Ansätze, Sicherheitsstandards in Verbindung mit der TCP/IP-Technologie zu etablieren. Dazu gehören:

- Mail-Security-Lösungen wie PEM, PGP und S/Mime, die einen sicheren Transfer von Mails oder Messages zwischen Benutzern ermöglichen und in der Anwendungsebene des TCP/IP-Stacks arbeiten.
- Client/Server-Sicherheit wie SSL und S-HTTP, die eine sitzungsorientierte Verschlüsselung oberhalb der TCP-Transportebene erlauben (Sitzungs- bzw. Darstellungsebene im OSI-Modell).
- Sicherheit auf der Netzebene, wie SKIP oder IPSec, die eine Verschlüsselung auf der IP-Ebene (Netzwerkebene) ermöglichen.

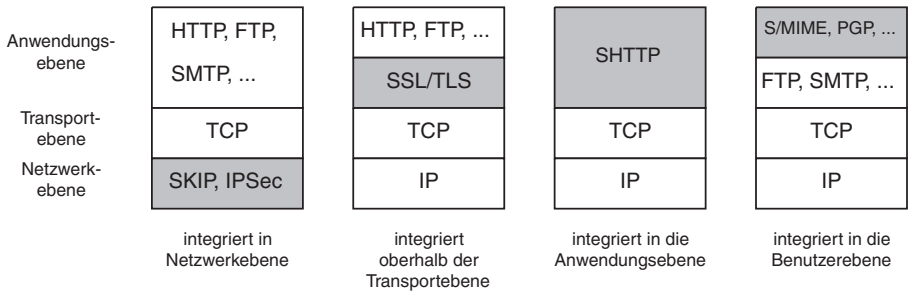


Abb. A.1: Sicherheitslösungen und ihre Integration

Bei Sicherheitsstandards spielt neben den Austauschformaten der Objekte das Key-Management eine besondere Rolle. Dieses muss so konzipiert sein, dass alle Beteiligten ihm vertrauen können. Diese schwierige Aufgabe kann nur realisiert werden, wenn sie – neben der Implementierung zuverlässiger Technologien – auch vom Gesetzgeber gestützt wird.

Bei geschlossenen Benutzergruppen mit eigener Sicherheitspolitik ist das Key-Management oft mehr mit technischen als mit organisatorischen Fragestellungen behaftet. Wenn aber Organisationen mit unterschiedlichen Verantwortungsbereichen miteinander gesichert Daten austauschen wollen, ist die Einführung eines gemeinsamen Key-Managements eine zentrale Aufgabe, die nicht leicht zu bewältigen ist.

neuKap17_a.fm Seite 530 Freitag, 18. Oktober 2002 3:53 15

Sicherheitsstandards

Sicherheitsstandards im Internet haben nur dann eine Chance auf weitverbreitete Anwendung, wenn eine sichere Infrastruktur bei der Verteilung von authentischen öffentlichen Schlüsseln geschaffen wird und in den Produkten kryptographische Verfahren mit hoher Sicherheitsgarantie eingesetzt werden.

Bei Kryptographie geht es um die Vertrauenswürdigkeit von Daten, Rechnersystemen und Kommunikationsstrukturen; der Aspekt der richtigen und sicheren Implementation von Krypto-Algorithmen ist daher von besonderer Bedeutung. Firewall-Systeme sollen nicht einfach nur funktionieren, sondern auch Sicherheit gewährleisten. Ein Standard bietet nicht dadurch zuverlässige Sicherheit, dass er »*Sicherheitsstandard*« genannt wird. In jüngster Vergangenheit zeigten sich Schwachstellen in der Implementierung, Konzeption und Einbettung von Sicherheitsstandards, auf deren vermeintliche Sicherheitsleistungen sich Unternehmen verlassen und die sie in vielen Anwendungsbereichen eingesetzt hatten.

In den folgenden Abschnitten werden die Sicherheitsstandards S-HTTP, SSL, SKIP und IPSec exemplarisch dargestellt und diskutiert. Drüber hinaus wird ein kurzer Abriss des Nachfolgers des schon in die Jahre gekommenen IP-Protokollstandards IPv4 gegeben, der IPv6 oder IPng genannt wird.

A.1 S-HTTP

Das Secure Hyper Text Transfer Protocol (S-HTTP) wurde von Enterprise Integration Technologies Corporation (EIT) entwickelt und ist kompatibel mit HTTP. S-HTTP enthält jedoch zusätzlich Sicherheitsfunktionen wie Absender-Authentikation, Ursprungsnachweis sowie Vertraulichkeit und Unversehrtheit der Daten. Diese Sicherheitsfunktionen sind, wie PEM und PGP, in die Anwendungen integriert, damit geschäftliche Vorgänge über das Internet jederzeit abgewickelt werden können /Hugh95/.

Da S-HTTP eine Weiterentwicklung von HTTP ist, können Browser, die S-HTTP unterstützen, sowohl mit HTTP-fähigen als auch mit S-HTTP-fähigen Servern kommunizieren. Auch für Server gilt, dass S-HTTP-fähige Server auch HTTP-fähig sind. Geschützte URLs werden durch den »shttp«-Protocol Designator ausgewiesen:

```
shttp://www.whitehouse.gov./presidential-desserts.html
```

S-HTTP ist sehr flexibel konzipiert und unterstützt symmetrische und asymmetrische Verschlüsselungsverfahren. So kann bei Bedarf auf die zeitintensive Registrierung von öffentlichen Schlüsseln durch eine offiziell anerkannte Institution verzichtet werden. Für die gesicherte Übertragung des geheimen Schlüssels sind in diesem Fall die Kommunikationspartner allein verantwortlich. Der Schlüssel kann dann z. B. aus einem Kerberos-Ticket gewonnen werden.

neuKap17_a.fm Seite 531 Freitag, 18. Oktober 2002 3:53 15

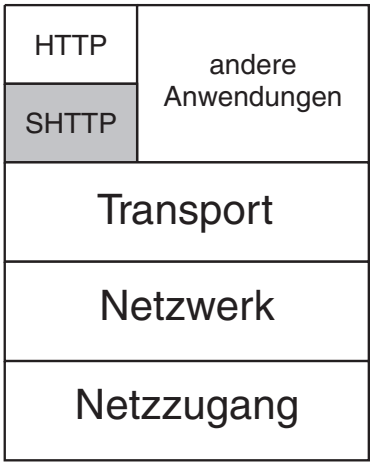


Abb. A.2: S-HTTP

Zu Beginn der Kommunikation handeln S-HTTP-fähige Browser und Server die Bedingungen aus, unter denen der Datenaustausch stattfinden soll. Dabei wird ein breites Spektrum an Anforderungen und Fähigkeiten abgedeckt. Von jedem Verhandlungspartner, d.h. sowohl vom Browser als auch vom Server, werden Präferenzen für und Anforderungen an relevante Objekte nach einem aus vier Teilen bestehenden Schema angegeben.

- Eigenschaft (Property)
  das ausgehandelte Verfahren (z.B. Algorithmus für digitale Signatur oder Algorithmus der Verschlüsselung)
- Wert (Value)
  beschreibende(s) Attribut(e) der Eigenschaft wie z.B. »Digitale Signatur mit RSA-Verschlüsselung« oder »DES-Verschlüsselung im CBC-Modus«
- Richtung (Direction)
  vom Verhandlungspartner aus gesehen, entweder »Sender« oder »Empfänger«
- Stärke (Strength)
  die vom Verhandlungspartner angestrebte Präferenz, entweder »Erforderlich«, »Optional« oder »Abgelehnt«

Ein ausgehandeltes Objekt sieht in der Realität dann wie folgt aus:

```
Property:Direction-Strength-Value[,Value...][Direction-
Strength=Value[,Value...]]
```

Zum Beispiel bedeutet

```
SHTTP-Signature-Algorithms:orig-required=RSA;recv-required=RSA
```

dass der Sender verlangt, dass sowohl er selbst als auch der Empfänger die Nachricht mit dem RSA-Algorithmus digital unterschreiben.

neuKap17_a.fm Seite 532 Freitag, 18. Oktober 2002 3:53 15

Analog dazu bedeutet

```
SHTTP-Privacy-Enhancements:orig-optional=encrypt;recv-
required=sign,encrypt
```

dass der Sender bereit ist, Daten zu verschlüsseln, und im Gegenzug vom Empfänger verlangt, dass dieser Daten verschlüsselt oder digital signiert.

Diese Verhandlung über die Sicherheitsaspekte der Kommunikation läuft ohne Mitwirkung des Benutzers ab, falls sich aus den erforderlichen und optionalen Anforderungen ein eindeutiger Zustand ergibt. Ist die Schnittmenge die leere Menge bzw. lehnt ein Partner die Anforderung seines Gegenübers ab, wird der Benutzer davon informiert. Er muss dann über das weitere Vorgehen entscheiden. Ergibt sich ein mehrdeutiges Verhandlungsergebnis (z.B. wenn beide Partner mehrere gleiche Verschlüsselungsverfahren optional einsetzen können), kann die Entscheidung je nach Implementierung durch vorgegebene Prioritäten oder eine Benutzereingabe erfolgen.

Folgende Objekte können in S-HTTP ausgehandelt werden:

- Modus der zu schützenden Daten
  verschlüsselt, digital signiert oder authentisiert;
  Authentikation wird durch einen MAC (Message Authentication Code) erreicht, der aus einer One Way Hashfunktion der Daten sowie dem angehängten Datum und einem Shared Secret berechnet wird. Da für die Berechnung des MAC keine Public-Key-Verschlüsselung notwendig ist, ist das Verfahren sehr viel schneller als die Verwendung digitaler Signaturen.
- Algorithmus der Datenverschlüsselung
  DES, Triple-DES mit zwei und drei Schlüsseln, IDEA, RC2, CDMF u.a.
- Optionen für Key-Management
  Secret Key, Public Key, Kerberos und Ad-hoc Challenge Response
- Einkapselungsformat der Nachrichten
  PEM, MOSS und PKCS-7
- One-Way-Hashfunktion
  MD2, MD5 oder SHA-1 (der von NSA entwickelte Secure-Hash-Algorithmus)
- Algorithmus der digitalen Signatur
  RSA oder NIST-DSS (der von NSA entwickelte Standard für digitale Signaturen)
- Public-Key-Zertifikate
  X.509 oder PKCS-6

S-HTTP ist ein flexibles und notwendigerweise auch komplexes Protokoll, das arbeitet, ohne dass der Benutzer mit Einzelheiten der Funktionsweise belastet wird. Der Benutzer wird von Browsern auf geschützte Abläufe aufmerksam gemacht, wenn dies notwendig ist, z.B. im Fall einer fehlgeschlagenen Aushandlung erforderlicher Optionen oder der Bestätigung von digitalen Signaturen bei Finanztransaktionen.

neuKap17_a.fm Seite 533 Freitag, 18. Oktober 2002 3:53 15

Bewertung

Falls S-HTTP mit einem symmetrischen Verfahren eingesetzt werden soll, spielt das Key-Management eine besondere Rolle. Wenn das Key-Management nicht in eine sichere Infrastruktur eingebaut werden kann (siehe dazu auch Kapitel 7: *Firewall und Verschlüsselung*), ist eine vertrauenswürdige Kommunikation nur im Fall von geschlossenen Benutzergruppen möglich. Im Zweifelsfall sollte ein Verfahren mit öffentlichen und privaten Schlüsseln gewählt werden.

A.2 SSL/TLS

Das SSL-Protokoll (Secure Sockets Layer) wurde von Netscape Communications Corporation entwickelt. Die neueren Versionen des SSL-Standards tragen den Namen TLS. SSL hat einen anderen konzeptionellen Ansatz als S-HTTP. Statt mehr Sicherheit im Internet durch eine Erweiterung von Anwendungen wie dem HTTP-Protokoll zu schaffen, setzt SSL auf Sicherheit zwischen den Rechnersystemen oberhalb des Transportprotokolls (TCP) und unterhalb der Anwendungsschicht. Dies bedeutet, dass der Applikationsprogrammierer HTTP Transaktionen wie gewohnt ausführen und davon ausgehen kann, dass diese durch das darunter liegende SSL-Protokoll geschützt werden. SSL stellt die Sicherheitsfunktionen Server-Authentikation und optional auch die Client-Authentikation sowie Vertraulichkeit und Unversehrtheit der Nachrichten zur Verfügung. Für die Anwendung stellt sich die SSL-Protokollebene transparent dar.

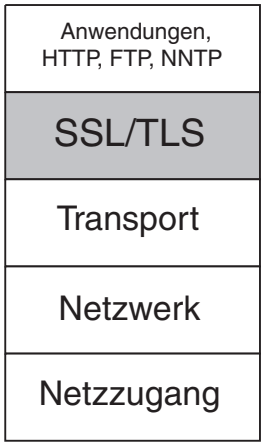


Abb. A.3: SSL

neuKap17_a.fm Seite 534 Freitag, 18. Oktober 2002 3:53 15

Im Internet greifen SSL-fähige Browser geschützt über den Protocol Designator »https« auf URLs zu, z. B.:

```
https://www.whitehouse.gov/first-lady-wardrobe.html
```

Da die gesamte SSL-geschützte Kommunikation im SSL Record Protocol gekapselt ist, in dem auch formatierte Header und Datenfelder enthalten sind, empfangen Webserver, die mit HTTP über SSL kommunizieren, die Nachrichten von Benutzern auf anderen Netzwerkports als Server, die nur über HTTP kommunizieren. Eine reine HTTP-Kommunikation findet normalerweise auf Port 80 statt, während HTTP über SSL auf dem TCP-Port 443 stattfindet (SMTP auf TCP-Port 464 und NNTP auf Port 563). Werden auf einem System sowohl geschützte als auch offene Internet-Transaktionen ausgeführt, sollten am besten verschiedene Server verwendet werden.

Wenn ein Benutzer über SSL eine Verbindung zu einem Server aufbaut, beginnt zunächst die SSL Handshake-Sequenz, die aus den folgenden Teilen besteht:

- Verhandlung über Verfahren zur Verschlüsselung und digitalen Unterschrift
- Austausch eines geheimen Session-Keys
- optionale Authentikation des Servers
- optionale Authentikation des Clients

Während der ersten Sequenz zur Festlegung der Verschlüsselung bzw. Unterschrift wird zunächst das Verfahren zum Austausch des Session-Keys für die später folgende symmetrische Verschlüsselung ausgehandelt. Als Optionen stehen dabei RSA und – zur Kommunikation ohne Sicherheitszertifikate – Diffie-Hellman zur Verfügung. Auch eine eventuell gewünschte Digitale Signatur wird in diesem ersten Schritt der Verhandlungen festgelegt.

Für die anschließend ausgehandelte Verschlüsselung stehen u. a. folgende Optionen zur Verfügung::

- keine Verschlüsselung
- RC4: Stream-Verschlüsselung mit 128-Bit-Schlüssel
- RC4 Export: mit 128-Bit-Schlüssel; aufgrund amerikanischer Exportbeschränkungen sind davon jedoch nur 40 Bit geheim: Während der Aushandlung des Session Key werden 40 Bit verschlüsselt übertragen und 88 Bit im Klartext.
- RC2: Blockverschlüsselung im CBC-Modus mit 128-Bit-Schlüssel
- IDEA: Blockverschlüsselung im CBC-Modus mit 128-Bit-Schlüssel
- DES: Blockverschlüsselung im CBC-Modus mit 56-Bit-Schlüssel
- Triple-DES: Im CBC-Modus mit 168-Bit-Schlüssel (effektiv: 112-Bit)

Die abschließende Verhandlung über den Message Authentikation Code (MAC) kann eine der folgenden Varianten ergeben:

- kein Message Digest
- MD5 mit 128-bit Hash

neuKap17_a.fm Seite 535 Freitag, 18. Oktober 2002 3:53 15

- SHA 160-bit Hash für den Digital Signature Standard (DSS)

Allen Algorithmen ist gemeinsam, dass Digitale Signaturen mit dem MD5 Hash-Algorithmus und dem RSA-Unterschriftsalgorithmus generiert werden. Die Public-Key-Zertifikate entsprechen dem X.509-Signatur-Standard.

Im zweiten Schritt des Verbindungsaufbaus wird der Session-Key übertragen. Anschließend bestätigt der Server dem Client seine Authentizität, die optional mögliche Client-Authentikation wird in der Praxis selten eingesetzt. Die Prüfung der Authentizität der Rechner wird über Sicherheitszertifikate von allgemein anerkannten Certification Authorities (CA) abgewickelt.

Wenn die meisten Komponenten von SSL auch direkt oberhalb der TCP-Ebene angesiedelt sind, gibt es einige Funktionen von SSL, die im TCP/IP-Stack noch weiter oberhalb wirken. Diese dienen dem Verbindungsaufbau und dem Austausch von Fehlermeldungen zwischen Client und Server während der Session.

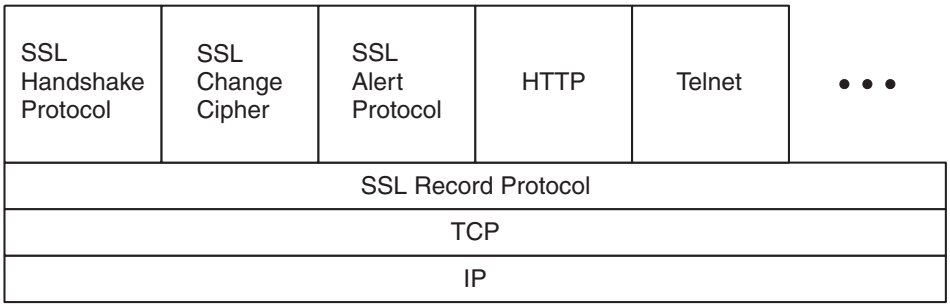


Abb. A.4: Komponenten von SSL

Bewertung

SSL/TLS ist eine Sicherheitsschicht, die oberhalb der Transportschicht und unterhalb der Anwendungsebene integriert wird. Von seiner Definition her könnten mit SSL sowohl TCP- als auch UDP-Dienste abgesichert werden, doch sind bislang nur TCP-Implementierungen erhältlich. Der Vorteil des Verfahrens ist die Unabhängigkeit der Sicherheitsmechanismen von der Applikation, sodass theoretisch auch Dienste wie Telnet oder E-Mail SSL nutzen könnten. Allerdings muss die SSL-Verbindung durch ein Firewall-System hindurchgehen. Dies bedeutet, dass eine verschlüsselte Kommunikation durch ein Firewall-System getunnelt wird. Aus Sichtweise des Firewall-Systems besteht somit ein Sicherheitsrisiko, da z. B. dessen Daten- und Kommunikationsfilter nicht wirken können. Inwieweit eine solche nicht kontrollierbare Kommunikationsverbindung von einem Rechnersystem aus dem zu schützenden Netz zu einem Server im unsicheren Netz (z. B. Internet) zugelassen werden kann, muss abhängig vom Schutzbedarf entschieden werden.

neuKap17_a.fm Seite 536 Freitag, 18. Oktober 2002 3:53 15

Konzeptionell wäre es besser, die Entschlüsselung im Firewall-System durchzuführen, damit die Kontrolle der Anwendungsdaten und insbesondere auch die Protokollierung auf dem Firewall-System dienstspezifisch durchgeführt werden kann.

SSL Key-Management

Das Key-Management von SSL ist derzeit so ausgelegt, dass der Client für die Verschlüsselung verantwortlich ist. Die öffentlichen Schlüssel zur Verifikation von Zertifikaten werden über die Software (Browser) verteilt. Dieses Verfahren ist für sicherheitsrelevante Anwendungen, bei denen die Echtheit der öffentlichen Schlüssel als Garantie für verbindliche Kommunikation eine besonders wichtige Rolle spielt, nicht sicher. Es bietet zwar einen gewissen Schutz gegen Abhören der Kommunikation aus dem Internet, nicht jedoch gegen professionelle Angriffe. Die Existenz von Demozertifikaten, die nach Einsendung einer E-Mail-Adresse von manchen Zertifizierungsbehörden ausgegeben werden, kann den SSL-Mechanismus aushebeln. Für einen wirkungsvollen Schutz müsste eine Zertifizierungshierarchie eingeführt werden, die das Verteilen der Public-Key-Systeme organisiert. Um ein wirklich sicheres Key-Management zu ermöglichen, müssen entsprechende vertrauenswürdige Instanzen eingesetzt werden. Eine solche vertrauenswürdige Instanz könnte z. B. die im Rahmen des Signatur-Gesetzes aufgebaute Infrastruktur sein.

A.3 SKIP

Die bisher vorgestellten Verfahren setzen im IP-Stack oberhalb der Transportebene auf. Da das IP-Protokoll von seiner Definition her verbindungslos ist, können so nur Verbindungen mit echten oder Pseudo-Sitzungen gesichert werden. Viele Möglichkeiten der IP-Protokollfamilie können aber nur unterhalb einer Sitzungsschicht genutzt werden (z. B. IP-Mulitcast oder UDP/IP-Datagramme), sodass allgemeinere Verfahren zur Sicherung auf IP-Ebene entwickelt und implementiert wurden.

Das von Sun entwickelte »Simple Key-Management for Internet Protocols« (SKIP) ist – wie der Name schon sagt – ein Verfahren zur einfachen und sicheren Übertragung von Schlüsseln auf IP-Ebene. Prinzipiell ist die Einbindung in beliebige Sicherungssysteme möglich, Sun selbst bietet mit SunScreen eine produktreife Implementierung an.

SKIP basiert auf dem verbreiteten Verfahren der öffentlichen Schlüssel nach Diffie-Hellman. Beide Partner berechnen aus ihrem eigenen geheimen Schlüssel und dem öffentlichen Schlüssel des jeweils anderen einen gemeinsamen Master-Key, der – ein besonderer Vorteil des Verfahrens – nicht über eine wie immer geartete Kommunikationsstruktur übertragen werden muss. Mit diesem Master-Key werden

neuKap17_a.fm Seite 537 Freitag, 18. Oktober 2002 3:53 15

zufällig generierte Traffic-Keys verschlüsselt, mit denen wiederum die Nutzdaten kodiert sind. Der verschlüsselte Traffic-Key wird mit jedem IP-Paket mitgesendet und kann sich demzufolge beliebig oft ändern. Der Master-Key selbst kann mittels eine Pseudozufallsgenerators und einer gesendeten Zahl n auf beiden Seiten synchron geändert werden (»Zero-Message Master-Key Update«).

