Automatisiertes Sammeln, Analysieren und Bewerten von Unternehmensinformationen im Internet

DIGITAL RISK MANAGEMENT (DRM)

Ein professionelles Digital-Risk-Management-System scannt das Clearnet, Deep Net und Darknet nach auffälligen, potenziell sensiblen Dokumenten und Informationen, um Hinweise für technische oder menschliche Sicherheitsrisiken identifizieren zu können. Die Prävention von Cyberangriffen ist nach wie vor eine entscheidend wichtige Säule, um die Digitalisierung zu meistern, Geschäftswerte langfristig zu schützen und die Anzahl an kritischen Sicherheitslücken im Unternehmen gering zu halten. Im Rahmen eines Master-Projekts hat sich das Institut für Internet-Sicherheit (ifis) mit dem Thema DRM auseinander gesetzt und insbesondere das Tool RISKREX [1] exemplarisch analysiert.

Im Laufe der Zeit produzieren Unternehmen, Behörden und andere Organisationen eine wachsende Menge an Informationen und Daten, die je nach Situation in den unterschiedlichen Bereichen des Internet (Clearnet, Deep Net und Darknet) gespeichert und oft nie wieder gelöscht werden. Hinzu kommen Informationen, die Dritte (Lieferanten, Partner, Kunden etc.) über das Unternehmen im Internet ablegen. An sich sind solche Informationen meist unkritisch – aus einzelnen Infos können Kriminelle in der Regel keine Angriffsziele entwickeln. Problematisch wird es aber, wenn die Menge der Daten immer größer wird und Angreifer intelligente Tools einsetzen, um die einzelnen Infos zu verketten (Bild 1). Mit der Kombination von Daten aus einem ständig wachsenden Pool sind Kriminelle eben doch in der Lage, die Erfolgsaussichten ihrer Angriffe drastisch zu erhöhen. Digital-Risk-Management-Systeme sollen Unternehmen dabei unterstützen, das Gefahrenpotenzial aus diesen Quellen besser einzuschätzen, potenzielle Angriffe zu verhindern und den Erfolg von Cybersicherheitsprojekten messen zu können.

Neue Ansätze – menschliche und technische Angriffsvektoren automatisiert zu erfassen, Datenpunkte sinnvoll zu kombinieren und Risiken datengetrieben zu reduzieren – ermöglichen neben der zielgerichteten Awareness-Kampagne auch die Erfolgsmessung von Cybersicherheitsprojekten. Ein Digital-Risk-Management-System fällt unter die Cybersicherheitsstrategie: „Vermeiden von Angriffen“ [2]. Gerade für den Mittelstand sind kosteneffiziente IT-Technologien ausschlaggebend, um den Bedarf zu ermitteln, welche Cybersicherheitsmaßnahmen zu welcher Zeit die richtigen sind. Die Durchführung von Awareness Kampagnen und Penetrationstests sind etablierte Formate zur Erhöhung des Cybersicherheitsniveaus. Es hängt jedoch vom Unternehmen ab, welche Cybersicherheitsmaßnahme eine erhöhte Priorität genießen sollte. Eine datengetriebene Analyse unterstützt Cybersicherheitsverantwortliche bei der Entscheidung.

DIGITALE RISIKEN ENTDECKEN, REDUZIEREN UND VERMEIDEN

Das weltweit größte Geschäftsrisiko 2020 sind Cybervorfälle. Inbegriffen sind Cyberkriminalität, IT-Ausfälle, Datenschutzverletzungen und Wirtschaftsspionage. Diese Bewertung ist angemessen, da zum Beispiel moderne Ransomware-Angriffe vor der Verschlüsselung Unternehmensdaten abgreifen und bei Nichtzahlung des Lösegeldes die Daten veröffentlichen. Mit der zunehmenden Digitalisierung rückt also auch die digitale Gefahr in den Mittelpunkt. Doch die abstrakte, unsichtbare Bedrohung ist schwer zu greifen.