Abb. A.5: IP-Paket nach der SKIP-Norm

Mit diesem Verfahren ist auch eine Multicast-Kommunikation möglich, allerdings gibt es keinen auf dem eigenen privaten Schlüssel und den öffentlichen Schlüsseln der Partner basierenden Master-Key. Deshalb muss vor Beginn der Übertragung von einem Gruppenmitglied ein »Group Interchange Key« (GIK) an alle Partner übermittelt werden. Da sich der GIK-Sender vorher von der Authentizität der Partner überzeugt haben muss, wird der theoretische Vorteil des SKIP-Verfahrens bei Multicast durch den großen Verwaltungsoverhead aufgezehrt.

Die von Sun auf den Markt gebrachte SKIP-Implementierung SunScreen kann mit einer Reihe von Verfahren zusammenarbeiten, die Diffie-Hellman Modulgröße (DH) kann – je nach Version – 512, 1024 oder 2048 Bit betragen.

Verschlüsselung des Master-Key:

- RC2: 40-Bit-Schlüssel
- DES: CBC-Modus mit 56-Bit-Schlüssel
- Triple-DES: CBC-Modus mit drei Schlüsseln zu 56 Bit (nur DH 2048)
- Safer CBC: 128-Bit-Schlüssel (nur DH 2048)

Verschlüsselung der Daten mittels Traffic-Key:

- RC2: 40-Bit-Schlüssel
- RC4: 40-Bit-Schlüssel
- DES: CBC-Modus mit 56-Bit-Schlüssel (nur DH 1024 und DH 2048)
- Triple-DES: CBC-Modus mit drei Schlüsseln zu 56 Bit (nur DH 2048)
- Safer CBC: 128-Bit-Schlüssel (nur DH 2048)

Die Authentikation erfolgt über MD5. Der Traffic-Key wird alle 30 Sekunden oder nach der Übertragung von 500 KByte geändert.

neuKap17_a.fm Seite 538 Freitag, 18. Oktober 2002 3:53 15

Bewertung

Im Bezug auf Firewall-Systeme verschärft SKIP die Problematik von SSL. Da alle Kommunikation oberhalb der IP-Ebene nur verschlüsselt abgewickelt wird, kann ein Firewall-System nur seine eingebauten Paketfilter-Verfahren zur Kontrolle der Verbindung einsetzen. Weitere Möglichkeiten zur Überprüfung hat es nicht. Vorteilhaft ist allerdings die völlige Transparenz der Sicherheitsmaßnahmen gegenüber der TCP- und UDP-Schicht.

A.4 IPv6

Während die bisher beschriebenen Verfahren Sicherheitsmechanismen in die bestehende IP-Norm (IP Version 4) integrieren, geht IP Version 6 einen anderen Weg. Dieses Protokoll, auch als IPng (next Generation) oder IPv6 bezeichnet, ist eine komplett neue Definition von IP und soll Version 4 im Laufe der nächsten Zeit ersetzen.

Unter Sicherheitsaspekten ist vor allem der modulare Aufbau des neuen IP-Headers interessant, der die starre Konvention von IP Version 4 ersetzt. Um auch zukünftigen, heute nicht absehbaren Entwicklungen Raum zu geben, wurde kein Header mit fester Länge implementiert, sondern mit einer einfach verketteten Liste Raum für Erweiterungen geschaffen. In den für die Absicherung des Datenverkehrs vorgesehenen Headern vom Typ »Authentication« (AH) und »Encapsulation« (ESP, Verschlüsselung) stehen Informationen, nach welchen Methoden die Authentikation bzw. Verschlüsselung stattfindet. Der letzte Header in der Kette ist gesondert markiert, anschließend folgen die Nutzdaten.

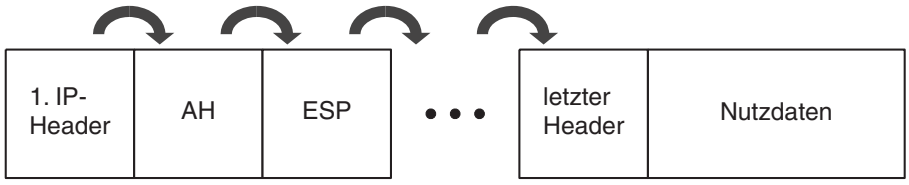


Abb. A.6: IP-Paket in der Version 6

Die neuen Header AH und ESP sind Bestandteil des Standards IPSec und werden in einem späteren Abschnitt dieses Kapitels noch ausführlicher beschrieben.

Bewertung

IP Version 6 ist ein gutes Stück davon entfernt, ein echter Standard zu sein. Zu unklar sind noch manche Fragen der Implementierung. Vor allem die Inkompatibilität mit dem alten Standard IPv4, die zum Austausch aller Netzwerkkarten

neuKap17_a.fm Seite 539 Freitag, 18. Oktober 2002 3:53 15

führt, stand einer größeren Verbreitung bisher im Wege. Auch der zweite große Vorteil von IPv6, der deutlich größere Adressraum bei den IP-Adressen, ist nicht mehr evident. Viele Firmen richten ihr internes Netz mit privaten Netzwerkadressen (den früheren Testadressen) ein und präsentieren sich nach außen durch ein Firewall-System und ein Minimum an zusätzlichen Rechnern. Da die AH- und ESP-Mechanismen mittlerweilen auch in die IP-Version 4 integriert wurde, besteht die Gefahr, dass IPv6 zu einer Randerscheinung in der Welt der Netzwerkprotokolle degradiert wird.

A.5 IPSec

Im Bereich der Standardisierung hat die Internet Engineering Task Force (IETF) einen Internet-Sicherheitsstandard definiert, der IPSec heißt.

IPSec definiert Mechanismen, um eine gesicherte Kommunikation über IP aufzubauen. Eine der häufigsten Implementierungen von IPSec ist zurzeit das virtuelle private Netz (VPN), es sind aber auch gewöhnliche Netzwerkverbindungen zweier Knoten denkbar.

IPSec wurde ursprünglich im Zusammenhang mit IP Version 6 (IPv6) entwickelt. Da sich die allgemeine Einführung von IPv6 wegen der Inkompatibilität zum alten Standard IPv4 immer wieder verzögert, wurden die Mechanismen von IPSec auch in IPv4 integriert. Die unter IPv6 eingeführten neuen Header zur Authentifizierung und Verschlüsselung werden dabei in IPv4 zu einer Erweiterung des Datenteils der IP-Pakete, sodass diese insgesamt länger werden.

A.5.1 IPSec – Internet Protocol Security Architecture

IPSec bietet im Wesentlichen zwei Mechanismen an, den so genannten Authentication Header (AH) und die Encapsulated Security Payload (ESP). IPSec wird auf einem Rechnersystem oder einem Security Gateway implementiert und schützt den IP Verkehr von und zu diesem Knoten. Die genauen Spezifikationen dieses Schutzes werden in einer gesonderten Datenbank abgelegt, der Security Policy Database (SPD). Die SPD kann als Sammlung von Regeln angesehen werden, ähnlich den Filterregeln eines Paketfilters. Für alle an- und abgehenden Pakete wird dort definiert, ob sie mittels IPSec behandelt, ohne IPSec weitergeschickt oder sogar verworfen werden. Falls Pakete mittels IPSec behandelt werden sollen, enthält die SPD einen Verweis auf eine so genannte Security Association (SA), in der die genaue Vorgehensweise (Algorithmen zur Verschlüsselung etc.) festgelegt ist.

neuKap17_a.fm Seite 540 Freitag, 18. Oktober 2002 3:53 15

A.5.2 Der Authentication Header (AH)

Der IP-Authentication Header (AH) wird für die Überprüfung der Integrität und Authentifizierung des Datenursprungs von IP-Datagrammen eingesetzt. Gleichzeitig bietet er Schutz gegen unerwünschte Wiederholungen von Paketen und den daraus resultierenden Problemen (Replay-Angriffe etc.)

Die Werte der Felder im IP-Header, die sich bei der Datenübertragung ändern (z. B. Flaggen), können allerdings nicht von AH geschützt werden.

AH kann alleine oder in Kombination mit ESP eingesetzt werden. Dabei gibt es zwei Betriebsweisen, den Transport- und den Tunnelmodus.

Format des AH-Headers

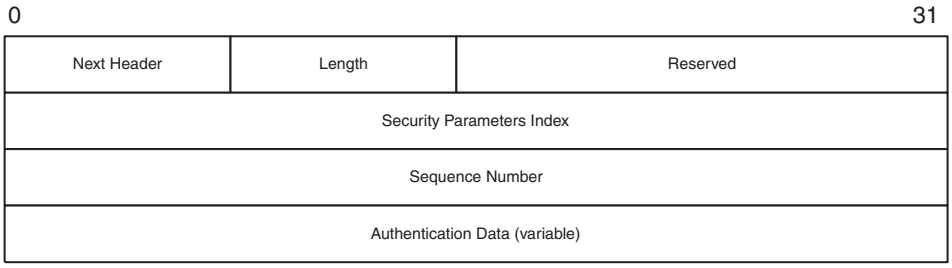


Abb. A.7: AH Format

Der AH-Header hat den IP-Protokolltyp 51 und setzt sich aus folgenden Feldern zusammen:

- »Nächster Header« ist ein 8-bit Feld, das den Typ der Daten hinter dem AH-Header angibt.
- »Länge« ist ein 8-bit Feld, welches die Länge des AH in 32-Bit Worten spezifiziert.
- Reserviert: dieses 16-bit Feld ist reserviert für zukünftige Nutzungen. Es muss stets zu Null gesetzt werden.
- Security Parameter Index: (SPI): ein 32-bit Wert, der zusammen mit der IP-Zieladresse einen Zeiger auf die dazugehörige SA ergibt.
- Die Sequenznummer ist ein 32-Bit-Feld, welches einen monoton steigenden Zahlenwert enthält. Damit können Wiederholungen von Paketen erkannt und Replay-Angriffe abgewehrt werden.
- Authentication Data ist ein Feld von variabler Länge, welches den Integrity Check Value (ICV) für dieses Paket enthält. Der Algorithmus zur Authentifizierung beinhaltet verschlüsselte »Message Authentication Codes« (MACs), die auf symmetrischen Verschlüsselungs-Algorithmen (z. B. DES) oder auf Oneway-Hashfunktionen wir MD5 oder SHA-1 basieren. Mit diesen Daten können die Unversehrtheit des Paketes und die Echtheit des Absenders überprüft werden.

neuKap17_a.fm Seite 541 Freitag, 18. Oktober 2002 3:53 15

Verarbeitung des AH-Headers

AH kann auf zwei Arten eingesetzt werden, im Transportmodus oder im Tunnelmodus. Im Tunnelmodus wird vor den alten IP-Header ein neuer gesetzt, der z. B. die Adresse eines Gateways enthält, *siehe auch Kapitel 7 bei Tunneling*. Das gesamte alte IP-Paket inklusive seiner Flaggen wird dabei in den Schutz des AH einbezogen.

Im Transportmodus wird der AH erst nach dem IP-Header, aber immer vor einem eventuellen ESP-Header eingebaut. Dabei gibt es Unterschiede zwischen IPv4 und IPv6: Bei IPv4 wird der AH zwischen IP-Header und dem Protokoll der höheren Ebene (TCP, UDP, ICMP, etc.) platziert. Bei IPv6 erscheint der AH als ein zusätzlicher Erweiterungsheader nach den Erweiterungsheadern »hop-by-hop«, »routing« und »Fragmentierung«.

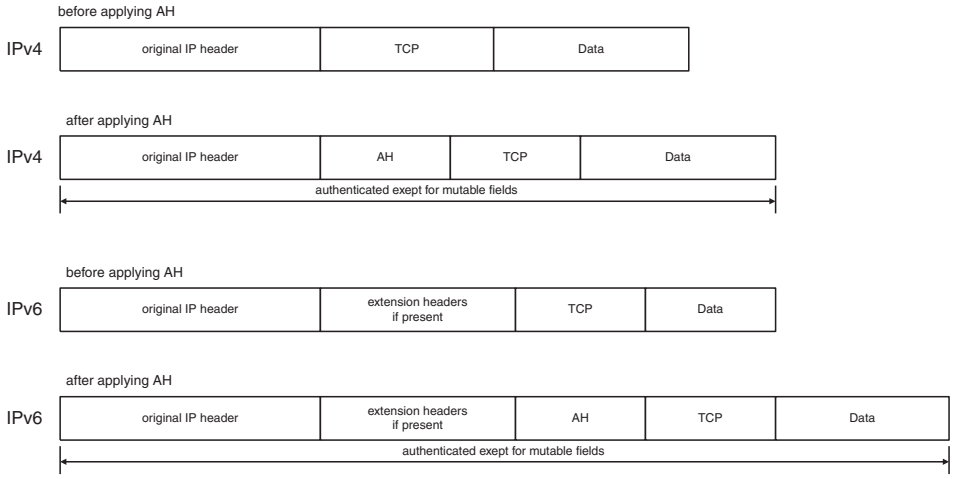


Abb. A.8: AH im Transportmodus

Abbildung A.8 illustriert AH im Transportmodus jeweils für IPv4 und IPv6.

Im Tunnelmodus transportiert der innere IP-Header die tatsächliche Quell- und Zieladresse, während der äußere IP-Header z. B. die Adresse des Security Gateways beinhaltet. Im Tunnelmodus schützt AH somit den gesamten inneren Bereich des Paketes einschließlich des inneren IP-Headers. Abbildung A.9 zeigt AH im Tunnelmodus jeweils für IPv4- und IPv6-Pakete.

Verarbeitung von ankommenden und abgehenden Paketen

Der AH wird vom Sender nur dann in ein ausgehendes Paket eingetragen, wenn zu dem Paket eine SA gefunden wird, die nach einem AH verlangt. Diese Zuordnung wird in der SPD festgelegt.

neuKap17_a.fm Seite 542 Freitag, 18. Oktober 2002 3:53 15

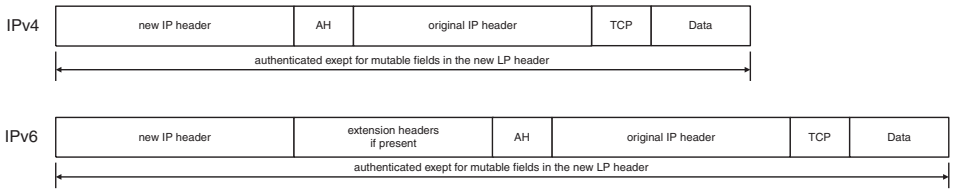


Abb. A.9: AH im Tunnelmodus

Nach Erhalt eines AH-Paketes sucht der Empfänger eine entsprechende SA, basierend auf der IP-Zieladresse und dem SPI aus dem AH-Datenteil.

Der SA-Eintrag zeigt dann an, ob das Sequenznummern-Feld geprüft wird, spezifiziert die Algorithmen für die ICV-Berechnung und stellt die dazu benötigten Schlüssel zur Verfügung.

Falls keine SA für diese Verbindung vorliegt (z. B., wenn der Empfänger keinen Schlüssel hat) wird der Empfänger das Paket abweisen und diese Aktion in eine Audit-Logdatei eintragen.

A.5.3 Encapsulated Security Payload (ESP)

Auch der ESP-Header kann IP-Pakete vom Typ IPv4 und IPv6 absichern. Der ESP-Header wird analog zum AH nach dem IP-Header und vor dem Header des Protokolls der höheren Ordnung (Transportmodus) oder vor einem eingebetteten IP-Header (Tunnelmodus) eingesetzt.

ESP wird eingesetzt, um Vertraulichkeit, Authentifizierung und Datenintegrität zu ermöglichen. Wie beim AH kann auch hier die unerwünschte Wiederholung von Paketen erkannt werden.

Soll der gesamte Datenfluss inklusive den IP-Adressen vertraulich behandelt werden, muss der Tunnelmodus eingesetzt werden. Dann sind auch die originalen IP-Adressen verschlüsselt und können nicht mehr gelesen werden. Der Tunnelmodus wird meist an Punkt-zu-Punkt-Verbindungen wie Firewalls oder anderen Security Gateways eingesetzt.

Format des ESP-Headers

Der ESP-Header hat den IP-Protokolltyp 50. Die Bedeutung der Felder entspricht denen bei AH, mit folgenden Abweichungen:

- Die Nutzdaten stehen in einem Feld variabler Länge. Außer den reinen Daten können hier auch Initialisierungsvektoren für den Verschlüsselungsalgorithmus eingetragen werden.
- Padding: Falls bestimmte Algorithmen eine feste Datenlänge erwarten, können die Nutzdaten mit dem Padding-Feld auf diesen Wert vergrößert werden.
- Länge Padding: zeigt die Anzahl der vorausgehenden Füllbytes an.

neuKap17_a.fm Seite 543 Freitag, 18. Oktober 2002 3:53 15

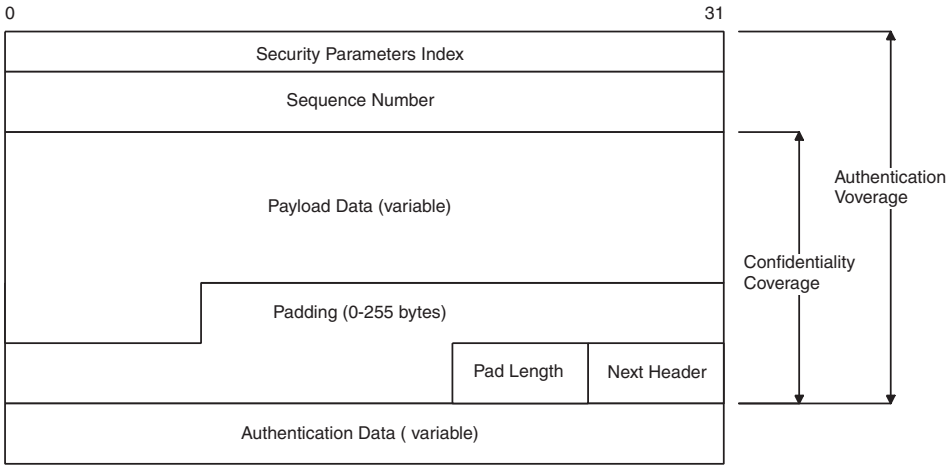


Abb. A.10: ESP Format

- Authentication Data ist ein Feld variabler Länge, welches einen ICV (Integrity Check Value) enthält, errechnet über den ESP-Header ohne die Authentifizierungsdaten selbst. Hiermit kann schon allein über den ESP-Header eine Authentifizierung des Paketes vorgenommen werden.

Abbildung A.11 illustriert ESP im Transportmodus für typische IPv4- und IPv6-Pakete.

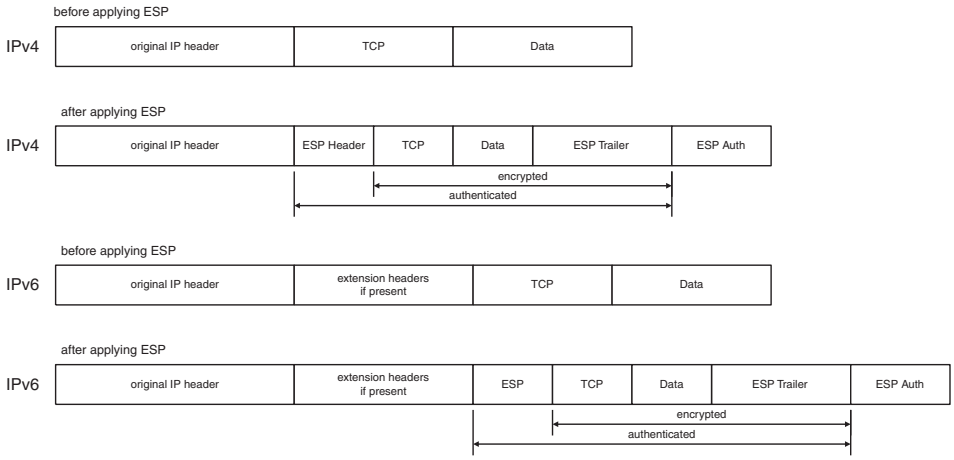


Abb. A.11: ESP im Transportmodus

neuKap17_a.fm Seite 544 Freitag, 18. Oktober 2002 3:53 15

Da im Gegensatz zum ESP-Header der AH sich auch auf den vorangestellten IP-Header (ohne die veränderlichen Flaggen etc.) bezieht, kann zur Vergrößerung der Sicherheit auch eine Kombination von AH und ESP gewählt werden.

Im IPv6-Kontext wird ESP als so genannter »End-to-End«-Datensatz behandelt, der immer nach den Erweiterungsheadern Hop-by-hop, Routing und Fragmentierung eingebaut wird. Weitere Erweiterungsheader können vor oder nach dem ESP-Header auftreten. Da aber ESP grundsätzlich nur die Felder nach dem ESP-Header schützt, ist es erstrebenswert, möglichst viel vom Paket hinter dem ESP-Header zu platzieren.

Abbildung A.12 zeigt ESP im Tunnelmodus.

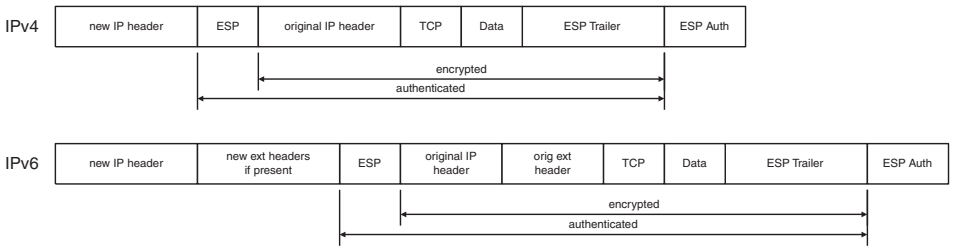


Abb. A.12: ESP-Pakete imTunnelmodus

Verarbeitung von ankommenden und abgehenden Paketen

Im Transportmodus baut der Sender nur die Protokollinformation der höheren Protokolle mit in den ESP-Bereich ein, im Tunnelmodus wird das komplette alte IP-Paket inklusive IP-Header in die ESP-Daten eingepackt und ein neue IP-Header mit der IP-Zieladresse (z. B. der Firewall) generiert.

ESP kommt bei ausgehenden Paketen nur dann zur Anwendung, wenn innerhalb der IPSec-Definition in der SPD festgestellt wird, dass das Paket mit einer SA verbunden ist und diese ESP erfordert.

Um ein verschlüsseltes Paket zu versenden, muss der Sender:

- den Bereich der ESP-Nutzdaten generieren. Diese Daten umfassen die originalen Nutzdaten des alten IP-Paketes und die Protokollinformation der höheren Schicht (Transportmodus) bzw. den gesamten alten IP-Header (Tunnelmodus)
- die notwendigen Füllzeichen einfügen (Padding), wenn der Algorithmus das verlangt
- das Resultat dieser Arbeiten verschlüsseln (also ESP-Nutzdaten, Padding, Padding-Länge) unter Verwendung des durch die SA angezeigten Algorithmus.

neuKap17_a.fm Seite 545 Freitag, 18. Oktober 2002 3:53 15

Ankommende IP-Fragmente werden vor der Entschlüsselung zunächst zusammengebaut. Danach sucht der Empfänger die entsprechende SA, basierend auf der IP-Zieladresse und dem SPI. Anschließend kann das Paket entschlüsselt und ggf. authentifiziert werden.

A.5.4 Security Association

Eine Security Association (SA) ist eine Sammlung von Schlüsseln und Regeln, um die Verarbeitung von AH und ESP zu automatisieren. Dabei wird für ankommende und abgehende Pakete für jeden Kommunikationspartner (IP-Adressse) je ein Eintrag angelegt, getrennt nach AH und ESP. Um eine typische bidirektionale Kommunikation zwischen zwei Hosts oder zwei Gateways abzusichern, werden somit zwei SAs (je eins für jede Richtung) benötigt. Werden AH und ESP zusammen eingesetzt, erhöht sich die Anzahl der Einträge sogar auf vier.

Dabei wird jeder SA-Eintrag eindeutig definiert durch den Security Parameter Index (SPI), der IP-Zieladresse und dem eingesetzten Sicherheitsprotokoll (AH oder ESP). der SPI muss in jedes gesendete Paket eingetragen werden.

Zwei SA-Typen sind möglich, durch sie werden Transport- und Tunnelmodus unterschieden. Dabei ist bei der Kommunikation zwischen zwei Sicherheits-Gateways oder zwischen einem Host und einem Sicherheits-Gateway nur der Tunnelmodus möglich.

A.5.5 IPSec-Datenbanken

Die Security Association SA ist das Bindeglied zwischen einem IP-Paket und den Algorithmen und Schlüsseln zur Authentifizierung und Verschlüsselung. Alle SAs eines Systems werden in einer Datenbank, der Security Association Database (SAD) abgelegt. Von der schon erwähnten Datenbank SPD (Security Policy Database) wird für jedes mittels IPSec zu behandelnde Paket ein Verweis auf die betreffende SA in der SAD erzeugt.

A.5.6 Schlüsselverwaltung unter IPSec

IPSec-Implementierungen erlauben sowohl eine manuelle als auch eine automatisierte Schlüsselverwaltung. Die IPSec-Protokolle AH und ESP sind weitgehend unabhängig von den SA-Managementtechniken, wenn auch die betreffenden Techniken einige der angebotenen Sicherheitsdienste beeinflussen.

Die einfachste Form der Verwaltung ist die manuelle: Jedes System wird mit den Schlüsseln und Daten konfiguriert, die notwendig sind, um die sichere Kommunikation mit anderen System sicherzustellen. Manuelle Techniken sind sinnvoll in kleinen und statischen Umgebungen. z. B. könnte ein kleines Unternehmen unter Benutzung von IPSec in Security Gateways ein VPN aufbauen. Wenn die Anzahl

neuKap17_a.fm Seite 546 Freitag, 18. Oktober 2002 3:53 15

der Security-Gateways klein ist und wenn alle Security Gateways unter eine gemeinsame Verwaltung fallen, kann diese manuell sein. Die manuelle Verwaltung ist auch dann sinnvoll, wenn nur ein bestimmter Teil der Kommunikation geschützt werden soll. Das gleiche gilt beim Einsatz von IPSec innerhalb einer Organisation, wenn nur eine kleine Anzahl von Rechnersystemen und/oder Security Gateways vorhanden sind. Die manuelle Verwaltung setzt oft statisch konfigurierte, symmetrische Schlüssel ein, wenn auch andere Optionen genutzt werden können.

In größeren Netzen oder in Netzen, die von verschiedenen Administratoren betreut werden, ist eine manuelle Schlüsselverwaltung im Allgemeinen nicht mehr möglich. IPSec unterstützt verschiedene Verfahren der Schlüsselverwaltung, als Standard ist ISAKMP/Oakley vorgesehen. Bei diesem zweistufigen Verfahren authentifizieren sich die Kommunikationspartner zunächst untereinander. Das geschieht mittels einer der im Standard DSS (Digital Signature Standard) festgelegten Prozeduren über öffentliche und private Schlüssel. Anschließend findet die Erzeugung und der Austausch von Schlüsseln für die ESP-Verschlüsselung mittels Diffie-Hellman statt. Aus den bei Authentifizierung und Schlüsselaustausch ausgetauschten Daten erzeugen beide Partner ihre SAs, mit denen die restliche Kommunikation dann abgewickelt wird.

IPSec lässt aber auch andere Verfahren der Schlüsserverwaltung zu, so etwa die mit dem Protokoll SKIP eingeführten Verfahren. Hier macht ein rascher zeit- oder datengesteuerter Schlüsselwechsel es Lauschern praktisch unmöglich, den Datenverkehr zu verfolgen. Selbst im (unwahrscheinlichen) Glücksfall der Entschlüsselung eines einzelnen Schlüssels kann nur ein winziger Ausschnitt aus dem Datenstrom in sinnvolle Daten verwandelt werden, nach dem nächsten Schlüsselwechsel muss der Hacker praktisch wieder von vorne anfangen.

Bewertung

IPSec ist unter den Standards zur Absicherung von Netzwerkverbindungen sicherlich die Attraktivste. Das Problem des gesicherten Schlüsselaustausches ist aber ebenso ungelöst wie bei den anderen Verfahren. Immerhin unterstützen viele Hersteller von VPNs oder Firewall-Systemen mittlerweile IPSec. Das bedeutet aber nicht, dass IPSec-fähige Geräte beliebiger Hersteller gesichert miteinander kommunizieren können. Zu vielfältig sind die in IPSec vorgesehenen Möglichkeiten, als dass auf sorgfältige Tests verzichtet werden kann. In naher Zukunft sind aber auch hier Fortschritte zu erwarten, da kein Hersteller auf die Möglichkeit verzichten will, sich durch eine problemlose Integrationsfähigkeit seiner Produkte einen Einstieg in neue Märkte zu sichern.

neuKap17_b.fm Seite 547 Freitag, 18. Oktober 2002 3:53 15

Wichtige Adressen

Im Folgenden sind einige wichtige Adressen angegeben, bei denen Hilfestellung zu Problematiken, die mit Firewall-Systemen zu tun haben, erhältlich ist.

- Bundesamt für Sicherheit in der Informationstechnik (BSI)
  Postfach 20 03 63, 53133 Bonn
  Telefon: (02 28) 95 82-444, Fax -427

  `E-Mail: cert@bsi.de`

  BSI-Mailbox: (02 28) 9 58 09 71
- Universität Siegen
  `Homepage: http://www.uni-siegen.de`
- Recht im Internet
  `Homepage: http://www.netlaw.de`
- Utimaco Safeware AG
  Niederlassung Aachen
  Germanusstraße 4, 52080 Aachen

  Tel.: (02 41) 1696-0, Fax: -199

  `Homepage: www.utimaco.de`
- Compumatica secure networks GmbH
  Germanusstraße 4, 52080 Aachen

  Tel.: (02 41) 1696-400, Fax: -410

  `Homepage: www.compumatica.de`

Computer Emergency Response Teams (CERT) sind Organisationen, die über bekannt gewordene Betriebssystemfehler und deren Behebungsmöglichkeiten informieren.

- Computer Emergency Response Team/Coordination Center (CERT/CC),
  Software Engineering Institute
  Carnegie Mellon University, Pittsburgh, PA 15213-3890

  Tel. +1 41 22 68-70 90 (24-Stunden-Hotline)

  ```
  E-Mail: cert@cert.sei.cmu.edu oder cert@cert.org
  ftp: cert.sei.cmu.edu (192.88.209.5)
  ```

neuKap17_b.fm Seite 548 Freitag, 18. Oktober 2002 3:53 15

- Die CERT-Mitteilungen werden in Newsgruppen (comp.security.announce und info.nsfnet.cert) und über Mailinglisten (Aufnahme durch E-mail an: `cert-advisory-request@cert.org`) veröffentlicht.

CERT in Deutschland

- BSI-CERT
  Bundesamt für Sicherheit in der Informationstechnik (BSI)
  Postfach 20 03 63, 53133 Bonn
  Telefon: (02 28) 95 82-444, Fax: -427

  E-Mail: `cert@bsi.de`

- DFN-CERT
  Universität Hamburg

  Fachbereich Informatik
  Vogt-Kölln-Straße 30, 22527 Hamburg

  Telefon: (0 40) 5 47 15-262, Fax: -241

  E-Mail: `dfncert@cert.dfn.de`

  ftp: `ftp.cert.dfn.de: /pub/security`

  gopher: `gopher.cert.dfn.de`

  Aufnahme in Mailingliste für CERT-Mitteilungen durch E-Mail an:
  `dfncert-request@cert.dfn.de`

  Mailinglisten für Diskussionen: `win-sec@cert.dfn.de`

  Mailinglisten für sicherheitsrelevante Informationen:
  `win-sec-ssc@cert.dfn.de`

  URLs:

  FTP: `ftp://ftp.cert.dfn.de/pub.security`

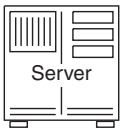
  WWW: `http://www.cert.dfn.de/dfncert.dfncert.html`

- Micro-BIT Virus Center/CERT
  Universität Karlsruhe
  Postfach 69 80, 76128 Karlsruhe
  Telefon: (07 21) 37 64 22, Fax: (07 21) 3 25 50

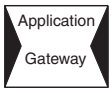
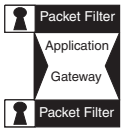
  E-Mail: `cert@rz.uni-karlsruhe.de`

neuKap17_c.fm Seite 549 Freitag, 18. Oktober 2002 3:53 15

Legende

Symbol	Bedeutung
	zu schützendes Netz mit hohem Schutzbedarf
	unsicheres Netz mit nicht abschätzbarem bzw. niedrigem Schutzbedarf
	Workstation, auf der TCP/IP-Applikationen laufen (Browser, Telnet-Client etc.)
	Workstation, auf der das Security Management realisiert ist
	Workstation mit IP-Verschlüsselung
	Workstation, mit der ein Angriff durchgeführt wird
	Notebook, auf dem TCP-Anwendungen laufen
	Notebook mit IP-Verschlüsselung
	Server-System, auf dem TCP-Anwendungen laufen (WWW-Server, FTP-Server, News-Server etc.)
	Modem
	Router

neuKap17_c.fm Seite 550 Freitag, 18. Oktober 2002 3:53 15

Symbol	Bedeutung
	allgemeines Symbol für Firewall-System
	Packet Filter
	Packet Filter mit Verschlüsselung (VPN-Gateway)
	Application Gateway
	High-level-Security-Firewall-System
	Virenscanner
	Intrusion-Detection/Response-System
	Chipkartenleser mit Pin-Pad
	Security Token, der den Benutzern Sicherheitsfunktionen zur Verfügung stellt
	Benutzer
	Chipkarte, die dem Benutzer Sicherheitsdienstleistungen zur Verfügung stellt (Smart Card)
	Mobiltelefon

neuKap17_d.fm Seite 551 Freitag, 18. Oktober 2002 3:53 15

Firewall-Produkte

In der folgenden Tabelle sind einige Firewall-Produkte mit ihren grundsätzlichen Merkmalen aufgelistet, soweit Angaben darüber zur Verfügung standen oder sie eingeschätzt werden konnten.

		Basis			Plattform			
Hersteller	Produkt	Software-basierend	Hardware-basierend	Soft-+ Hardware-basierend	Unix und Derivate	Windows NT	proprietär	Sonstige
Checkpoint	Firewall-1	●	-	- *)	●	●	-	-
Cisco	PIX	-	-	●	-	-	●	-
Utimaco Safeware / Compumatica secure networks	CryptoWall	-	-	●	●	-	●	-
Sun Microsystems	Sun Screen SecureNet 3.1	●	-	-	●	●	-	-

	Techno-logie		Authentisierung					Proxies				
Produkt	Application-Gateway	Packet-Filter	ASCII	Kryptocard	SecureID	RADIUS	Sonstige	SMTP-Proxies	Telnet-Proxies	FTP-Proxies	HTTP-Proxies	Sonstige
Firewall-1	●	●	●	●	●	●	-	●	●	●	●	●
PIX	-	●	-	-	-	●	●	●	-	-	●	●
CryptoWall	●	●	●	●	-	-	●	●	●	●	●	●
Sun Screen SecureNet 3.1	-	●	●	-	●	●	●	-	-	-	-	-

*) Von verschiedenen Herstellern werden Appliances angeboten (z.B. die Safe@-Produktlinie von SofaWare und die Nokia Firewall/VPN Appliance).

neuKap17_d.fm Seite 552 Freitag, 18. Oktober 2002 3:53 15

	Protokoll-Gateway			Kryptographische Mechanismen					
Produkt	Circcuit Level	Umsetzung für IPX	sonstige	DES	Dynamic-Key Exchange	Private-Key	Public-Key	Digitale Signaturen	sonstige
Firewall-1	●	-	-	●	●	●	●	●	●
PIX	●	-	-	●	-	-	-	-	-
CryptoWall	●	-	●	●	-	●	-	-	-
Sun Screen SecureNet 3.1	-	●	-	●	●	●	●	-	-

	Besonderheiten					
Produkt	Virenschutz	VPN-Funktionen	IP Masquerade	HTML-Seiten sperren	Helpdesk, Hotline	Zertifizierung
Firewall-1	●	●	●	●	?	ITSEC E3 *)
PIX	-	●	●	●	?	?
CryptoWall	●	●	●	-	●	ITSEC E3 hoch **)
Sun Screen SecureNet 3.1	-	●	-	-	?	?

*) Lediglich Zertifizierung von Teilkomponenten, Zertifizierung wurde in Großbritannien durchgeführt.

**) Lediglich Zertifizierung von Teilkomponenten.

neuKap17_e.fm Seite 553 Freitag, 18. Oktober 2002 3:53 15

Literaturverzeichnis

/aCam2001/	Markus a Campo, Norbert Pohlmann: »Virtual Private Networks«, MITP-Verlag, Bonn, 2001
/AHKP91/	M.D. Abrams, J. Heaney, O. King, L.J. LaPadula, I.D. Olson: »Generalized Framework for Access Control«, Proceedings of the 14th National Computer Security Conferenz, Oct. 1991
/Alad99/	Aladdin. »Safe Internet Connectivity for the Home & Small Office«, White Paper, Aladdin Knowledge Systems, USA , Seattle 1999
/AbO92/	M.D. Abrams, I.D. Olson: »Rule-Based Trusted Access Control«, in: IT-Security, Proceedings of the IFIP/SEC ´92 Singapore, North-Holland 1992
/BaHoKn/	A. Badach, E. Hoffmann u. O. Knauer: »High Speed Internetworking: Grundlagen und Konzepte für den FDDI und ATM«, Bonn u.a.: Addison-Wesley, 1994
/BLP74/	D.E. Bell, L.J. LaPadula: »Secure Computer System – A Refinement of the Mathematical Model«, NTIS AD-780 528, MTR 2547 Vol. III, MITRE Corp., Bedford, MA, USA, 1974
/Borowka/	Petra Borowka: »Brücken und Router: Wege zum strukturierten Netzwerk«, Bergheim: DATACOM-Verlag Lipinski, 1992
/BSI97/	BSI: »Mit Sicherheit in die Informationsgesellschaft«, Tagungsband, 5. Deutscher IT-Sicherheitskongreß des BSI, Ingelheim: SecuMedia Verlag, 1997
/BSI98/	BSI – Bundesamt für Sicherheit in der Informationstechnik: »Object Code and Optimizing Compiler Analyzing Tool – Analyse der Risiken ausführbarer Web-Contents«, Teil 1; BSI Studie, Bonn, 1998
/BSI99/	BSI: »IT-Grundschutzhandbuch«, BSI 7152, Köln: Bundesanzeiger-Verlag, 1999
/BSI00/	BSI – Bundesamt für Sicherheit in der Informationstechnik: »DDoS Analyse der Angriffe Erkenntnisse, Auswertung, Tendenzen«, BSI-Studie, Bonn 2000
/CCITT/	CCITT: »The Directory – Authentication Framework«, Draft Recommendation X.509, Gloucester: 11/1987
/CERT95/	CERT im DFN: »Sicherheit in vernetzten Systemen«, Hamburg: Workshop, 1995

neuKap17_e.fm Seite 554 Freitag, 18. Oktober 2002 3:53 15

/CESG3/	UK Systems Security Confidence Levels: CESG Memorandum No. 3, Communications-Electronics Security Group: 01/1989
/Chau87/	D. Chaum: »Security without Identification: Transaction Systems to Make Big Brother Obsolete«, Comm. ACM 28, 10/1985, S. 1030-1044, Deutsche Übersetzung in: »Sicherheit ohne Identifizierung«, Informatik-Spektrum 10, 1987, S. 262-277
/CheBe/	W. R. Cheswick, St. M. Bellowin: »Firewalls und Sicherheit im Internet« – Schutz vernetzter Systeme vor cleveren Hackern, Deutsche Übersetzung von Thomas Maus, Mit einem Beitrag über das deutsche Recht von Prof. Dr. U. Sieber, Bonn: Addison-Wesley Publishing Company, 1996
/ChZw96/	D. B. Chapman & E. D. Zwicky: »Einrichten von Internet Firewalls – Sicherheit im Internet gewährleisten«, Bonn: O´Reilly, Internat. Thomson-Publishing, 1996
/Cole99a/	Tim Cole: »Erfolgsfaktor Internet – Warum kein Unternehmen ohne Vernetzung überleben wird«, ECON, 1999
/Cole99b/	Tim Cole, Michael Matzer: »Managementaufgabe Sicherheit«, Hanser, 1999
/Comm98/	ISO/IEC SC27 N2161: »Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and gerneral model« 1998
/DTIEC/	DTI Commercial Security Centre Evaluation Levels Manual, V22 Department of Trade and Security, 02/1989
/Goeb2002/	A. Goebel: »Digitale Signatur«, Vortrag CeBIT 2002, SAP Deutschland AG & Co. KG
/Hamp96/	J. F. Hampe: »Intranet: Einordnung und Entwicklungstrends«, Beitrag zum Kongreß zur Einführung und Anwendung von Intranets in Unternehmen, München: ComMunic, 09/1996
/Harl2000/	Magnus Harlander: »Hochverfügbarkeit und Loadbalancing«, IT-Sicherheit – Praxis der Daten- und Netzsicherheit, DATAKONTEXT-Fachverlag, Köln, 5/2000
/Görtz99/	Horst Görtz, Jutta Stolp: »Informationssicherheit in Unternehmen, Sicherheitskonzepte und -lösungen in der Praxis« Bonn, Addison-Wesley, 1999
/Hugh95/	L.J. Hughes, Jr.: »Actually Useful Internet Security Techniques«, Indianapolis: New Riders Publishing, 1995

neuKap17_e.fm Seite 555 Freitag, 18. Oktober 2002 3:53 15

/ISO9798/	Information Processing Systems – Open Systems Interconnection, Electronic Data Ingerchange for Administration, Commerce and Transport (EDIFACT) – Application Level Syntax Rules
/ITSEC91a/	Commission of the European Communities: »Information Technology Security Evaluation Criteria (ITSEC)«, Brussels, Luxembourg: 1991
/ITSEC91b/	Office for Official Publications of the European Communities: »Information Technology Security Evaluation Criteria«, Luxembourg: 06/1991 (=Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaften): »Kriterien für die Bewertung der Sicherheit von Systemen in der Informationstechnik«, Luxemburg: 06/1991)
/ITSEM94/	Commission of the European Communities, Directorate-General XIII »Information Technology Security Evaluation Manual (ITSEM)« ECSC-EEC-EAEC, Brüssel/Luxembourg, 1994
/Kyas96a/	O. Kyas: »Internet professionell«, Technologische Grundlagen & praktische Nutzung, Bonn: International Thomson Publishing, 1996
/Kyas96b/	O. Kyas: »Sicherheit im Internet – Risikoanalyse, Strategien, Firewalls«, Bergheim: DATACOM-Verlag, 1996
/NCSA/	NCSA: »Firewall Policy Guide«, NCSA Security White Paper Series, Carlisle: NCSA Publication, 1994
/Pohl90/	Norbert Pohlmann: »Das RSA-Verfahren und dessen Anwendung«, DuD, Vieweg, 1990
/Pohl92/	Norbert Pohlmann: »Vernetze Systeme: Alptraum oder Chance zur Lösung der Sicherheitsproblematik?«, Bergheim: DATACOM-Verlag, 1992
/Pohl96/	Norbert Pohlmann: »Datenschutz – Sicherheit in öffentlichen Netzen«, Heidelberg: Hüthig Verlag, 1996
/Pohl97a/	Norbert Pohlmann: »Sinn und Zweck von IT-Sicherheitsstudien, Teil 1 – Feststellung des Schutzbedarfes und Bedrohungsanalyse«, in: W&S – Wirtschaftsschutz & Sicherheitstechnik, Heidelberg: Hüthig Verlag, 3/97