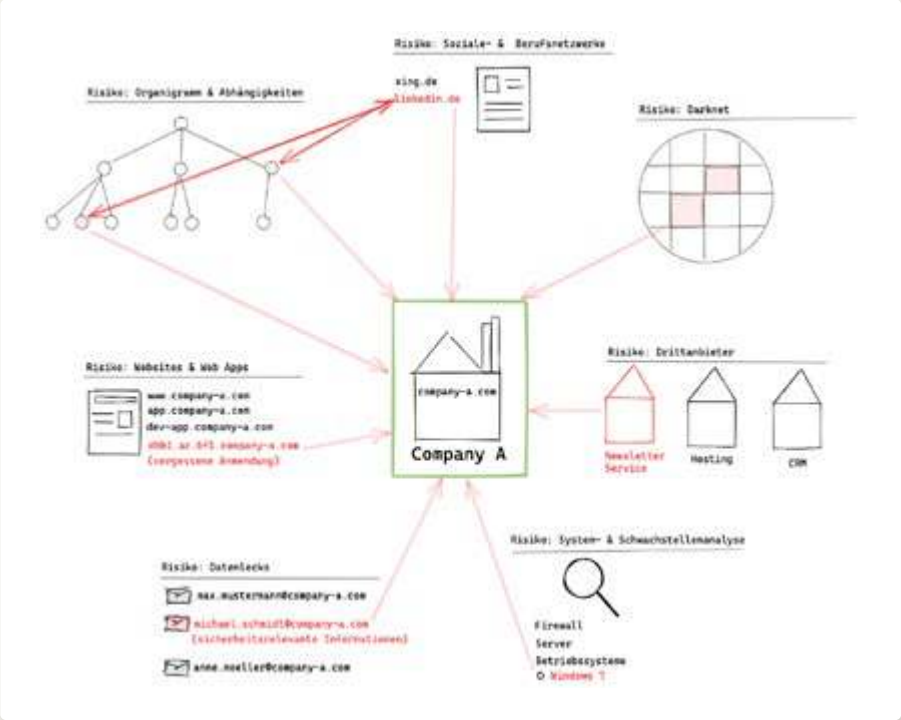

Bild 1: Die Sicht der Angreifer auf Unternehmen

Instagram, Facebook, LinkedIn und XING sind soziale beziehungsweise Berufsnetzwerke, die von ausgefüllten Profilen, einer regen Diskussion und fleißig geteilten Beiträgen leben. Daten, die nicht in den Händen der Betreiber bleiben, werden zur Gefahr für alle Beteiligten [3]. Eine frühzeitige Erkenntnis über den Abfluss von Daten (sicherheitsrelevante Informationen, wie Nutzername/Passworte, Antworten von Sicherheitsfragen etc.) und den notwendigen, anschließenden Maßnahmen, wie zum Beispiel die Änderung der Sicherheitsfragen, Software-Tokens und Passwörter, kann von einem Digital-Risk-Management-System erkannt und angestoßen werden. Unternehmen, die nicht für einen ausreichenden Schutz gesorgt haben, droht im Anschluss an den Datendiebstahl noch zusätzlich ein hohes Bußgeld, wenn es sich um datenschutzrelevante Informationen handelt.

2019 allein wurden 8,5 Milliarden Datensätze gestohlen [4]. Dass diese Datengrundlage als Basis für kriminelle Aktivitäten herhält, ist Cybersicherheitsspezialisten längst bekannt. Betroffene spüren die negativen Auswirkungen häufig erst dann, wenn die Daten von Fremden aktiv ausgenutzt werden [5]. Dabei ist der Umfang und die Gültigkeit der Daten häufig ausschlaggebend für den potenziellen Schaden, der verursacht werden kann.