neuKap17_e.fm Seite 556 Freitag, 18. Oktober 2002 3:53 15

/Pohl97b/	Norbert Pohlmann: »Sinn und Zweck von IT-Sicherheitsstudien, Teil 2 – Vom Anforderungskatalog bis zu den Ergebnissen einer IT-Sicherheitsstudie«, in: W&S – Wirtschaftsschutz & Sicherheitstechnik, Heidelberg: Hüthig Verlag, 04/1997
/Pohl 99a/	»Mailtrust macht europäische E-Mail sicher« LANline – Das magazin für Netze, Daten- und Telekommunikation Awi LANline Verlagsgesellschaft, Grasbrumm 10/99
/Pohl 99b/	»Die Zukunft von Firewall-Systemen« DATACOM – Fachzeitschrift für die elektronische Datenkommunikation CMP-WEKA-Verlag, Poing 1/99
/Pohl2000a/	Norbert Pohlmann: »Dezentrale Firewalls schließen Lücken«, KES – Kommunikations- und EDV-Sicherheit, SecuMedia Verlag, Ingelheim 4/2000
/Pohl2000b/	Norbert Pohlmann: »Die Grenzen digitaler Schutzmauern: kalkuliertes Restrisiko« Computerwoche extra, Computerwoche Verlag, München 7/2000
/Pohl2000c/	Norbert Pohlmann: »Personal Firewall« Behörden Online – Innovative Verwaltung, CPM Communication Press, Sankt Augustin 11/2000
/Pohl2000d/	Norbert Pohlmann: »Personal Firewall – Sicherheitsmechanismen für PC gegen Internet-Bedrohungen« IT-Sicherheit – Praxis der Daten- und Netzsicherheit, DATAKONTEXT-Fachverlag, Köln 5/2000
/Pohl2000e/	Norbert Pohlmann: »Personal Firewall-Systeme« Information Security Bulletin – Deutsche Ausgabe, Fachzeitschrift für Führungskräfte im IT-Sicherheitsbereich, CHI Publishing Ltd., Gt. Easton, Großbritannien, 11/2000
/Pohl2001a/	Norbert Pohlmann: »Organisationshandbuch Netzwerksicherheit«, Loseblattwerk mit CD, wird 5 x jährlich aktualisiert, Augsburg: INTEREST-VERLAG, siehe auch: *www.interest.de*
/Pohl2001b/	Norbert Pohlmann: »Grenzen von Firewall-Systemen«, DATACOM – Fachzeitschrift für die elektronische Datenkommunikation, CMP-WEKA-Verlag, Poing 4/2001
/Pohl2001c/	Norbert Pohlmann: »Möglichkeiten und Grenzen von Firewall-Systemen« in: »Kommunikationssicherheit im Zeichen des Internet. Grundlagen, Strategien, Realisierungen, Anwendungen«, hrsg. v. Patrick Horster, Vieweg Verlag, Wiesbaden 2001
/Pohl2001d/	Norbert Pohlmann: »Kosten und Nutzen von Firewall-Systemen – Betriebswirtschaftliche Betrachtung einer IT-Sicherheitsmaßnahme«, IT-Sicherheit – Praxis der Daten- und Netzsicherheit, DATAKONTEXT-Fachverlag, Köln 1/2001

neuKap17_e.fm Seite 557 Freitag, 18. Oktober 2002 3:53 15

/Pohl2001e/	Norbert Pohlmann: »Personal Firewalls: One More Step Towards Comprehensive Security«, Information Security Bulletin, The International Journal for IT Security Professionals, CHI Publishing Ltd., Gt. Easton, Großbritannien, 3/2001
/Pohl2002a/	Norbert Pohlmann: »Authentisierungverfahren mittels Mobiltelefon«, IT-Sicherheit – Management der Daten- und Netzsicherheit, DATAKONTEXT-Fachverlag, 1/2002
/Pohl2002b/	Norbert Pohlmann: »Nutzen und Chancen von Public-Key-Infrastrukturen«, in: »Sicherheitsinfrastrukturen in Wirtschaft und Verwaltung«, hrsg. v. Patrick Horster, IT-Verlag 2002
/PoRi95/	Norbert Pohlmann und Wolfgang Ring: »Faxmanipulation am Beispiel einer Rangbescheinigung«, in: »Elektronischer Rechtsverkehr – Digitale Signaturverfahren und Rahmenbedingungen«, hrsg von: Bundesnotarkammer, Köln: Verlag Dr. Otto Schmidt, 1995
/Rula94/	Christoph Ruland: »Informationssicherheit in Datennetzen«, Bergheim: DATACOM-Verlag, 1993
/Sand00/	Sandbox: »Protection against Malicious Mibile Code«, White Paper, Sandbox Security AG, Germany, Puchheim, 2000
/Santifaller/	M. Santifaller: »TCP/IP und ONC/NFS in Theorie und Praxis – UNIX in lokalen Netzen«, 2. Auflage, Bonn: Addison-Wesley Publishing Company, 1993
/SCSSI/	Catalogue de Critères Destinés à évaluer le Degré de Confiance des Systèmes d'Information, Service Central de la Sécurité des Systèmes d'Information, 07/1989
/Sieber/	Ulrich Sieber: »Computerkriminalität und Informationsstrafrecht – Entwicklungen in der internationalen Informations- und Risikogesellschaft«, in: Computer und Recht 02/1995
/Sobi99/	M. Sobirey: »Datenschutzorientiertes Intrusion Detection«, Vieweg-Verlag, 1999
/STOA/	Scientific and Technological Options Assessment (STOA) of the European Parliament: Report: »An Appraisal of the Technologies to Political Control«, Download und aktuelle Ergänzungen des Reports unter: `www.europarl.eu.int/dg4/stoa/en` oder `http://cryptome.org/stoa-atpc.htm`
/Strömer/	Tobias H. Strömer: »Online-Recht – Rechtsfragen im Internet und in Mailboxnetzen«, Heidelberg: dpunkt-Verlag, 1997
/Tann98/	A.S. Tannenbaum: »Computer Networks« PrenticeHall, New Jersey, 1998

neuKap17_e.fm Seite 558 Freitag, 18. Oktober 2002 3:53 15

/TCSEC/	Department of Defence (USA): Trusted Computer Systems Evaluation Criteria, DOD 5200.28-STD, 12/1985
/WashEv/	K. Washburn, J. Evans: »TCP/IP: Aufbau und Betrieb eines TCP/IP-Netzes«, Bonn u.a.: Addison-Wesley Publishing Company, 1994
/Weck/	G. Weck: »Datensicherheit: Methoden, Maßnahmen und Auswirkungen des Schutzes von Informationen«, Stuttgart: Teubner, 1984
/Woel99/	Woelke von der Brüggen: »Schutz gegen Malicious Mobile Code«, White Paper, Soft Research Linited, Irland 1999
/ZSIEC/	BSI: Criteria for the Evaluation of Trustworthiness of Information Technology (IT) Systems, German Information Security Agency (Bundesamt für Sicherheit in der Informationstechnik) 9, 01/1989

neuKap17_f.fm Seite 559 Freitag, 18. Oktober 2002 3:53 15

Sicherheitsanforderungen an Internet-Firewalls (BSI)

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in Zusammenarbeit mit Firewall-Herstellern Sicherheitsanforderungen an Internet-Firewalls erarbeitet, die vom BSI im März 1996 veröffentlicht wurden und im Folgenden vollständig und unverändert wiedergegeben werden.

F.1 Einleitung

Die Zusammenfassung vorhandener Teilnetze zu globalen Netzen wie dem Internet führt zu einem neuen Informationsangebot, welches über kurz oder lang für viele Menschen von großer Bedeutung sein wird. Gleichzeitig führt die zunehmende lokale Vernetzung von Rechnersystemen in der Industrie und in Behörden sowie die Zugangsmöglichkeiten für private Personen über kostengünstige Internet Provider dazu, dass von fast jedem Arbeitsplatzrechner und von vielen privaten PCs aus auf die vielfältigen Informationsquellen zugegriffen werden kann.

Diese weltweite Vernetzung lässt aber auch neue Gefährdungen entstehen, da prinzipiell nicht nur ein Informationsfluss von außen in das zu schützende lokale Netz oder auf den privaten PC stattfinden kann, sondern auch in die andere Richtung (Verlust der Vertraulichkeit). Darüber hinaus gefährdet die Möglichkeit *remote*, d.h. von einem entfernten Rechner aus (z.B. aus dem Internet) Befehle auf Rechnern im lokalen Netz ausführen zu lassen, die Integrität und die Verfügbarkeit der lokalen Rechner und dadurch indirekt auch die Vertraulichkeit der lokalen Daten.

F.2 Gefährdungen bei der Benutzung des Internet

Im Folgenden werden einige der wesentlichen Probleme beschrieben, die bei der Benutzung des Internets auftreten können. Für fast alle diese Probleme gibt es Lösungen, sodass eine Nutzung des Internets mit ausreichender Sicherheit möglich ist.

neuKap17_f.fm Seite 560 Freitag, 18. Oktober 2002 3:53 15

F.2.1 Vielfalt der Netzdienste

Durch den Anschluss eines für sich alleine sicheren Rechner-Systems an ein Netz, sei es ein Inhouse-LAN oder auch das Internet, entstehen Gefährdungen dadurch, dass die Vielzahl neuer Programme, die für die verschiedenen Zugänge notwendig sind, fehlerhaft konfiguriert sein können oder Programmierfehler enthalten. Während der Zugang zu einem Stand-Alone-System im Wesentlichen durch den LogIn-Prozess o.Ä. geregelt wird, existiert für jeden Dienst, der über einen Netzzugang ermöglicht werden soll, ein eigener Daemon-Prozess. Dieser kann falsch konfiguriert oder fehlerhaft sein.

Eindringlinge mit hohem Kenntnisstand über Fehler in diesen Programmen oder sogar im Betriebssystem-Kern können diese dann ausnutzen, bevor der Administrator diesen Kenntnisstand erreicht und die Sicherheitslücken schließen kann. So nutzte z.B. der Autor des Internet-Wurms einen Fehler in der Routine *gets* des Programms *fingerd* aus, um den Speicher mit einer Rücksprungadresse auf eine *SUID*-Root Shell zu überschreiben. Ein ähnlicher Fehler entstand auch bei der Programmierung eines *http*-Daemons, der zu einem entsprechenden CERT (Computer Emergency Response Team) Advisory im Februar 1995 führte.

Andererseits können fertige »Hackprogramme« oder bekannte Bugs auch bei geringem Kenntnisstand hohen Schaden anrichten. So testet z.B. das Programm *ISS* (Internet Security Scanner) systematisch beliebig viele Systeme auf häufig vorhandene Konfigurationsfehler wie einen *guest* Account ohne Passwort oder falsch exportierte Dateisysteme.

Eine große Gefährdung geht von falsch konfigurierten Diensten aus, deren Kontrollmechanismen dann leicht zu umgehen sind oder anders als vorgesehen arbeiten. Der WWW-Client *Mosaic* beispielsweise bietet die Möglichkeit, Skripten ausführen zu lassen, die jede beliebige Befehlsfolge enthalten können und über die der Anwender nur in einer kleinen Statuszeile informiert wird. Diese Option lässt sich allerdings bei der Installation abschalten.

F.2.2 Verlust der Vertraulichkeit und Integrität

Wesentliche Gefährdungen bei der Benutzung des Internets stellen der Verlust der Vertraulichkeit durch ein Mitlesen der versandten Daten und der Verlust der Integrität durch die Manipulation der Daten dar. Viele der im Internet benutzten Dienste übertragen die Benutzernamen und Passwörter offen. So kann jeder, der privilegierten Zugang zu einem der an der Übertragung beteiligten Gateways, Router oder Server hat, diese Daten lesen oder verändern. Dieses Problem war auch Thema eines Anfang 1994 herausgegebenen CERT Advisory mit dem Titel »Ongoing Network Monitoring Attacks«, welches eine große Resonanz in der Presse hatte. Hierbei wurden so genannte *sniffer*-Programme gezielt zum Mitlesen von Passwörtern und

neuKap17_f.fm Seite 561 Freitag, 18. Oktober 2002 3:53 15

Benutzernamen in den Rechnern installiert. Man kann davon ausgehen, dass auf diese Weise mehrere 10 000 Accounts unsicher geworden sind.

Das Mitlesen der versandten Daten ermöglicht auch so genannte Replay Attacks, bei denen einmal zur Authentisierung benutzte Daten, wie z. B. verschlüsselte Passwörter, von einem Angreifer bei einem späteren Zugangsversuch wieder eingespielt werden.

Ein besonderes Problem stellt auch der Einsatz von PCs in einem LAN dar, da hier jeder Benutzer Programme zum Mitlesen oder Verändern der Daten ablaufen lassen kann. Auch der Schutz, den die Einführung der so genannten privilegierten Ports (Portnummer < 1024) bieten soll, wird durch nicht vertrauenswürdige Rechner in einem LAN unwirksam.

F.2.3 Konzeptionsfehler

Einige TCP/IP spezifische Gefährdungen sind in [1] beschrieben. Die wichtigsten sind:

- *IP-Spoofing*: Der mit diesem Ausdruck bezeichnete Konzeptionsfehler der TCP/IP Protokoll-Umgebung wurde schon im Jahre 1985 von Robert Morris beschrieben [2]. Der Fehler beruht darauf, dass bei vielen Diensten – insbesondere auch bei Firewall-Anordnungen – die Authentisierung der Rechner nur über die IP-Adresse erfolgt. Nutzt man darüber hinaus noch aus, dass die von den Rechnern zur Synchronisation benutzten Sequenznummern leicht zu erraten sind, ist es möglich, Pakete an jede beliebige Adresse zu schicken und damit entsprechend konfigurierte Dienste wie *rlogin* zu benutzen, ohne jemals ein Antwortpaket von dem missbräuchlich benutzten Rechner zu erhalten.

  Weitere Dienste, die hiervon bedroht werden, sind *rsh, rexec,* X-Window, RPC-basierende Dienste wie NFS und der TCP-Wrapper, der ansonsten ein sehr sinnvoller Dienst zur Einrichtung einer Zugangskontrolle für TCP/IP-vernetzte Systeme ist. Leider sind auch die in der Schicht zwei (ISO/OSI-Modell) eingesetzten Ethernet- oder Hardware-Adressen leicht zu fälschen und somit für eine Authentisierung nicht geeigneter.

  In LANs, in denen das Address Resolution Protocol (ARP) eingesetzt wird, sind sehr viel wirkungsvollere Spoofing-Angriffe möglich. Es reicht dann meist schon, die Kontrolle über einen der Rechner im LAN zu bekommen, um das gesamte Netz zu kompromittieren.

- *Source Routing:* Der Missbrauch des Routing-Mechanismus und -Protokolls ist wahrscheinlich die einfachste protokoll-basierte Angriffsmöglichkeit. Man nutzt hierbei aus, dass sich in einem IP-Paket der Weg, auf dem das Paket sein Ziel erreichen soll oder den die Antwortpakete nehmen sollen, vorschreiben

neuKap17_f.fm Seite 562 Freitag, 18. Oktober 2002 3:53 15

lässt, sodass nicht die durch die Routing-Tabellen angegebenen sicheren Wege benutzt werden.

Auch der Einsatz von dynamischem Routing stellt eine Angriffsmöglichkeit dar, da es möglich ist, Routing-Informationen an einen Rechner zu schicken, die dieser in der Regel ungeprüft zum Aufbau seiner Routing-Tabellen benutzt. Weitere Sicherheitsüberlegungen im Zusammenhang mit Routing finden sich in [3].

- *ICMP*: Das Internet Control Message Protocol lässt sich in mehrfacher Weise missbrauchen. Zum einen können über *Redirect* Pakete die Routing-Tabellen eines Rechners geändert werden. Zum anderen lassen sich durch gefälschte *Destination Unreachable* oder *Time to Live Exceeded* Pakete »denial of service« Angriffe durchführen, durch die bestehende Verbindungen unterbrochen werden können.

  Die Gefahren durch diese Konzeptionsfehler lassen sich verringern, wenn die in einer TCP/IP-Verbindung zwischen zwei Rechnern benutzten Sequenznummern zufällig gewählt werden, sodass es für einen Dritten nicht möglich ist, die nächste Nummer zu erraten und für ein gefälschtes Paket zu verwenden.

F.2.4 Missbrauch von frei verfügbaren Informationen

Viele Programme, die für die ungehinderte Weitergabe von Informationen in einem »offenen« Umfeld konzipiert wurden, liefern potenziellen Angreifern Daten, die diese missbrauchen können. Hierzu gehören z. B. der *finger*-Daemon, mit dessen Hilfe Namen, Telefonnummern, Raumnummern usw. von Benutzern entfernter Rechner abgefragt werden können. Diese Angaben lassen sich dann für Wörterbuchattacken zum Knacken von Passwörtern benutzen. Weitere Gefahren gehen von der Weitergabe von Konfigurationsdaten aus, wie sie z. B. die Befehle *showmount, rpcinfo* oder *netstat* liefern.

Der Einsatz eines Domain Name Systems (DNS), das für die Umsetzung eines Internet-Namens wie *rechner1.universität.de* in die zugehörige Adresse zuständig ist, stellt eine weitere Gefahrenquelle dar, da ein Angreifer durch die Übernahme dieses Servers die Möglichkeit hat, gefälschte Nummern zu verschicken, sodass jeglicher Verkehr von ihm kontrolliert werden kann. Ein DNS Server sollte also an einer besonders geschützten Stelle im Netz stehen!

F.3 Schutzmöglichkeiten

Um die oben beschriebenen Bedrohungen abwehren zu können, bieten sich verschiedene Möglichkeiten an, die sich gegenseitig ergänzen. Dies sind der Einsatz von Verschlüsselungsverfahren sowohl auf der Anwendungsschicht als auch in den unteren Schichten (z. B. X.25-Verschlüsselung, IPv6), die für eine gesicherte

neuKap17_f.fm Seite 563 Freitag, 18. Oktober 2002 3:53 15

Übertragung der Daten sorgen. Des Weiteren ist die Aufklärung und ständige Fortbildung der Anwender und Administratoren ein wesentlicher Punkt, da nur so neuen Gefährdungen begegnet werden kann. Hilfestellung bei vorbeugenden Maßnahmen und zur Schadensbegrenzung bei erfolgten Angriffen bieten die Computer Emergency Response Teams (CERT), von denen eines beim BSI (siehe Abschnitt 5) angesiedelt ist.

Eine weitere Schutzmöglichkeit gegen Angriffe aus dem Internet bieten Internet Firewalls (i.f. auch kurz als Firewall bezeichnet), d.h. eine Anordnung von Hard- und Software, die als *alleiniger* Übergang zwischen zwei zu trennenden TCP/IP Netzen dient, von denen das eine einen höheren Schutzbedarf hat. Das BSI hat in Zusammenarbeit mit Anwendern und Herstellern einen Kriterienkatalog (siehe Abschnitt 4) für den Einsatz von Firewalls in Sicherheitsbereichen (z.B. Behörden) erarbeitet. Als einführende Literatur zu diesem Thema sind [4] und [5] geeignet.

Ausgehend von den Schutzzielen, die in einer Sicherheitsanalyse gemäß Sicherheitshandbuch des BSI [8] definiert wurden, muss sich die Schutzbedarfsfeststellung für das zu schützende Netz gegenüber Angriffen aus dem Internet an der Schutzklasse der im zu schützenden Netz übertragenen und gespeicherten Daten orientieren. Kann keine sichere Trennung der Informationen vorgenommen werden, so bestimmen die Informationen mit dem höchsten Schutzbedarf das Schutzniveau.

Schutzziel:	**Vertraulichkeit und Integrität**	**Verfügbarkeit**
	Die unbefugte Kenntnisnahme oder Veränderung der lokal übertragenen oder gespeicherten Daten und der unbefugte Zugang zu lokalen Rechnern	Der Angriff auf die Verfügbarkeit der lokalen Netzkomponenten
Schutzbedarf (Schutzklasse):		
mittel (1)	mit einfachen Mitteln soll abgewehrt werden.	
hoch (2)	mit qualifizierten Angriffen soll abgewehrt werden. Ein Restrisiko wird in Kauf genommen.	
sehr hoch (3)	muss verhindert werden. Ein minimales Restrisiko wird in Kauf genommen. (Keine 100% Sicherheit möglich!)	

Für die zu schützenden Netze müssen alle notwendigen technischen Sicherheitsmaßnahmen durchgeführt werden, die dem Schutzbedarf der zugeordneten Schutzklasse entsprechen. Da die zurzeit verfügbaren Firewall-Lösungen keine Möglichkeiten für eine Einstufung der übertragenen Informationen oder der Benutzer im Sinne einer regelbasierten Zugriffskontrolle (MAC) bieten, sind die dargestellten Maßnahmen nicht geeignet, um Informationen mit unterschied-

neuKap17_f.fm Seite 564 Freitag, 18. Oktober 2002 3:53 15

lichen Sicherheitsanforderungen getrennt voneinander zu bearbeiten (Multi Level Security). Des Weiteren bieten die zurzeit verfügbaren Firewall-Lösungen keinen einheitlichen Standard für die verschlüsselte Übertragung von Informationen, sodass für eine sichere Datenübertragung über unsichere Kanäle wie dem Internet zusätzliche Geräte und Maßnahmen nötig sind.

Beim mittleren Schutzbedarf sollten alle im Grundschutzhandbuch [6] des BSI für Firewalls relevanten Maßnahmen durchgeführt werden. Eine objektive Überprüfung der Umsetzung dieser Maßnahmen bietet eine Evaluierung nach E3 mittel gem. ITSEC [7] für die unten aufgeführten Funktionalitäten (s. Abschnitt 4).

Der hohe Schutzbedarf lässt sich durch den Einsatz einer Firewall erreichen, die nach E3 hoch gem. ITSEC für die unten aufgeführten Funktionalitäten evaluiert wurde. Eine Analyse des Quellcodes, wie sie ab dieser Evaluierungsstufe gefordert wird, ist zur Abwehr von qualifizierten Angriffen unumgänglich. Das vorhandene Restrisiko besteht dann im Wesentlichen aus der Unzulänglichkeit der Software, die ggf. bei einer Evaluierung nach höheren Stufen gem. ITSEC aufgedeckt würde. Das Risiko lässt sich durch den Einsatz redundanter Komponenten von verschiedenen Herstellern für den Aufbau der Firewall verringern.

Die Verarbeitung von Informationen mit sehr hohem Schutzbedarf erfordert aus Sicherheitsgründen in der Regel eine Isolierung der dafür vorgesehenen Komponenten. Muss trotzdem von diesen Komponenten aus eine Informationsbeschaffung im Internet durchgeführt werden, so ist dies nur über eine Firewall vertretbar, die nach E6 hoch gem. ITSEC für die unten aufgeführten Funktionalitäten evaluiert worden ist. Die bei dieser Evaluierungsstufe erhobene Forderung einer Evaluierung auch des Objektcodes erscheint zur Abwehr gezielter nachrichtendienstlicher Angriffe unumgänglich, da auch eine Manipulation der Betriebssysteme und Compiler direkt beim Hersteller nicht auszuschließen ist. Diese Maßnahme erzeugt sehr hohe Kosten, sodass in der Regel der Einsatz eines separaten Netzes mit isolierten Komponenten, das ausschließlich für die Informationsbeschaffung im Internet eingesetzt wird, vernünftiger erscheint. Hierdurch würde auch die Gefährdung durch die Übertragung von Informationen zwischen zwei Anwendungen auf einem Arbeitsplatzrechner (»Cut and Paste«) auf das jetzt schon vorhandene Maß begrenzt werden.

Des Weiteren ist zum Erreichen eines sicheren Umfelds für die hohe und sehr hohe Schutzstufe die Durchführung einer Sicherheitsanalyse gemäß Sicherheitshandbuch des BSI [8] erforderlich!

neuKap17_f.fm Seite 565 Freitag, 18. Oktober 2002 3:53 15

F.4 Forderungen an Firewalls

Sicherheitsspezifische Funktionen sind alle Funktionen einer Firewall, die direkt zum Erreichen der Sicherheitsziele beitragen.

Sicherheitsrelevante Funktionen tragen zum sicheren Funktionieren der Firewall bei und leisten häufig nicht nur Dienste für die sicherheitsspezifischen Funktionen, sondern auch für nicht sicherheitsbezogene Funktionen. Für gewöhnlich hängen sicherheitsspezifische Funktionen vom korrekten Betrieb der sicherheitsrelevanten Funktionen ab. Sicherheitsrelevante Funktionen sind alle Bestandteile, die für die Ausführung der sicherheitsspezifischen Funktionen benötigt werden, also z. B. Teile des Betriebssystems wie Netzwerktreiber, Bibliotheksfunktionen o. Ä. Sie müssen also auch gem. der oben aufgeführten Evaluationsstufen geprüft werden, wobei auch Wechselwirkungen zu berücksichtigen sind! Zur Erreichung einer größtmöglichen Vereinfachung und Standardisierung sollten die sicherheitsrelevanten Funktionen über eine kleine Anzahl von genau definierten Schnittstellen angesprochen werden können.

Die sicherheitsspezifischen Funktionen einer Firewall lassen sich wie folgt unterteilen:

a) Funktionen zum Schutz gegen direkte Angriffe auf die Firewall-Anordnung (siehe F.4.1).
b) Funktionen zum Schutz des zu sichernden Netzes gegen Angriffe aus dem unsicheren Netz (siehe F.4.2).

F.4.1 Forderungen zur Abwehr von Angriffen auf die Firewall-Anordnung

In Klammern beigefügte Erläuterungen dienen der Verständlichkeit und sind nicht Bestandteil der Forderungen. Insbesondere werden die durch diese Maßnahme abgewehrten *Bedrohungen (B)* dargestellt.

Da die Verwaltung und Wartung der Firewall-Anordnung in der Regel von einem kleinen Kreis von Administratoren und Revisoren durchgeführt wird, ist die in ITSEC F-C2 beschriebene Funktionalität mit den folgenden Zusätzen ausreichend:

(Wichtig ist, dass für Administrator und Revisor unterschiedliche Zugriffsrechte realisiert werden können. Die Forderung der Stufe F-B1, zusätzlich zur benutzerbestimmbaren Zugriffskontrolle Funktionen zur Verwaltung von Sensitivitätsattributen einzuführen, wird hier nicht erhoben, da die auf der Firewall vorhandenen Daten (Access-Listen, Benutzerdaten, Protokollinformationen) nicht unterschiedlich eingestuft werden müssen.)

neuKap17_f.fm Seite 566 Freitag, 18. Oktober 2002 3:53 15

F.4.1.1 Identifikation und Authentisierung für Administrator und Revisor nur über einen vertrauenswürdigen Pfad.

(Dies könnte z. B. die Konsole, eine verschlüsselte Verbindung oder ein separates Netz sein.
B: Mitlesen oder Verändern der Authentisierungsinformationen. Auch bei einer Evaluierung mit der angestrebten Mechanismenstärke »Mittel« ist eine starke Authentisierung erforderlich.)

F.4.1.2 Die Defaulteinstellung der Rechte muss sicherstellen, dass die Rollen Administrator und Revisor realisiert sind.

(B: Falsch gesetzte Rechte ermöglichen es auch nicht autorisierten Benutzern, die Access-Dateien zu verändern oder die Protokolle zu lesen.)

F.4.1.3 Bei einem Ausfall der Protokollierungskomponente muss eine Warnung ausgegeben werden, die ein unverzügliches Eingreifen des Administrators ermöglicht. Es muss möglich sein, die Firewall so zu konfigurieren, dass bei einem Ausfall der Protokollierungskomponenten jegliche nicht administrative Nutzung (im Sinne von F.4.1.1) der Firewall unterbunden wird.

(Wenn eine ordnungsgemäße Protokollierung nicht mehr möglich ist (z. B. weil auf dem zugehörige Datenträger kein Platz mehr ist), muss die Firewall jeglichen Verkehr blockieren. Protokollierungskomponenten sind u. a. Prozesse in den Packet-Filtern oder im Application Gateway, die Protokollinformationen über Veränderungen an Konfigurationsdateien oder über abgewiesene oder durchgelassene Pakete erzeugen oder die Datenträger, auf denen die Protokollinformationen gespeichert werden.
B: Keine Protokollierung von Angriffsversuchen.)

F.4.1.4 Integritätstests der eingesetzten Programme und Dateien mindestens einmal täglich: Es muss möglich sein, die Firewall so zu konfigurieren, dass bei einer Integritätsverletzung jegliche nicht administrative Nutzung der Firewall (im Sinne von F.4.1.1) unterbunden wird. Die für den Integritätstest notwendigen Programme und Dateien müssen auf einem Medium speicherbar sein, welches hardware-mäßig gegen Schreibzugriffe gesichert werden kann. Es muss protokolliert werden, welche Änderungen (mit Datum und Uhrzeit) an der Konfiguration der Firewall vorgenommen wurden.

(Die Tests sollten regelmäßig, aber nicht immer zur gleichen Zeit durchgeführt werden können. Es sollten Verfahren eingesetzt werden, die eine Änderung der Daten und Programme, die auf einer der Komponenten der Firewall vorliegen, rechtzeitig erkennen lassen.
B: Durch Ausnutzung verschiedener Gefährdungen ist es oftmals möglich, die Benutzerrechte für einige oder alle Dateien auf dem angegriffenen Rechner zu

neuKap17_f.fm Seite 567 Freitag, 18. Oktober 2002 3:53 15

erlangen und diese – insbesondere auch Programme wie z. B. LogIn – zu verändern, sodass ein erneuter Angriff auf diesen Rechner sehr vereinfacht wird. Die Access-Listen sind die wesentlichen Daten für den Betrieb der Firewall und müssen besonders gesichert werden.)

F.4.1.5 Es muss möglich sein, die Firewall so zu konfigurieren, dass bei einem Systemabsturz jegliche nicht administrative Nutzung der Firewall (im Sinne von F.4.1.1) unterbunden wird.

(Dies lässt sich z. B. durch ein Booten in den Single-User-Mode erreichen. B: Erzeugung eines neuen, weniger geschützten Betriebssystem-Kerns oder Benutzung alter oder fehlerhafter Access-Listen bei einem Neustart, der durch einen Angreifer erfolgt.)

F.4.1.6 Auf den eingesetzten Komponenten darf nur Software vorhanden sein, die für die Funktionsfähigkeit der Firewall nötig ist. Die benutzte Software (inkl. aller Konfigurationsdateien) muss ausführlich dokumentiert und begründet werden.

(Dies sind z. B. Treiber, die aus dem Betriebssystem-Kern entfernt werden müssen, oder Software für die grafische Benutzeroberfläche. Das Verbleiben von Software muss dokumentiert und begründet werden.
B: Ausnutzung von Sicherheitslücken in Programmen, die für den Betrieb der Firewall nicht nötig sind und u. U. nicht richtig konfiguriert oder fehleranfällig sind.)

F.4.2 Forderungen zur Abwehr von Angriffen aus dem Internet auf das zu sichernde Netz

F.4.2.1 Obligatorische Forderungen:

F.4.2.1.1 Die Firewall-Anordnung muss für den Fall des hohen und sehr hohen Schutzbedarfs aus mindestens zwei getrennten Filtern bestehen. Die Filter müssen hintereinander angeordnet sein, sodass für eine Verbindung zwischen den beiden beteiligten Netzen beide Filter passiert werden müssen. Die Filter müssen mit unterschiedlicher Hard- und Software (Betriebssystem) arbeiten und unterschiedliche Formate für die Beschreibung der Filterregeln benutzen.

(Die beiden Filter können z. B. ein Packet-Filter und ein Dual-homed Application-Gateway sein. Durch die unterschiedlichen Betriebssysteme (d.h. unterschiedliche Quellen, Autoren usw.) wird erreicht, dass mögliche Software-Fehler in einer Komponente nicht sofort zum Überwinden der Firewall benutzt werden können. Durch die unterschiedliche Beschreibung der Filterregeln wird die Wahrscheinlichkeit erhöht, dass Fehler, die bei der Verwaltung einer Komponente gemacht werden, von der richtig konfigurierten

neuKap17_f.fm Seite 568 Freitag, 18. Oktober 2002 3:53 15

anderen Komponente abgefangen werden.
B: Ein Fehler in einer Komponente erleichtert einen erfolgreichen Angriff.)

F.4.2.1.2 Die Einstellung der Filterregeln bei einer Erstinstallation und die Anordnung der Komponenten muss sicherstellen, dass alle Verbindungen, die nicht explizit erlaubt sind, blockiert werden. Auch bei einem völligen Ausfall der Firewall-Komponenten dürfen nur Verbindungen durchgelassen werden, die explizit erlaubt worden sind.

(Es muss die Regel »Alles, was nicht ausdrücklich erlaubt ist, ist verboten« realisiert sein. Zum Beispiel darf ein Benutzer, der keinen Eintrag in einer Access-Liste hat, keine Möglichkeit haben, Dienste des Internets zu benutzen.
B: Ausnutzung eines nicht als sicherheitsgefährdend angesehenen und deshalb nicht verbotenen Dienstes durch einen Angreifer. Automatisches Umleiten der Pakete um ein defektes Gateway zu umgehen.)

F.4.2.1.3 Die Struktur des zu schützenden Netzes muss verdeckt werden können, d.h. dass keine internen Informationen wie Benutzernamen, Rechnernummern, -namen und Mailadressen nach außen gelangen können.

(Dies lässt sich z. B. durch den Einsatz eines Application-Gateways und zweier DNS Server erreichen.
B: Mail-Adressen, IP-Nummern, Rechnernamen können bei einem nicht durch eine Firewall geschützten Netz von jedem Benutzer im Internet abgerufen werden, wodurch sich Rückschlüsse auf die interne Netzstruktur und die internen Anwender ziehen lassen.)

F.4.2.1.4 Die Verwaltung der Komponenten muss zentral über einen vertrauenswürdigen Pfad (z. B. ein separates Netz oder über eine verschlüsselte Verbindung) erfolgen und übersichtlich sein (graphisches Interface).

(B: Mitlesen oder Verfälschung der Access- oder Protokoll-Daten.)

F.4.2.1.5 Der Aufbau von Verbindungen auf der Anwendungsschicht durch die Firewall muss benutzerabhängig und zeitabhängig erlaubt oder verboten werden können.

(Dies lässt sich z. B. durch den Einsatz von Proxy-Prozessen für jeden der in F.4.2.1.9 aufgeführten Dienste erreichen.
B: Unbefugte Benutzung.)

neuKap17_f.fm Seite 569 Freitag, 18. Oktober 2002 3:53 15

F.4.2.1.6 Zur Benutzer-Identifikation müssen starke Authentisierungsmethoden benutzt werden.

(B: Mitlesen von Passwörtern.)

F.4.2.1.7 Es muss möglich sein, mehrere Benutzer zu einer Gruppe zusammenzufassen.

(B: Fehler bei Einstellung der Access-Listen durch eine unübersichtliche Anzahl von Benutzern.)

F.4.2.1.8 Die Filterregeln müssen auf ihre Widerspruchsfreiheit überprüft werden.

(B: Ein nicht unmittelbar erkennbarer Fehler in den Filterregeln.)

F.4.2.1.9 Es müssen mindestens die Protokolle Telnet, FTP, SMTP, DNS, NNTP, und HTTP unterstützt werden. Für Telnet-Verbindungen vom Internet zur Firewall (kommende Verbindungen) muss durch zusätzliche Prozesse eine Verschlüsselung der übertragenen Nutzinformationen durchgeführt werden.

(Dies kann z. B. durch den Einsatz spezieller Telnet Server und Clients geschehen.
B: Werden diese grundlegenden Dienste nicht zur Verfügung gestellt, werden u. U. andere, unsichere Wege ins Internet genutzt.)

F.4.2.1.10 Für Verbindungen auf der Anwendungsschicht müssen zusätzlich alle Befehle, die den Import von Daten in das zu schützende Netz (z. B. ein *retr* bei *FTP*) oder den Export von lokalen Daten ins Internet (z. B. ein *post* bei *http*) bewirken, benutzerabhängig und zeitabhängig erlaubt oder verboten werden können.

(B: Unerlaubtes Verschicken von Daten ins Internet.)

F.4.2.1.11 Für jede aufgebaute und abgewiesene Verbindung auf der Anwendungsschicht muss eine Protokollierung von Benutzer-Identifikation, IP-Adresse des Quell- und Zielrechners, Portnummer, Zeit und Datum durchgeführt werden, wobei auch Einschränkungen auf bestimmte Verbindungen möglich sind.

(Die Einschränkungen müssen z. B. ermöglichen, dass nur abgewiesene Verbindungsversuche protokolliert werden. Der vertrauenswürdige Pfad kann z. B. durch eine verschlüsselte Verbindung oder ein separates Netz realisiert werden.
B: Erfolgreiche Angriffe können nicht erkannt, entstandene Veränderungen nicht rückgängig gemacht werden.)

neuKap17_f.fm Seite 570 Freitag, 18. Oktober 2002 3:53 15

F.4.2.1.12 Spezielle, einstellbare Protokollmeldungen müssen zu einer unverzüglichen Warnung führen.

(B: Zu spätes Erkennen eines Angriffs.)

F.4.2.1.13 Die Protokollinformationen von allen Komponenten müssen über einen vertrauenswürdigen Pfad an eine zentrale Stelle geschickt werden können.

(B: Veränderung der Protokollinformation vor ihrer endgültigen Speicherung.)

(B: Durch einen Fehler in einem Proxy-Server kann die Ausführung von allen im benutzten Dateibaum vorhandenen Programmen möglich werden.)

F.4.2.1.14 Bei der Benutzung von FTP muss es möglich sein, den Verbindungsaufbau für die Datenverbindung (FTP-DATA) von der Firewall ins Internet durchführen zu lassen (Benutzung des PASV Kommandos).

(B: Verbindungsaufbau vom unsicheren Netz ins zu schützende Netz für die FTP-DATA Verbindung.)

F.4.2.1 Zusätzliche Forderungen bei Verwendung von Filtern auf der Ebene drei (IP) und vier (TCP, UDP), im Folgenden auch als Packet-Filter bezeichnet:

F.4.2.1.1 Die Weiterleitung von Paketen muss abhängig von

a) IP-Quell- und IP-Zieladresse einzelner Rechner oder kompletter Teilnetze und

b) Quell- und Zielport für TCP und UDP erlaubt oder verboten werden können. Dies wird in Filterregeln festgelegt.

(Der Quell-Port ist z. B. für einen Zone-Transfer zwischen den UDP-Ports 53 zweier DNS Server wichtig.
B: Zugang zum zu schützenden Netz von allen Rechnern im Internet möglich.)

F.4.2.1.2 Die Filterung gemäß F.4.2.2.1 muss getrennt für jedes Interface möglich sein.

(B: Um IP-Spoofing-Angriffe abzuwehren, dürfen Pakete, die den Packet-Filter vom unsicheren Netz aus erreichen, keine IP-Adresse von Rechnern aus dem zu schützenden Netz haben. Dies kann nur an dem mit der unsicheren Seite verbundenen Interface festgestellt werden.)

F.4.2.1.3 Die Reihenfolge der Filterregeln darf nicht automatisch vom Packet-Filter verändert werden.

(B: Unbekannte Ergebnisse der Filterregeln und u. U. eine Aufhebung des Schutzes durch den Packet-Filter.)

neuKap17_f.fm Seite 571 Freitag, 18. Oktober 2002 3:53 15

F.4.2.1.4 Wenn mehr als zwei Interfaces vorhanden sind, muss eine Filterung getrennt für kommende und gehende Pakete möglich sein.

(Bei Packet-Filtern mit zwei Interfaces sind die eingehenden Pakete des einen Interfaces automatisch die ausgehenden des anderen Interfaces.
B: Unübersichtlichkeit der Access-Regeln.)

F.4.2.1.5 Bei TCP-Paketen muss eine Unterscheidung, ob ein Verbindungsaufbau stattfindet oder eine bestehende Verbindung benutzt wird, d.h. eine Unterscheidung zwischen ACK und ACK-losen Paketen, möglich sein.

(Nur so lässt sich sicherstellen, dass ein Verbindungsaufbau nur vom zu schützenden Netz ins unsichere Netz erfolgt.
B: Ungesicherter Verbindungsaufbau ins zu schützende Netz.)

F.4.2.1.6 Die Filterregeln müssen auf ihre Widerspruchsfreiheit überprüft werden.

(B: Ein nicht unmittelbar erkennbarer Fehler in den Filterregeln.)

F.4.2.1.7 Protokollierung von IP-Nummer, Dienst, Zeit und Datum für jedes Paket, wobei auch Einschränkungen auf bestimmte Pakete (z.B. nur Pakete mit einer speziellen Quell-Adresse) möglich sind.

(B: Erfolgreiche Angriffe können nicht erkannt, entstandene Veränderungen nicht rückgängig gemacht werden.)

F.4.2.1.8 Spezielle, einstellbare Protokollmeldungen müssen zu einer unverzüglichen Warnung führen.

(B: Zu spätes Erkennen eines Angriffs.)

F.4.2.1.9 Die Protokollinformationen müssen über einen vertrauenswürdigen Pfad an eine zentrale Stelle geschickt werden können.

(Die Protokollierung der Hardware-Adresse ist z.B. bei einem Angriff über mehrere Hops interessant.
B: Verfälschung der Protokollinformationen.)

F.4.2.1.10 Im Falle der Kombination des Packet-Filters mit einem Router darf die Sicherheit der Firewall nicht durch eine Veränderung der Routing-Einträge gefährdet werden. Es muss statisches Routing benutzt werden.

(B: Möglichkeit, Routing-Informationen an einen Rechner zu schicken, die dieser in der Regel ungeprüft zum Aufbau seiner Routing-Tabellen benutzt.)

F.4.2.1.11 Source-Routing Informationen müssen standardmäßig ignoriert werden.

(B: Ausnutzung der Möglichkeit, in einem IP-Paket den Weg, auf dem das Paket sein Ziel erreichen soll oder den die Antwortpakete nehmen sollen, vorzuschreiben, sodass nicht die durch die Routing-Tabellen angegebenen sicheren Wege benutzt werden.)

neuKap17_f.fm Seite 572 Freitag, 18. Oktober 2002 3:53 15

F.4.3 Organisatorische Maßnahmen

Es müssen sämtliche relevante im IT-Grundschutzhandbuch [6] des BSI beschriebenen Maßnahmen für die eingesetzten Systeme durchgeführt werden (insbesondere natürlich die für Firewall-Systeme beschriebenen), sofern sie nicht einer oben aufgeführten Forderung widersprechen. Besonders wichtig sind:

F.4.3.1 Sicherheitspolitik (Security Policy):

F.4.3.1.1 In der Sicherheitspolitik muss festgelegt werden, welche Anwendungen für welche Benutzer und/oder Rechner zugelassen werden sollen und für welche Anwendungen Vertraulichkeit und/oder Integrität gewährleistet werden müssen.

F.4.3.1.2 Es muss festgelegt werden, welche Ereignisse protokolliert werden und wer die Protokolle auswertet. Die Protokollierung muss den datenschutzrechtlichen Bestimmungen entsprechen.

F.4.3.1.3 Die Benutzer müssen über ihre Rechte und Pflichten umfassend informiert werden.

F.4.3.1.4 Die Sicherheitsvorgaben sollten so beschaffen sein, dass sie auch zukünftigen Anforderungen gerecht werden, d.h., es sollte eine ausreichende Anzahl von Verbindungsmöglichkeiten vorgesehen werden. Jede spätere Änderung muss streng kontrolliert werden und insbesondere auf Seiteneffekte überprüft werden.

F.4.3.1.5 Es ist nötig, Ausnahmeregelungen insbesondere für neue Dienste und kurzzeitige Änderungen (z.B. Tests) festzulegen.

F.4.3.2 Geschlossener Sicherheitsbereich:

F.4.3.2.1 Ein geschlossener Sicherheitsbereich ist für die Komponenten der Firewall erforderlich.

F.4.3.2.2 Es müssen mechanisch stabile Umfassungen (einbruchs- und feuerhemmend) für die beteiligten aktiven Geräte verwendet werden.

F.4.3.2.3 Zutrittskontrolle

F.4.3.3 Administratoren:

Den Administratoren der Firewall und deren Vertretern muss vom Betreiber großes Vertrauen entgegengebracht werden können. Sie haben – in Abhängigkeit vom eingesetzten System – weitgehende und oftmals alle Befugnisse. Sie sind in der Lage, auf gespeicherte Daten zuzugreifen, diese ggf. zu verändern und Berechtigungen so zu vergeben, dass erheblicher Missbrauch möglich ist.

Das eingesetzte Personal muss daher sorgfältig ausgewählt werden. Es muss in regelmäßigen Abständen darüber belehrt werden, dass die Be-

neuKap17_f.fm Seite 573 Freitag, 18. Oktober 2002 3:53 15

fugnisse nur für die erforderlichen Administrationsaufgaben verwendet werden dürfen.

Das in Bundesbehörden eingesetzte Personal für Administrationsaufgaben ist gem. den Vorgaben des Sicherheitsüberprüfungsgesetzes, z. B. für VS-Vertraulich, zu überprüfen.

Bei Administration durch Externe darf nur überprüften Personen unter Beachtung festzulegender erhöhter Sicherheitsmaßnahmen der Zugriff erlaubt werden.

F.4.3.4 Revision:

Die Revision der Sicherheitsmaßnahmen (z. B. der Access-Listen) und Protokolldateien muss durch eine unabhängige Stelle sowohl innerhalb der Behörde wie auch durch Externe unterstützt erfolgen. Dies können z. B. vom Hersteller beauftragte Fachleute sein. Die durchzuführenden Prüfungen sind in einem Prüfkonzept festzulegen, welches sich eng an die erstellten Sicherheitsvorgaben (Security Policy) hält.

F.5 Adressen zu Anhang F

- *BSI-CERT*:
  Bundesamt für Sicherheit in der Informationstechnik, Referat V2,
  Postfach 20 03 63, 53133 Bonn

  Telefon: 02 28/95 82-427, FAX: 02 28/95 82-427

  E-Mail: `CERT@BSI.DE`

- *DFN-CERT*: Universität Hamburg – Fachbereich Informatik,
  Vogt-Kölln-Str. 30, 22527 Hamburg,
  Telefon: 0 40/54 94-22 62, Fax: 0 40/54 94-22 41

EMail:	für Vorfälle und Sicherheitslücken: `DFNCERT@CERT.DFN.DE`
	Anfragen über Mailing-Listen, Workshops: `DFNCERT-REQUEST@CERT.DFN.DE`
Mailing-Listen:	für Diskussionen: `WIN-SEC@CERT.DFN.DE`
	für sicherheitsrelevante Informationen: `WIN-SEC-SSC@CERT.DFN.DE`
URLs:	FTP: `ftp://ftp.cert.dfn.de/pub/security`
	WWW: `http://www.cert.dfn.de/dfncert/dfncert.html`

- *Micro-BIT Virus Center*: EMail: `CERT@RZ.UNI-KARLSRUHE.DE`

  Telefon: 07 21/37 64 22, Fax: 07 21/3 25 50

  CERT Tools and Advisories: FTP: FTP.CERT.ORG

neuKap17_f.fm Seite 574 Freitag, 18. Oktober 2002 3:53 15

- *Firewall-Mailing-Liste*: EMail »*subscribe firewalls*« an `MAJORDOMO@GREATCIRCLE.COM`
- *Risk Forum*: EMail »*subscribe*« an `RISKS-REQUEST@CSL.SRI.COM` oder News-Gruppe `comp.risks`
- *News-Gruppen*: `comp.security.announce`, `comp.security.misc`, `comp.security.unix`, `comp.security.firewalls`, `sci.crypt`.

F.6 Literatur zu Anhang F

[1] Bellovin, S.M., Security Problems in the TCP/IP Protocol Suite, Computer Communication Review, *19,2* (1989)32–48
[2] Morris, R.T. 1985, A Weakness in the 4.2BSD UNIX TCP/IP Software, Computing Science Technical Report, 117, AT&T Bell Laboratories, Murray Hill, New Jersey.
[3] Sandy Murphy, Data Security Letter, 5/94, 8–13
[4] William R. Cheswick, Steven M. Bellovin, Firewalls and Internet Security, Addison Wesley 1994
[5] D. Brent Chapman and Elizabeth D. Zwicky, Building Internet Firewalls, O'Reilly & Associates, Inc. 1995
[6] IT-Grundschutzhandbuch, BSI 7152, Bundesanzeiger-Verlag Köln
[7] Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), hrsg. v.d. Europäischen Union, 1991, ISBN 92-826-3003-X
[8] IT-Sicherheitshandbuch, BSI 7105, Bundesanzeiger-Verlag Köln

neuKap17_g.fm Seite 575 Freitag, 18. Oktober 2002 3:54 15

Anhang G

Glossar, Abkürzungen

Als Nachschlagewerk für den Bereich Informationstechnologie empfiehlt sich das über 3000 Seiten umfassende, regelmäßig aktualisierte Loseblattwerk: »Informationstechnologie von A–Z« aus dem INTEREST-Verlag, siehe: `www.interest.de`

ActiveX

Von Microsoft entwickelte Programmiersprache als Antwort auf →Java und →JavaScript. Der Programmcode (ActiveX Control) wird mit einem ActiveX-fähigen →Browser von einem →Web-Server geladen und auf dem lokalen Rechnersystem ausgeführt.

AES

= Advanced Encryption Standard, neuer Standard für →symmetrische Verschlüsselungsverfahren, →Rijndael-Algorithmus

AOL

= America Online; Onlinedienst und Internet-Provider

AP

= Authentication Process

Applet

In →Java geschriebener Programmcode, der auf dem lokalen Rechnersystem innerhalb einer eigenen Umgebung ausgeführt wird.

Application Gateway

Das Rechnersystem, auf dem ein oder mehrere →Proxies realisiert sind.

ARPA

= Advanced Research Projects Agency

neuKap17_g.fm Seite 576 Freitag, 18. Oktober 2002 3:54 15

ARPANET

= Advanced Research Projects Agency Network; weltweit erstes Datennetz, basierend auf paketorientierter Datenübertragung. Aus dem ARPANET entstand das heutige →Internet.

ASP

= Application Service Provider, stellt outgesourcte IT-Infrastruktur (Hardware, Software, Lizenzen) zur Verfügung.

Asymmetrische Verschlüsselung

auch Public-Key-Verfahren genannt; Verschlüsselungsverfahren, bei dem zwei verschiedene Schlüssel eingesetzt werden. Mit dem einen der beiden Schlüssel werden die Daten oder das Dokument verschlüsselt und/oder signiert, und die Entschlüsselung/Prüfung kann nur mit dem entsprechenden anderen Teilschlüssel erfolgen. Hierzu werden Algorithmen aus der Komplexitätstheorie verwendet.

Asynchroner Transfermodus

Der Asynchrone Transfermodus (ATM) ist ein Datenübertragungsverfahren, das die →Bandbreite erheblich steigern kann. Es ermöglicht das gleichzeitige Übertragen von Daten aus verschiedenen Quellen und kann so die Übertragungskapazitäten optimal ausnutzen. Damit kann eine Bandbreite von bis zu 2,3 GBit erzielt werden.

ATM

= →Asynchroner Transfermodus

Authenticode

Kontrollverfahren für die Anwendung von →ActiveX controls. Ein Programmierer von ActiveX controls hat den Zugriff auf sämtliche Systemressourcen und besitzt damit die gleichen Rechte wie der gerade angemeldete Anwender. Um einen Missbrauch zu verhindern, kann mit der Authenticode-Technologie die Herkunft der verwendeten ActiveX controls durch digitale Signatur nachgewiesen werden.

Authentikation

Authentikation bedeutet die Verifizierung (Überprüfung) der Echtheit bzw. der Identität einer Person oder Sache. Eine Authentikation kann benutzerorientiert (→Benutzerauthentikation) oder rechnerorientiert (anhand der Rechneradresse) durchgeführt werden.

B2B

= Business-to-Business, Applikation, bei der Rechnersysteme unterschiedlicher Firmen untereinander automatisch Geschäftsabläufe abwickeln

Backdoor

= Hintertür; eine versteckte bzw. undokumentierte Programmfunktion, mit deren Hilfe vom Benutzer nicht autorisierte Personen auf dessen Rechnersystem bzw. die darauf gespeicherten Daten zugreifen können (vgl. →Trojanisches Pferd)

Bandbreite

Mit Bandbreite bezeichnet man die Datenmenge, die ein bestimmter Leitungstyp pro Zeiteinheit transportieren kann. Eine analoge Telefonleitung etwa hat eine Bandbreite von ca. 56 KBit, eine ISDN-Leitung schafft 64 KBit, bzw. im Duplex-Betrieb 128 Kbit das Ethernet 10 MBit, das Fast Ethernet 100 MBit. Ein →ATM schließlich erreicht eine Bandbreite von bis zu 2,3 GBit.

Bastion

→Application Gateway, der als einziges Rechnersystem aus dem unsicheren Netz angesprochen werden kann

BDSG

= Bundesdatenschutzgesetz

Benutzerauthentikation

Die →Authentikation ist an den Benutzer gebunden. Dazu exisitieren bei Firewall-Systemen verschiedene Authentikationsmechanismen, z. B.:

- Eingabe von User-ID und Passwort
- S/Key
- Token (Challenge/Response)
- Chipkarten.

Biometrie

Biometrische Authentikationsverfahren benutzen unverwechselbare physikalische Besonderheiten des Anwenders wie Fingerabdruck oder Gesichtscharakteristika zu seiner Authentifizierung.

Blowfish

→symmetrisches Verschlüsselungsverfahren, unterlag dem →Rijndael-Algorithmus beim Wettstreit um den neuen Advanced Encryption Standard (→AES)

neuKap17_g.fm Seite 578 Freitag, 18. Oktober 2002 3:54 15

Browser

Browser nennt man die Software, mit der Internet-Seiten gelesen werden können. Der Browser greift über das HyperText Transfer Protocol (→HTTP) auf Web-Server zu. Dokumente werden im HTML-Format vom Browser interpretiert und dem Benutzer inklusive der Bilddaten dargestellt. Geläufige Browser sind z. B. Netscape Navigator, MS Internet Explorer und Lynx.

Brute Force Attack

Beim →Hacking von kryptographischen Schlüsseln oder Passworten kann man unterschiedlich raffiniert vorgehen. Man kann beispielsweise versuchen, Anhaltspunkte zu finden und auszuwerten. Brute Force (rohe Gewalt) bezeichnet dagegen die primitivste Art des Angriffs: man probiert einfach blindlings alle denkbaren Möglichkeiten durch. Ein solcher Angriff ist heute nicht mehr vielversprechend: Wer per Brute Force Attack einen 128-Bit-Schlüssel ermitteln will, braucht voraussichtlich ein Vielfaches der Lebenszeit unseres Sonnensystems.

BSI

= Bundesamt für Sicherheit in der Informationstechnik, siehe auch: `www.bsi.de`

CA

= Certification Authority; Zertifizierungsstelle, die Benutzerschlüssel als Zertifikat (elektronischer Ausweis) ausgibt. Die Zertifikate dienen zum einen der authentischen Übermittlung von Daten und zum anderen der Identitätsprüfung des Urhebers.

CCITT

= Comité Consultatif International Télégraphique et Téléphonique

CERT

= Computer Emergency Response Team; Aufgabe des CERT ist es unter anderem, als Internet-Feuerwehr schnell und effizient auf kritische Vorfälle (z. B. Hacker-Angriffe, Sicherheitslücken, Viren etc.) zu reagieren und Hilfe zu leisten und Informationen aufzubereiten und bereitzustellen. In Deutschland wird das CERT vom →DFN unterstützt.

CGI

= Common Gateway Interface; Programmschnittstelle zwischen beim Web-Server eingehenden Benutzerdaten (z. B. ausgefüllte Formulare) und angeschlossenen Programmen wie z. B. Datenbanken. Mithilfe von CGI-Skripten kann man Web-Seiten dynamisch gestalten und mit interaktiven Elementen versehen.

Chiffrierfehler

Wenn bei der Anwendung oder Konzeptionierung eines Verschlüsselungsverfahrens Pannen oder Nachlässigkeiten passieren, spricht man von Chiffrierfehlern. Sie haben in der Regel zur Folge, dass die erzeugten Schlüssel weniger komplex sind bzw. aus einer kleineren Menge von Kombinationen hervorgehen, als technisch möglich wäre.

Common Point of Trust

Einziger Übergang zwischen unterschiedlichen Netzen, der als vertrauenswürdig angesehen und mithilfe eines Firewall-Systems realisiert wird.

Content Security

Internet-Dokumente (HTML-Seiten, E-Mails) sind durch Schadensprogramme →Malware gefährdet.

Cookies

Informationen, die der →Web-Server im →Browser des Clients ablegt, beispielsweise eine Kundennummer, über die der Benutzer bei einem Folgebesuch der Website identifiziert werden kann.

Corporate Network

Unternehmen und Behörden bauen mit Knoten, Routern und Multiplexern ihre eigenen Kommunikationsnetze, so genannte »Corporate Networks«, auf.

Cracker

→Hacker, der unbefugt in fremde Computersysteme eindringt und gespeicherte Daten und Programme in böser Absicht manipuliert oder inspiziert: also mit krimineller Energie bzw. für persönlichen Vorteil.

CRL

= Certification Revocation Lists; Schwarze Liste von Zertifikaten (Benutzern), die in einem →TrustCenter geführt wird

Daemon

Ein UNIX-Prozess, der im Hintergrund abläuft und nur bei Bedarf aktiviert wird. Typische Daemons sind z. B. ftpd (→ftp-Daemon) und httpd (→http-Daemon).

DECNET

Von Digital Equipment Corporation (DEC) entwickelte und verwendete Kommunikationsarchitektur für Rechnersysteme

neuKap17_g.fm Seite 580 Freitag, 18. Oktober 2002 3:54 15

Denial of Service

Denial of Service bedeutet soviel wie Funktionsausfall oder Funktionsverweigerung. Dahinter verbirgt sich eine Vielzahl verschiedener Angriffsmöglichkeiten, die alle das Ziel haben, Internetrechner zum Absturz zu bringen oder in bestimmten Funktionen lahm zu legen. Klassische Beispiele sind das Mail-Bombing – das geplante Überlasten eines Mail-Empfängers mit einer Unzahl von E-Mails – oder das Versenden von »Nukes«, das sind IP-Pakete, die ungesicherte Betriebssysteme kurzerhand zum Absturz bringen.

DENIC

= Deutsches Network Information Center; Sitz in Karlsruhe; unter anderem für die Vergabe von →Domain-Namen mit der Endung ».de« zuständig, siehe auch: www.denic.de

DES

= Data Encryption Standard; eines der bekanntesten und am meisten verbreiteten und untersuchten symmetrischen Verschlüsselungsverfahren. Der DES wurde 1976 in den USA normiert (ANSI X3.92). Der DES-Algorithmus hat ursprünglich eine Länge von 64 Bit, wovon 56 signifikant sind. Der DES-Algorithmus wird heute meist als Triple-DES mit 128-Bit →effektiver Schlüssellänge verwendet.

DFN

= Deutsches Forschungsnetz; Der DFN-Verein war am Aufbau des deutschen Wissenschaftsnetzes →WIN beteiligt und unterstützt das →CERT in Deutschland (DFN-CERT).

Diffie-Hellman

Verfahren zum Austausch eines geheimen Schlüssels über öffentliche Netzwerke

Digitale Signatur

Die Digitale Signatur garantiert den Ursprung einer Software, einer Nachricht oder sonstiger Daten. Die Digitale Signatur entspricht also einer eigenhändigen Unterschrift, die den Absender eindeutig identifiziert sowie sicherstellt, dass die empfangenen Daten nicht verfälscht wurden. Technisch basiert die Digitale Signatur auf der →asymmetrischen Verschlüsselung, d.h. dem Public-Key-Verfahren.

Digitales Zertifikat

Wer remote seine Identität nachweisen möchte – etwa durch eine Chipkarte und Eingabe einer PIN –, beruft sich damit auf eine Instanz, die dokumentiert, dass mit dieser Chipkarte und PIN auch genau diese Person verbunden ist. Diese Instanz – Zertifizierungsinstanz bzw. →Certification Authority (CA) – bürgt für die Authentizität des Kartenbesitzers und dokumentiert diese durch ein Zertifikat. Dieses Zertifikat – in digitaler Form – dient Organisationen, die remote access zulassen, als ›Ausweis‹ für den User.

DMZ

= De-Militarised Zone; ein entkoppeltes, isoliertes Teilnetzwerk, das zwischen das zu schützende Netz und das unsichere Netz geschaltet wird

DNS

= Domain Name Service; Internet-Dienst, mit dessen Hilfe die→IP-Adressen der Hosts den entsprechenden →Domainnamen und umgekehrt zugeordnet werden können. So genannte DNS Server verwalten die Datenbanken mit den Adressen.

Domainnamen

Untergliederungseinheit der hierarchisch aufgebauten und weltweit eindeutigen Namen von Rechnersystemen im Internet. Die Domainnamen müssen bei den zugehörigen Verwaltungsstellen (→NIC, →DENIC) beantragt werden.

DSA

= Digital Signatur Algorithm, staatlichen Signaturverfahren in den USA, arbeitet u.a. mit dem Algorithmus →ElGamal

E-Business

= Electronic Business, Abwicklung von Geschäftsvorgängen über elektronische Medien wie das Internet

E-Commerce

= Electronic Commerce; umfasst im Prinzip alle Schritte von Geschäftsprozessen, die auf elektronischem Wege vollzogen werden. Im Mittelpunkt stehen dabei zunächst die Möglichkeiten, sich online über Produktangebote zu informieren und Bestellungen vorzunehmen. Aber auch die Zahlung vom heimischen PC aus – Online Banking – wird bald zum E-Commerce-Alltag gehören. Und bei Zahlungen gilt noch mehr als bei Bestellungen: es muss sichergestellt sein, dass der Auftraggeber eindeutig identifizierbar ist und dass kein Unbefugter in die Transaktionen Einblick erhält.

neuKap17_g.fm Seite 582 Freitag, 18. Oktober 2002 3:54 15

Effektive Schlüssellänge

Werden Verschlüsselungsverfahren mehrfach durchlaufen, kann man nicht einfach die Schlüssellänge multiplizieren. Die Kryptologen haben deshalb den Begriff »effektive Schlüssellänge« eingeführt. Beispiel Triple-DES: Bei dreimaligem Durchlauf mit je 56-Bit Schlüssellänge entspricht die Sicherheit des Verfahrens nicht etwa einer einmaligen Verschlüsselung mit der Schlüssellänge von 3 * 56-Bit = 168 Bit, sondern ist mit 128 effektiver Schlüssellänge geringer.

ElGamal

→asymmetrisches Verschlüsselungsverfahren

E-Mail

Elektronische Post; Austausch von Textnachrichten und Computerdateien über ein Kommunikations-Netzwerk, z. B. lokales Netzwerk oder das →Internet

Ethernet

Das Ethernet wurde ursprünglich von Xerox für die Verknüpfung von Minicomputern im Palo Alto Research Center entwickelt. Inzwischen ist Ethernet eine weit verbreitete Technik zum Vernetzen von Rechnern in einem →LAN.

Extranet

Extranet heißt der Informationsaustausch zwischen →Intranets von Geschäftspartnern via →Internet (→TCP/IP basierend).

Finger

Internet-Dienst zur Ermittlung und zur Verwaltung der Benutzerinformationen eines Rechnersystems. Die dazugehörige Software ist standardmäßig Bestandteil jedes UNIX-Betriebssystems.

FTP

= File Transfer Protocol; Internet-Dienst zur Übertragung von Dateien

Gateway

Mit Gateway bezeichnet man die Verbindung zwischen zwei Netzen oder Teilnetzen, z. B. das »Tor«, durch das Daten aus dem →Internet in ein lokales Netz gelangen. Gateways arbeiten auf Schicht 7 des ISO/OSI-Modells und können zwei oder mehr Netze mit völlig verschiedenen Protokollen verbinden. Für die Informationssicherheit ist das Gateway der neuralgische Punkt – hier installiert man eine →Firewall, um aus dem Gateway ein →»Secure Gateway« zu machen.

neuKap17_g.fm Seite 583 Freitag, 18. Oktober 2002 3:54 15

GDD

= Gesellschaft für Datenschutz und Datensicherheit

Gopher

Internet-Dienst, der Textinformationen in Form von hierarchisch verschachtelten Auswahlmenüs strukturiert.

GSM

= Global System for Mobile Communications; Standard für digitale Mobilfunknetze

Hacker

Als Hacker werden allgemein Anwender bezeichnet, die sehr vielfältige Kenntnisse im Umgang mit der Computertechnologie und Computerprogrammierung besitzen und sich oft damit beschäftigen. Der Begriff wird auch häufig für Personen verwendet, die sich unbefugten Zugang zu fremden Computersystemen verschaffen. Das Hacking sollte man aber keinesfalls mit Computersabotage, Computerspionage oder Computerbetrug gleichsetzen. Viele Hacker arbeiten aus sportlichen oder wissenschaftlichen Motiven und machen ihre Erkenntnisse der Öffentlichkeit zugänglich, was der Entwicklung von Sicherheitsmechanismen zugute kommen kann. Im Gegensatz zum →Cracker »arbeiten« Hacker also ohne kriminelle Energie bzw. nicht für persönlichen Vorteil.

Hacking

→Hacker

HMAC

Algorithmus, der eine →One-Way-Hashfunktion mit Verschlüsselung kombiniert und so eine Digitale Signatur eines Dokumentes erzeugt.

HTML

= HyperText Markup Language; Seitenbeschreibungssprache, mit der Elemente (Texte, Grafiken, →Hyperlinks, etc.) der Web-Seiten einfach formatiert werden können. HTML ist das derzeit wichtigste im WWW verwendete Dateiformat.

HTTP

= HyperText Transfer Protocol; Internet-Dienst, mit dem Daten zwischen →Web-Server und →Web-Browser ausgetauscht werden.

neuKap17_g.fm Seite 584 Freitag, 18. Oktober 2002 3:54 15

Human Firewall

Initiative des »Human Firewall Council«, eines in den USA gegründeten Konsortiums von Sicherheitsexperten aus Politik, Wirtschaftsunternehmen und gemeinnützigen Organisationen, die das Ziel verfolgt, das Sicherheitsbewusstsein jedes einzelnen Benutzers und eine darauf ausgerichtete IT-Sicherheitspolitik als Wirkungsgrundlage technischer Schutzmaßnahmen zu fördern; nähere Informationen unter `www.humanfirewall.org`

Hyperlink

Ein mithilfe von →HTML markierter Querverweis in einer Web-Seite auf eine Informationsquelle (→URL) im World Wide Web. Durch Aktivierung eines Hyperlinks z. B. per Mausklick wird der Benutzer zu dieser Quelle geführt, wobei er von →Web-Server zu Web-Server geleitet werden kann.

ICMP

= Internet Control Message Protocol; Ein Internet-Protokoll der Netzwerkschicht, welches eine Fehlerkorrektur und andere Informationen liefert, die für die IP-Paketverarbeitung von Bedeutung sind.

IDEA

= International Data Encryption Algorithm; 1990 von Lai und Massey als Alternative zum →DES vorgestelltes →symmetrisches Verschlüsselungsverfahren mit 128 Bit Schlüssellänge

IKE

= Internet-Key-Exchange, Verfahren zum Austausch von Schlüsseln, Standardverfahren für →IPSec

Internet

Das Internet ist ein weltweites, dezentrales Rechnernetz, das auf dem →TCP/IP-Protokoll basiert. Das Internet ist inzwischen das populärste Netz der Welt mit über 300 Millionen Anwendern (Stand: 12/2000). Es bietet seinen Benutzern zahlreiche Dienste an, wie z. B. →FTP, →E-Mail, →World Wide Web, →Gopher.

Intranet

Internes Netz einer Organisation oder eines Unternehmens, das auf der Internet-Technologie und dem →TCP/IP-Protokoll basiert.

neuKap17_g.fm Seite 585 Freitag, 18. Oktober 2002 3:54 15

IP

= Internet Protocol; Dieses Netzwerkprotokoll definiert den Aufbau und die Adressierung von Datenpaketen in TCP/IP-Netzwerken.

IP-Adresse

Weltweit eindeutige Adresse eines am Internet angeschlossenen Rechnersystems. Die IP-Adresse besteht aus einem Zahlencode von vier Zahlen von 0 bis 255 (z.B. 192.168.1.2). Die Vergabe erfolgt international vom →NIC bzw. in Deutschland vom →DENIC.

IP Spoofing

Das Einfügen einer falschen IP-Absenderadresse in eine Internet-Übertragung. Das Ziel dieser Aktion ist der unberechtigte Zugriff auf ein Computersystem.

IPRA

= Internet Policy Registration Authority

IPSec

Verfahren zur Erweiterung der normalen →IP-Pakete um →Authentikation und Verschlüsselung, zukünftiger Standard

IPv6

= Internet Protocol Version 6; erweiterte Version des Internet-Protokolls mit vergrößertem Adressraum sowie Funktionen für Sicherheit

IPX

= **I**nternetwork **P**acket E**x**change; von Novell verwendetes Netzwerkprotokoll. Im Schichtenmodell (→OSI-Modell) ist IPX auf der gleichen Ebene wie das IP einzuordnen.

ISDN

= Integrated Services Digital Network; weltweites digitales Kommunikationsnetzwerk zur integrierten Übertragung von Sprache und Daten.

ISO

= International Organization for Standardization; internationale Vereinigung, in der jedes Mitgliedsland durch die führende Standardisierungsorganisation vertreten ist. Die ISO arbeitet an der weltweiten Vereinheitlichung technischer Standards, u.a. auf den Gebieten der Kommunikation und des Informationsaustausches. Hier ist an erster Stelle das weithin akzeptierte →OSI-Modell zu nennen.

neuKap17_g.fm Seite 586 Freitag, 18. Oktober 2002 3:54 15

ISS

= Internet Security Systems; amerikanischer Hersteller des Firewall-, Intranet- und Web-Security-Scanners. Die Scanner testen Rechnersysteme auf Schwachstellen, indem sie bekannt gewordene Internet-Angriffe ausführen.

IT

= Information Technology

ITSEC

= Information Technology Security Evaluation Criteria; von Frankreich, Deutschland, Großbritannien und den Niederlanden festgelegte Kriterien für die Zertifizierung von IT-Systemen

Java

Von Sun Microsystems entwickelte plattformunabhängige Programmiersprache für das Internet. Java-Programme (→Applets) werden von einem →Web-Server auf das lokale Rechnersystem übertragen und dort von einem Java-Interpreter ausgeführt.

Java-Applet

→Applet

JavaScript

Von Netscape definierte und in die HTML-Syntax integrierte Skriptsprache. JavaScript-fähige →Web-Browser interpretieren den in einer Web-Seite enthaltenen Programmcode und führen ihn aus.

Kompromittierung

Kompromittierung ist ein allgemeiner Oberbegriff für alle Formen der Vertraulichkeitsverletzung.

Kryptoanalyse

Ziel der Kryptoanalyse ist die Entschlüsselung von Geheimschriften und Codes. Im Bereich des elektronischen Datenverkehrs kann man Kryptoanalyse als eine Form von →Hacking bezeichnen.

neuKap17_g.fm Seite 587 Freitag, 18. Oktober 2002 3:54 15

Kryptogesetz

Das so genannte Kryptogesetz definiert, unter welchen Bedingungen ein kryptographisches Verfahren zur →Verschlüsselung und Signatur von →E-Mails als so sicher gilt, dass der so übermittelte Inhalt rechtsverbindlichen Charakter hat wie ein Dokument auf Papier. Das deutsche Gesetz hierzu hat Pioniercharakter.

Kryptographie

Kryptographie ist der Zweig der →Kryptologie, der sich gezielt mit der Entwicklung von Verschlüsselungs- und Codierungsverfahren befasst. Diese Wissenschaft ist sehr alt – schon im alten Ägypten beschäftigte man sich mit Geheimschriften. Heute geht es dagegen vorwiegend um mathematische Verschlüsselungsverfahren für den elektronischen Datenverkehr. Auch die →Digitale Signatur beruht auf kryptographischen Verfahren.

Kryptographischer Algorithmus

Jedes kryptographische Verfahren beruht darauf, einen verständlichen Text nach bestimmten Regeln in unverständlichen Zeichensalat zu verwandeln. Bei elektronischer Verschlüsselung geschieht dies nach einem bestimmten Algorithmus, wobei die Länge des Algorithmus beeinflusst, wie schwer →Hacker den Text entschlüsseln können. Zurzeit gelten Schlüssellängen von 128 Bit als sicher.

Kryptographisches Protokoll

Die auf Algorithmen basierenden Verschlüsselungsverfahren müssen in die technologischen Gegebenheiten der Datenkommunikationsstrukturen eingebunden werden – dafür sorgt ein kryptographisches Protokoll.

Kryptologie

Oberbegriff für →Kryptographie und →Kryptoanalyse

Kryptoregulierung

Kryptoregulierung ist der staatliche Versuch, die Verbreitung und Verwendung leistungsfähiger Verschlüsselungsverfahren einzuschränken. Grund: Die Behörden fürchten, dass zu raffinierte Verfahren die Möglichkeiten zur Verbrechensbekämpfung beschneiden könnten. Die USA leiden unter sehr strikter Kryptoregulierung; in Deutschland konnte ein solches Gesetz verhindert werden.

LAN

= Local Area Network – auf deutsch auch: lokales Netz. Darunter fallen Netzwerke, die einen relativ kleinen, abgegrenzten Bereich umfassen – im Gegensatz zum →WAN.

neuKap17_g.fm Seite 588 Freitag, 18. Oktober 2002 3:54 15

LDAP

= Lightweight Directory Access Protocol, Protokoll zum Zugriff auf →Verzeichnis-Dienste

M-Business

= Mobile Business, Abwicklung geschäftlicher Vorgänge über Mobiltelefone

M-Commerce

= Mobile Commerce, Handel über elektronische Medien (Internet) unter Einbeziehung von Mobiltetefonen

MAC

= Media Access Control; Protokoll der Netzzugangsebene

oder

= Message Authentication Code; →One-Way-Hashfunktion

Mailbombe

die unerwünschte Zusendung einer großen Menge von E-Mails (oder einer einzelnen sehr großen E-Mail) an einen bestimmten Empfänger oder eine Gruppe von Empfängern mit dem Ziel, den empfangenden Mailserver (bzw. ein Postfach) zu blockieren

Mailbox

elektronischer Briefkasten; Rechnersystem, das per →Modem angewählt wird und auf dem ein Programm läuft, das dem Benutzer erlaubt, Nachrichten anderer Benutzer zu lesen oder ihnen zu schreiben. Meist besteht zusätzlich die Möglichkeit, Dateien herunter- oder heraufzuladen. (siehe auch →E-Mail)

MailTrusT

Ein →TeleTrusT Projekt, in dem die Interoperabilität vielfältiger technologischer Komponenten und Produkte, die die Anwendung der →Digitalen Signatur ermöglichen, durch kompatible Ausführung von Verschlüsselung und gemeinsamer Schnittstelle erreicht wurde.

Malware

Eine besondere Gefahr beim Austausch von Dateien als Anhänge von Mails oder WWW-Dokumenten, ist die Gefahr, dass neben der eigentlichen Information (Daten, Programme) so genannte Malware (Viren, Würmer, Trojanische Pferde, ...) mitgesendet wird, die im Prinzip immer den Empfänger Schaden soll.

neuKap17_g.fm Seite 589 Freitag, 18. Oktober 2002 3:54 15

MAZ

Größter deutscher Internet-Provider, Sitz in Hamburg

MD4/MD5

Von Rivest entwickelte →One-Way-Hashfunktionen zur Unterstützung von Authentikationsverfahren

Mime

= Multipurpose Internet Mail Standard. Standard zum Verschicken von Multimediadateien bei E-Mails

Modem

= **Mo**dulator/**Dem**odulator; Ein Gerät, das den Austausch von Daten über Drahtleitungen ermöglicht. Die klassische Verwendung nutzt die konventionelle Telefonleitung, um sich ans →Internet anzuschließen und →E-Mails zu verschicken. Es gibt aber auch Modems für ISDN-Leitungen, Fernsehkabel, Stromleitungen, Standleitungen usw.

Modulation

Manche Datenleitungen, etwa die analoge Telefonleitung, werden durch einen ständigen Stromfluss aufrechterhalten – das so genannte Trägersignal. Die eigentliche Informationsübermittlung geschieht durch geringfügige Schwankungen oder sonstige Veränderungen, also durch Modulation des Trägersignals.

MTA

= Message Transport Agent; Programm, das für die Annahme und Weiterleitung von →E-Mails verantwortlich ist

Multiplexverfahren

Technik, die es ermöglicht, mehrere separate Signale über eine einzelne Leitung zu übertragen

Nameserver

→DNS

neuKap17_g.fm Seite 590 Freitag, 18. Oktober 2002 3:54 15

NCSA

= National Computer Security Association; Verein von Anwendern und Hard- und Software-Herstellern mit dem Ziel, Benutzern bei der Erhöhung der Sicherheit, der Wahrung der Integrität ihrer Informationen und der Reduzierung der Bedrohungen durch Computer-Viren zu unterstützen. NCSA entwickelte Kriterien für die Zertifizierung von Firewall-Systemen.

Netz

Netz oder Netzwerk nennt man eine Gruppe von Computern und angeschlossenen Geräten, die durch Kommunikationseinrichtungen miteinander verbunden sind. Die Netzwerkverbindungen können permanent (z. B. über ein Kabel) oder zeitweilig (etwa über das Telefon oder andere Kommunikationsverbindungen) eingerichtet werden und verschiedene Größenordnungen und Ausdehnungen haben.

NMS

= Network Management System

NNTP

= Network News Transport Protocol; Internet-Dienst, mit dem die News-Artikel transportiert werden

One-Way-Hashfunktion

Auf eine Nachricht, deren Länge variabel ist, wird eine so genannte One-Way-Hashfunktion angewendet, die eine kryptographische Prüfsumme fester Länge als Ergebnis erzeugt (z. B. →MD5).

OSI

= Open Systems Interconnection

OSI-Schichtenmodell

auch OSI-Referenzmodell genannt; ein von der →ISO entwickeltes Kommunikationsprotokoll, das allgemeine Regeln für die Kommunikation in Netzwerken enthält

OTP

= One-Time-Password (Einmal-Passwort); das Konzept »Einmal-Passwort« legt fest, dass ein Passwort nur einmal für eine Authentikation verwendet werden darf.

Passwort

Das einfachste Authentikationsverfahren ist das Passwort-Verfahren. Die Stärke dieses Verfahrens beruht allerdings lediglich auf der Geheimhaltung und der Qualität (Länge/Nichttrivialität) des Passwortes.

PEM

= Privacy Enhanced Mail; in den →RFCs 1421-1424 festgelegter Standard für die Verschlüsselung und Authentizität von →E-Mails

PGP

= Pretty Good Privacy; ein von Phil Zimmerman entwickeltes Verschlüsselungsverfahren, welches auf →RSA und →IDEA basiert.

Phreaker

Personen, die in Telefonleitungen, Anrufbeantwortern und →Voiceboxen ihr Unwesen treiben.

PIN

= Personal Identification Number; eine Codenummer, die einem berechtigtem Benutzer zugewiesen ist

PKI

= Public Key Infrastructure, Infrastruktur zur Erstellung und Verwaltung von Schlüsselpaaren und →Zertifikaten

POP3

= Post Office Protocol; Standard zur Übermittlung von →E-Mails

PPP

= Point to Point Protocol; wird zum Austausch von Datenpaketen per →Modem im →Internet verwendet. Das PPP liegt eine Ebene unter →TCP/IP und kümmert sich nur um die serielle Datenübertragung und ihren Aufbau.

Private-Key-Verfahren

→Symmetrisches Verschlüsselungsverfahren

neuKap17_g.fm Seite 592 Freitag, 18. Oktober 2002 3:54 15

Proxy

Ein Proxy ist ein Stellvertreter des →Servers gegenüber dem Client und ein Stellvertreter des Client gegenüber dem Server. Nach der →Authentikation des Clients bzw. des Servers gegenüber dem Proxy arbeitet dieser für beide Seiten transparent. Proxies existieren für die Dienste →HTTP, →SMTP, →FTP, →Telnet u.a.

Public-Key-Verfahren

→Asymmetrisches Verschlüsselungsverfahren

RC4 / RC5

→Symmetrische Verschlüsselungsverfahren

Registration Authority (RA)

= Registration Authority; Bestandteil einer →PKI, untergeordnete Institution, die einen Teil der Routineaufgaben einer →CA übernimmt

Remote access

Mit Remote access wird die Möglichkeit bezeichnet, aus räumlicher Distanz über ein öffentliches Netz Zugang zu einem Rechnersystem oder lokalem Netz zu erhalten und dort agieren zu können. Da Remote access-Verbindungen von Natur aus ein besonders großes Risiko bedeuten, müssen Sicherheitsvorkehrungen getroffen werden, um Authentizität und Vertraulichkeit zu garantieren. Mit Verschlüsselungs- und Zugangskontrollsystemen kann Remote Access gesichert werden.

RFC

= Request for Comment; Textdokumente, die Vorschläge für neue Internet-Standards zusammenfassen

Rijndael

→symmetrisches Verschlüsselungsverfahren mit einer für die nächsten Jahrzehnte ausreichenden Schlüssellänge, soll das weit verbreitete →DES ablösen

RIP

= Routing Information Protocol; →Router

Router

Router sind Geräte zur Kopplung verschiedener Netze. Sie leiten Datenpakete auf der günstigsten Route »durch das Gewirr der Netzwerke« zu ihrem Ziel. Dabei arbeiten sie meistens auf Schicht 3 des ISO/OSI-Referenzmodells.

RSA

→Asymmetrisches Verschlüsselungsverfahren, benannt nach den Entwicklern Rivest, Shamir und Adleman. Das bekannteste, bewährteste und am besten untersuchte asymmetrische Verfahren.

SATAN

= System Administrator Tool for Analyzing Networks; ein Programm zur Überprüfung von IP-Netzwerken. Getestet werden dabei Schwachstellen, die ein Angreifer über das Internet ausnutzen kann, um sich unbefugt Zugang zu einem Rechnersystem zu verschaffen.

Secure Gateway

→Gateway nennt man den Zugang, der ein lokales Netz mit einem öffentlichen Netz verbindet. Wenn der Betreiber des lokalen Netzes kontrollieren will, wer wann unter welchen Bedingungen Zugang zu welchen Diensten erhalten soll, richtet er durch Sicherheitsmaßnahmen einen Secure Gateway ein. Ein Secure Gateway muss v.a. in der Lage sein, die Authentizität von Besuchern zu überprüfen und entsprechende Zugangsrechte zu differenzieren. Größtmögliche Sicherheit bietet hier ein High-level-Firewall-System.

Security Policy

Eine wohldurchdachte Security Policy bildet die Grundlage für die Sicherheit in Organisationen. Dazu zählen die Definition von Sicherheitszielen, die Bestimmung des Schutzbedarfs der Daten, die Analyse der Kommunikationsstrukturen und anderes mehr. Erst auf dieser Basis können konkrete Sicherheitsmaßnahmen geplant und durchgeführt werden.

Security Token

Ein Security Token ist ein Datenträger (z. B. Chipkarte oder Diskette), mit dem der User seine Zugangsberechtigung nachweisen kann, wenn er die richtige →PIN kennt. Die →Authentikation funktioniert nach dem Challenge-Response-Prinzip: Das Firewall-System, das den Zugriff gewähren kann, stellt eine Challenge, auf die der Security Token eine Response schickt und damit den User authentifiziert.

Server

Ein Server ist ein Rechner innerhalb eines lokalen Netzes, der den anderen Rechnern seines Netzes Informationen zur Verfügung stellt.

neuKap17_g.fm Seite 594 Freitag, 18. Oktober 2002 3:54 15

SET

= Secure Electronic Transaction, Protokoll aus dem Bereich des →E-Commerce, erlaubt das Bezahlen von Waren und Dienstleistungen über das Internet

SHA

= Secure Hash Algorithm, oft auch SHA-1 genannt, →One-Way-Hashfunktion

S-HTTP

= Secure HTTP; um Kryptographiefunktionen erweiterte Version des Protokolls →HTTP

SKIP

= Simple Key Management for Internet Protocols, Protokoll zum Schlüsselaustausch, wird beim Einsatz von →IPSec wahlweise anstelle des üblichen →IKE verwendet

S/MIME

= Secure Multipurpose Internet Mail **S**tandard

um Mechanismen zur Authetication, Verschlüsselung und Signatur erweiterter →MIME Standard

SMIB

= Security Management Information Base

SMTP

= Simple Mail Transport Protocol; Internet-Dienst zur Übertragung von →EMails.

SNA

= Systems Network Architecture; von IBM entwickelte und verwendete Kommunikationsarchitektur für Rechnersysteme

SSL

= Secure Socket Layer; Protokollschicht zum sicheren Transport von höheren Internetprotokollen wie →HTTP

Symmetrische Verschlüsselung

auch Private-Key-Verfahren genannt; Verschlüsselungsverfahren, bei dem für die Verschlüsselung der Daten der gleiche Schlüssel verwendet wird wie für ihre Entschlüsselung. Die bekanntesten symmetrischen Verschlüsselungsverfahren sind →DES und →IDEA.

TCP

= Transmission Control Protocol; das Protokoll innerhalb des →TCP/IP, das die Trennung der Datennachrichten in Pakete steuert und die empfangsseitige Zusammensetzung und Überprüfung auf Vollständigkeit der Datenpakete überwacht.

TCP/IP

= Transmission Control Protocol/Internet Protocol; Kommunikations-Architektur im Internet/Intranet. →TCP, →IP

TeleTrusT e.V.

TeleTrusT e.V. – siehe: `www.teletrust.de` – wurde 1989 gegründet, und hat sich die Förderung von Wissenschaft, Normung und Bildung im Bereich der Entwicklung einer verlässlichen Informations- und Kommunikationstechnik zum Ziel gesetzt. Im TeleTrusT arbeiten Forschung, Anbieter, Organisationen und Behörden zusammen. Der TeleTrusT war an der Formulierung des deutschen Signaturgesetzes beratend mitbeteiligt.

Trojanisches Pferd

ein unverdächtig erscheinendes Programm, das im Hintergrund vor dem Benutzer verborgene und von diesem unerwünschte Funktionen ausführt, z. B. eine →Backdoor öffnet, gespeicherte Daten verändert oder vertrauliche Informationen sammelt und an einen Server schickt.

Die Bezeichnung »Trojanisches Pferd« geht auf Homers Odyssee zurück: Nachdem die Griechen Troja lange erfolglos belagert hatten, ließen sie ein hölzernes Pferd vor den Stadtmauern zurück, in dem sich ihre tapfersten Soldaten versteckten. Die Trojaner holten das Pferd in die Stadt, in der Nacht öffneten die versteckten Krieger ihren Mitstreitern die Tore und Troja wurde verwüstet.

TrustCenter

→CA

neuKap17_g.fm Seite 596 Freitag, 18. Oktober 2002 3:54 15

UDP

= User Datagram Protocol; ein verbindungsloses Übertragungsprotokoll für das Internet. Im Gegensatz zum →TCP/IP findet bei diesem Protokoll keine Überprüfung der ordnungsgemäßen Zustellung von Datennachrichten statt.

URL

= Uniform Resource Locator; ein URL bezeichnet die eindeutige Adresse eines Internet-Servers bzw. einer bestimmten Information darauf. Er beinhaltet Angaben wie Typ der Ressource, mit der verbunden werden soll (z. B. →WWW, →FTP, →Gopher), Serveradresse, Portnummer, etc. Ein URL wird im →Browser eingegeben oder durch einen →Hyperlink aktiviert.

USV

= unterbrechungsfreie Stromversorgung; wird an hochverfügbaren Rechnersystemen eingesetzt, um den Ausfall der Stromversorgung zu überbrücken oder die Stromversorgung solange zu gewährleisten, bis die Rechnersysteme kontrolliert heruntergefahren worden sind

Verschlüsselung

Informationen werden verschlüsselt, um sie gegen unberechtigte Einblicke oder Verwendung zu schützen. Verschlüsselungsverfahren beruhen auf komplexen mathematischen Berechnungen (Algorithmen), wobei die Länge der Schlüssel und die Qualität des Algorithmus maßgeblich für die Sicherheit sind.

Verzeichnis-Dienst

Bestandteil einer →PKI, enthält frei definierbare Datenstrukturen und ein Protokoll zum Zugriff darauf

Viren

Programme, die sich selbst unbemerkt in andere Programme kopieren und zu einem definierten Zeitpunkt meist zerstörerische Aktivitäten ausführen.

Voicebox

Rechnersystem für Teilnehmer in Mobilfunknetzen, das wie ein Anrufbeantworter Nachrichten aufzeichnet

VPN

= Virtual Private Network; logisches Netz innerhalb eines konventionellen Netzes, in dem nur verschlüsselte Verbindungen zwischen einzelnen Rechnersystemen oder Teilnetzen zugelassen werden. Durch die Verschlüsselung geschieht die Kommunikation über das öffentliche Netz vertraulich, sodass die Verbindung quasi privat (virtual private) stattfindet.

W3C

= World Wide Web Consortium; Organisation zur Koordinierung der weiteren Entwicklung des →WWW durch Erarbeitung von Spezifikationen und Referenz-Software.

WAN

= Wide Area Network. Darunter versteht man offene, weiträumige Netze – z. B. ISDN, X.25.

WAP

= Wireless Application Protocol, »Netzwerkstack« für Mobiltelefone

Web-Server

Rechnersystem, das den auf →HTTP basierenden Internet-Dienst →WWW zur Verfügung stellt

WIN

= **Wi**ssenschafts**n**etz; mithilfe des →DFN aufgebautes Datennetz, das alle wichtigen Universitäten und Forschungseinrichtungen Deutschlands miteinander verbindet

WTLS

= Wireless Transport Layer Security, Ebene innerhalb des →WAP-Stacks, nimmt Sicherungsfunktionen wahr, an das Netzwerkprotokoll →SSL angelehnt

Würmer

Programmcodes, die sich – ähnlich wie Viren – selbsttätig in Netzwerken verbreiten; im Unterschied zu Viren integrieren Würmer sich jedoch nicht in andere Programme oder Dateien

WWW

= World Wide Web; die komplette Sammlung von Hypertext-Dokumenten, die auf HTTP-Servern weltweit abgelegt sind

neuKap17_g.fm Seite 598 Freitag, 18. Oktober 2002 3:54 15

X.400

OSI-Standard für E-Mail-Systeme

X.500

OSI-Standard für Benutzerverzeichnisse

X.509

Weit verbreiteter Standard für →Zertifikate

Zertifikat

Datenstruktur, die eine Identifikation des Besitzers, seinen öffentlichen Schlüssel, ein Ablaufdatum und die Digitale Signatur einer →Certification Authority enthält

fw5SIX.fm Seite 599 Freitag, 18. Oktober 2002 4:51 16

Stichwortverzeichnis

A

Abhören der Teilnehmer-Identitäten 83
Abhören von Daten 82
Abschottung von Organisationseinheiten 306
Abschreckungswirkung 370
ACK-Bit 127
Active Server Pages 379
ActiveX 376, 385
ActiveX-Controls 77
Adaptive Proxy 179
adaptive screening 143
AH 538
Aktive Angriffe 85
aktive Elemente 77
Aktive Firewall-Elemente 116
Aktivierung der Chipkarte 227
Alarmierung 48, 371
Alibi-Funktion 295
Analogien 43
Analysemodul 117, 470
Angreifer 34
Angriffe auf das Firewall-System 473
Angriffe aus dem Netz 462
Angriffsrisiko 92
Anomalien 437
Anschaffung 396
Anschaffungskosten 388
Anwendungsebene 57, 457
Applet-Filter 160
Application Gateway 144, 187
Application Level Proxies 147
Architektur 116
Architekturentwurf 400
ARPA 51
ARPANET 51
ASP 379
asymmetrisches Verschlüsselungsverfahren 215
Audit 154
Auditor 182
Audit-Rechner 424
Audit-Tools 427
Aufrechterhaltung des Betriebs 389
Ausspähen von Daten 521
Auswertungskonzepte 439
Authentication Header 540
Authentication Process 135
Authentication Proxy 165
Authenticode-Technologie 386
Authentikation 271
Authentikationsmechanismus 118
Authentikationsmodul 117
Authentikationsverfahren 271
Authentizität 36

B

Bastion 144
Bedrohung 32
Beeinträchtigung der Aufgabenerfüllung 94
Benutzerfreundlichkeit 181, 403
benutzerorientierte Application Level Proxies 150
benutzerorientierter Packet Filter 134
Beschaffungsphase 387
besondere Zweckbindung 375
Betriebsdokumentation 402
Betriebssicherungsmechanismen 118
Betriebssystem-Plattform 292
Betriebsumgebung 402
Beweissicherung 372
Beweissicherung der Handlungen von Benutzern 370
block if full 138

fw5SIX.fm Seite 600 Freitag, 18. Oktober 2002 4:51 16

Boykott des Kommunikationssystems (Denial of Service) 87
Brandschutzmauer 43
Browser 75
BSI 559

C
Certification Authority 262
CGI 377
Challenge-Response-Verfahren 274
Chancen 36
Chipkarte (SmartCard) 226
Circuit Level Proxies 166
Client Server 32
Codebits 71
Common Gateway Interface 377
Common Point of Trust 47, 299
Computerdelikte 513
Computerkriminalität 31, 34, 93, 513
Computermanipulationen 514
Content Security 160
Cookies 78
Cracker 31

D
Data Encryption Standard 214
Datei-Filter 158
Daten-Filter 160
Datengeheimnis 375
Datenschutzaspekte 375
DECNET-Protokolle 123
Definition eines Firewall-Elements 468
De-Militarised Zone 195
DENIC 60
DES-Algorithmus 214
Designkonzept 118
Destination Unreachable 65
Dienste-Check-Liste 342
Digitale Signatur 235
Digitaler Zeitstempel 232
DMZ 195
DNS 72
DNS Proxy 212
DNS Server 212
DNS-Konzepte 211
Domain Name Service 72
Domainnamen 60, 364
Down-Sizing 32
Dual-homed Application Gateway 189
dynamischer Packet Filter 133

E
Echo Request 66
EchoReply 65
Editor 182
Eignung 402
Einbindungs- und Durchsetzungsmodul 470
Einbindungsmodul 116
Einfügen und Löschen bestimmter Daten 86
Einmal-Passwort 274
Einsatzfall 206
Einsatzumgebung 488
Eintrittswahrscheinlichkeit 92
Einwohnermeldeämter 219
elektronische Brandschutzmauer 43
elektronische Post (E-Mail) 52
elektronischer Pförtner 43
elektronisches Äquivalent 45, 235
E-Mail 28
E-Mail-Anwendung 213
E-Mail Security 229
Encapsulated Security Payload 542
Encapsulation 538
Entkopplung von Diensten 48
Entscheidungsmodul 117
Entwicklungsumgebung 401
Erkennung von Sicherheitsverletzungen 369
Erpressung 514
ESP 542
ESP-Header 542
Ethernet-Pakete 123
Evaluationsstufe 411
Evaluierung 396
Exportbeschränkung 295
externe Anbindung 307
externe Benutzer 343
externe Zugänge 346

F
Fehlbedienung 90
Fehlrouting von Informationen 89
Feinentwurf 400
Fernmeldegeheimnis 90
Finanzielle Auswirkungen 95
finger 97, 467
Firewall-Bedürfnisse 291
Firewall-Beschaffung 387
Firewall-Einsatz 346
Firewall-Elemente 115
Firewall-Hersteller 559
Firewall-Konzepte 185

fw5SIX.fm Seite 601 Freitag, 18. Oktober 2002 4:51 16

Firewall-Lösungen 287
Firewall-Plattform 292
Firewall-Produkte 287, 288
Firewall-Schutzmodul 117
Firewall-Sicherheitspolitik 339, 355
Firewall-Software 291
Firewall-Systeme 43
Free-Run-Modus 138
FTP 29, 73
  aktive Methode 128
  passive Methode 129
FTP Proxy 157
FTP-Verbindungsaufbau 127

G
Gefahren aus dem Internet 30
generic Top Level Domains 60
generische Proxies 166
geschachtelte Firewall-Konstellationen 365
geschützte Leitungsführung 345
GIK 537
Global Authentication 165
globale Ausdehnung 33
Grenzen 354
Grenznetz 195
Group Interchange Key 537
Grundgesetz 517
gTLD 60

H
Hacker 31, 515
Hacker-Gemeinde 96
Hacking 514
Hardwarefehler durch Umwelteinflüsse 89
High-level-Security-Firewall-System 197
Hintertüren 354
HTML (Hyper Text Markup Language) 75
HTTP 75, 77
HTTP-Proxy 159
hybride Verschlüsselungstechnik 217

I
ICMP 64
ICMP-Angriffe 109
ICSA-Kriterien 397, 412
ICSA-Zertifizierung 411
Idee eines Angriffes 96
Identifikation 271
IDS 431
illegale IP-Adressen 363
Inbetriebnahme 388
Industriespionage 527
Infrastruktur 345
infrastrukturelle Sicherheitsmaßnahmen 391
Installationsphase 388
Integrität 33, 35
Integritätstest 117
interne Angriffe 355
interne Benutzer 343
Internet 32
Internet-Adressen 58
Internet-Polizei 30
Internet-Routing-Angriffe 112
Internet Firewalls 559
Internet Server 200, 301
Internet-Technologie 297
Intranet 32, 297
Intranet-Anwendung 297
Intranet Security 303
Intranet Server 203
Intrusion Detection/Response-Systeme 113, 430
Intrusion-Response 431
IP 538
IP-Adressen 361
IP-Adressen-Spoofing 108
IP-Authentication Header 540
IP-Forwarding 291
IP-Maskerade 99
IP-Optionen 63
IP-Protokoll 61
IPSec 539
IPv4 59, 538
IPv6 59, 538
isoliertes Teilnetzwerk 195
ISS 98, 468
ITSEC-Kriterien 397
ITSEC-Zertifizierung 398
IT-Sicherheit 33
IT-Sicherheitskriterien 398

J
Java 376, 380
Java-Applets 77
JavaScript 376, 384
JavaScript-Befehle 77

fw5SIX.fm Seite 602 Freitag, 18. Oktober 2002 4:51 16

K
KES/Utimaco-Studien 112
Kommando-Filter 157, 160
Kommunikationsanforderungen 341
Kommunikationsprofile 343
Kommunikationsprotokolle 61
Konfigurationsfehler 98, 468
Kontrolle auf der Anwendungsebene 48
Kontrolle der Protokolldaten 347
Konzeptionsfehler 561
Kosten 392
Kosten im Jahr 392
Kosten pro Benutzer 392
Kreditkartenbetrug 524
Kriminalitätsprophylaxe 518
Kriminalitätsstatistik 522
kryptographische Prüfsumme 217

L
Linux 289
Logbuch 118, 153, 369

M
Mail 91
Mail Proxy 148
Mail-Konzept 209
MailTrusT 244
Malware 313
Malware-Filter 161
Mechanismen 33
Mechanismenstärke 407
Message Transfer Agent (MTA) 74, 148
Minimale Software 118
Modem-Anschlüsse 311
Modem-Verbindungen 312
Modifikation von Daten 86

N
n:1 Port-Relay 167
n:m Port-Relays 168
nachweisbare Sicherheit 295
Need-to-know-Prinzip 347
negative Außenwirkung 95
negativer Filterregeln 130
Network Address Translation 361
Network Information Center (NIC) 361
Network News Transfer Protocol (NNTP) 79
Netzwerkebene 57
Netzwerkmanagement-System (NMS) 183
Netzwerkschicht 456
Netzzugangsebene 57
Netzzugangsschicht 456
News 29
NNTP 79
NSA 34

O
Observer 182
offene und transparente Sicherheit 294
offizielle IP-Adresse 361
ökonomische Aufklärung 34
One-Way-Hashfunktion 217
Operator 182
Opfer 513
Organisation 346
organisatorische Sicherheitsmaßnahmen 391
OSI-Referenzmodell 54
OSPF (Open Shortest Path First) 64
Out-Sourcing 32

P
Packet Filter 120, 185
Packet Filter mit Verschlüsselungs-
funktionen 301
Paradigmenwechsel 517
Passive Angriffe 82
Passwortregeln 273
Passwort-Verfahren 273
Permit Proxy 170
Persönlichkeitsrecht 514
Persönlichkeitsrechtsverletzungen 514
Personalausweis 219
personelle Sicherheitsmaßnahmen 391
Pförtner 44
PGP 237
Plug Gateways 166
Portnummern 67
Port-Relays 166
positiver Filterregeln 130
potenzielle Bedrohungen 92
Private-Key-Verfahren 214
Produktauswahlverfahren 388
Produktpiraterie 514
Protokollierung von Ereignissen 370
Proxy 145
  Application Level 147
  Authentication 165
  Circuit Level 166
  FTP 157
  HTTP 159

fw5SIX.fm Seite 603 Freitag, 18. Oktober 2002 4:51 16

SMTP 148
spezielle 166
Telnet 152
Prüflabor 398
Prüfstelle 398
Public Domain Software 287
Public-Key-Verfahren 215

R
Recht im Internet 513
Rechteverwaltung 48, 182
rechtsfolgenfreier Raum 513
Redirect 66
Redundanzsystem 136
Regelwerk 118, 470
Reisepass 219
reservierte IP-Adressen 361
RIP (Routing Information Protocol) 64
Risiko 36, 112
Risikogesellschaft 518
Routing Protokolle 63

S
S/Key 275
S/MIME (Secure MIME) 237
SA 545
Sabotage 514
SATAN 98, 468
Scannerprogramme 97, 467
scheinbare Sicherheit 293
Scheinsicherheit 295
Schutzbedarf 207
Screened Subnet 195
Secure Socket Layer 213
Security Administrator 182
Security Association 545
Security Audit 416
Security Audit-Systeme 113
Security Gateway 323
Security Management 118, 181
Security Newsletter 113
Security Token 278
Security-Administrators 349
Servicearbeiten 372
sichere Anordnung 346
sichere Einbindung 119
sicherer Betrieb 391
Sicherheitsanforderungen 559
Sicherheitsbewusstsein 31
Sicherheitsdienste eines Firewall-Systems 476
Sicherheitsgefühl 339
Sicherheitskonzept 45, 339
Sicherheitslücken 348
Sicherheitsmaßnahmen 345, 391
Sicherheitsmechanismen 214
Sicherheitspolitik 339, 417, 470
sicherheitsrelevante Aktionen 436
sicherheitsrelevante Informationen 138
Sicherheitsverletzungen 432
Sicherheitsvorgaben 399
Sicherheitsziele 340
Signatur 231
Signaturkarte 280
Simple Key-Management for Internet Protocols 536
Single-homed Application Gateway 190
Single-Shot-Modus 138
Site-Hacking 525
skalierbare Sicherheit 307
SKIP 536
smart filtering 143
SmartCard 226
SMTP 74
SMTP-Protokoll 74
SMTP-Proxy 148
Social Engineering 353
SOCKS 172
SOCKS-Versionübersicht 176
Software-Diebstahl 514
Software-Fehler 89
Software-Piraterie 527
Source Quench 66
Spezielle Proxies 166
Spionage 31, 514
Splitted DNS 212
SSL 213, 262
staatliche Restriktionen 295
Stärke der Sicherheitsmechanismen 403
stateful inspection 142, 143
STOA 527
Store-and-Forward-Prinzip 148
Strafgesetzbuch 517
symmetrisches Verschlüsselungsverfahren 214

fw5SIX.fm Seite 604 Freitag, 18. Oktober 2002 4:51 16

T
TCP 70
TCP/IP-Protokollarchitektur 56, 455
TCP/IP-Technologie 53
technische Sicherheitsmaßnahmen 391
Telekommunikationsgesetz 517
TeleTrusT 243
Telnet 72
Telnet Proxy 152
Tests 400
TLS 262
Traffic-Key 537
Transparent Proxy 166
transparente Sicherheit 294
Transportebene 57
Transportmodus 540
Transportschicht 456
Trittbrettfahre 87
Trustcenter 219
Tunnelmodus 540
Two-Way Authentication 281

U
UDP 69
Übertragungsfehler 89
Unrechtsbewusstsein 34
unterbrechungsfreie Stromversorgung (USV) 345
URL-Blocker 160

V
Vandalismus 96
Veränderung der Geschäftsprozesse 33
Verantwortlichkeiten 346
Verarbeitungsmodul für sicherheitsrelevante Ereignisse 117
Verbergen der internen Netzstruktur 49
Verbindlichkeit 36
Verfügbarkeit 36, 366
Verifikation von Signaturen 234
Verkehrsflussanalyse 83
Verschlüsselung 213
Verstoß gegen Gesetze/Vorschriften/ Verträge 93
vertrauenswürdiger Administrator 351
Vertrauenswürdigkeit 294
Vertraulichkeit 33, 35
Vertraulichkeit der Nachrichten 49
Vertretungsregelungen 351
Virengefahr 313
Viren-Scanner 314
Virtual Private Network 213, 256
Vortäuschung einer falschen Identität (Maskerade-Angriff) 87
VPN 213, 256
Box 301

W
Wartungs- und Reparaturarbeiten 350
Weiterentwicklung 414
Wert der Informationen 33
Widerspruchsfreiheit 181
Wiederholen oder Verzögern von Informationen 86
Wirkung der Sicherheitsdienste 481
Wirtschaftsspionage 34, 516, 524, 526
World Wide Web 29, 52

Z
Zertifikat 230
Zertifikations-Systeme 218
Zertifizierung 396
Ziele von Firewall-Systemen 48
zugangsgesicherter Raum 345
Zugangskontrolle 32, 181
Zugangskontrolle auf Benutzerebene 48
Zugriffsrechte 347
zusätzliche Sicherheitsmaßnahmen 344
zustandsorientierte Packet Filter 142

fw5SIX.fm Seite 605 Freitag, 18. Oktober 2002 4:51 16

ISBN 3-8266-0935-2
www.mitp.de

Franz-Joachim Kauffels

Durchblick im Netz, 5. Auflage

Kauffels wendet sich mit diesem jetzt in der fünften Auflage vorliegenden Buch an alle, die wissen wollen, wie Netze und Kommunikationstechnik funktionieren, und was man damit anfangen kann. Dem neugierigen Leser sollen die Spannbreite und Funktionsweise der heutigen Datenkommunikation vor Augen geführt werden, ohne dass er dabei allzusehr mit technischen Einzelheiten belastet wird.

Aus dem Inhalt:

- Vom Draht zum Downsizing
- Bauplan/Systemarchitektur von Netzen
- Wie Bits reisen
- PC-Netze, der große Erfolg
- Serverbetriebssysteme: NetWare, Windows , UNIX/Linux
- Integration der Netze und Dienste: ISDN, xDSL , ATM
- Internetworking: Bridging, Routing, Switching
- Entwicklung optischer Netze
- Wireless LANs / Drahtlose Netze
- TCP/IP, Internet, WWW
- GroupWare, Intranet
- Netzwerksicherheit, E-Commerce

fw5SIX.fm Seite 606 Freitag, 18. Oktober 2002 4:51 16

fw5SIX.fm Seite 607 Freitag, 18. Oktober 2002 4:51 16

ISBN 3-8266-4093-4
www.mitp.de

Petra Borowka

InterNetworking

4. Auflage

Das vorliegende Buch eignet sich als strategischer Ratgeber ebenso wie als technische Referenz. Es vermittelt für Netzwerkplaner unentbehrliches Know-how zu Design-Konzepten, Protokollen, Standards und deren aktuelle Relevanz auf dem nach wie vor wachsenden Markt des Enterprise Networking. Highlights dieser vierten Auflage sind die neu erschlossenen Themen SAN/NAS, Voice over IP, VPN, MPLS, Rapid STP und 802.1x Security.

Aus dem Inhalt:

- Entwicklung gekoppelter Netze
- Netzwerkstrukturierung: Systematische Einführung
- Brücken-Technik
- Transparent Bridging, Spanning Tree
- Source Routing-Brücken
- Filter, Trunking, Load Balancing
- Port-basierte Zugangskontrolle mit 802.1x
- Routing-Technik
- Protokolle und Routing im TCP/IP-Umfeld
- Multiprotokoll-Technik
- Layer-2/3/4/7-Switches
- Virtuelle LANs
- QoS mit etablierten Frame-Technologien
- LAN/WAN-Verbindung
- Multiprotocol Label Switching
- Voice over IP
- Virtual Private Networks
- Anbindung von Hochleitungsservern, Adapter Load Balancing, Load Balancer Switches
- Storage-Netzwerke (SAN, NAS)

fw5SIX.fm Seite 608 Freitag, 18. Oktober 2002 4:51 16