Gerade die Zusammenführung von gestohlenen Datensätzen kann zu einer Identifizierung einzelner Personen führen. Besonders existenzbedrohend für die betroffene Mitarbeiter, und eine Vorlage für Erpressungen, ist der Zustand, wenn dieser Mitarbeiter auf einer Fremdgeh- oder Pornografie-Website, die von einem Datendiebstahl betroffen war, registriert gewesen ist [6]. Dieses Wissen ermächtigt Angreifer dazu, Druck auf die betroffenen Mitarbeiter auszuüben. Dieser menschliche Risikofaktor kann durch die Verwendung eines Digital Risk Management Tools vorhergesehen und seine Ausnutzung durch Kriminelle verhindert werden (Bild 1). Handlungsempfehlungen und weitere Informationen zu zahlreichen Betrugs- und Erpressungsmaschen werden den Verantwortlichen bei Entdeckung oder Bedarf bereitgestellt.

Eine große Herausforderung ist die Mehrfachverwendung von Passwörtern. Umständliche Passwortregeln galten dabei lange als Mittel der Wahl, um diese Gefahr zu reduzieren beziehungsweise zu beseitigen. Die Theorie hat sich in der Praxis jedoch nicht bestätigt. Aus diesem Grund empfiehlt das Bundesamt für Sicherheit in der Informationstechnik (BSI) seit 2020 nicht weiter die regelmäßige Änderung von Passwörtern [7]. Aber: Für jede Plattform ein eigenes Passwort. Das Passwort sollte auch erst beim Verdacht des Diebstahls geändert werden. In der Vergangenheit hat die minimale Abänderung von Passwörtern ausgereicht, um die Anforderungen beziehungsweise Regeln zu erfüllen. Der eigentliche Zweck, nämlich gestohlene Passwörter unbrauchbar zu machen, wurde dabei nicht von jedem erfüllt. Ein modernes Digital Risk Management Tool, wie zum Beispiel RISKREX, durchsucht zurückliegende und aktuelle Datendiebstähle vollumfänglich und informiert betroffene Mitarbeiter entweder direkt oder berichtet an den für die Cybersicherheit Verantwortlichen.

Ein Passwortwechsel kann dann, basierend auf der Betroffenheit von Datenlecks, ausgelöst werden. Dies entspricht der Forderung des BSI für die „Regelung des Passwortgebrauchs", die ein Passwortwechsel fordert, nachdem unautorisierten Personen das Passwort bekannt geworden ist. Ein Verdachtsmoment für den Wechsel genügt. Unternehmen, die ein technologisch fortschrittliches Digital-Risk-Management-System einsetzen, ersetzen zum Großteil die Kosten für die individuelle Anfertigung von IT-Sicherheitsanalysen, basierend auf menschlichen und technischen Angriffsvektoren. Werden schwerwiegende Probleme erkannt, kann Kontakt zu etablierten Partnern aufgenommen werden.

DIE SICHT VON AUSSEN AUF DAS EIGENE UNTERNEHMEN (HACKER-VIEW)

Auch kompromittierte Kontaktdaten über Dritte oder freiwillig preisgegebene Daten über soziale Netzwerke haben das Potenzial, das letzte Puzzlestück in der Cyber Kill Chain zu sein. So sind auch Informationen über genutzte Telefonnummern, die installierten Instant Messenger sowie deren Nutzungsrate für Kriminelle interessant. Die Durchführung von Betrugsmaschen, wie zum Beispiel die des Geschäftsführerbetrugs (CEO Fraud), erfordert umfangreiche Informationen über Zielpersonen, Unternehmen und Kontaktpersonen [8].

Dieses umfangreiche Geflecht aus Informationen und Daten zu überblicken, erfordert umfangreiche Recherchearbeiten, die bisher zum größten Teil von Cybersicherheitsanalysten durchgeführt werden. Dabei ist genau der Blick auf das Unternehmen von außen, den

auch Cyberkriminelle haben, essenziell für die Einschätzung von digitalen Risiken. Weniger ist mehr! Je schwieriger Informationen über die Infrastruktur, Belegschaft und das Organigramm zu erhalten sind, desto besser gelingt der Schutz gegen Angreifer.

Dabei reicht der Blick auf die Schutzmaßnahmen durch Technik längst nicht mehr. Dass Angreifer sich spektakulär über das Mobiltelefon des Angestellten in das Firmennetz hacken, entspringt eher der Fantasie eines Hollywood-Regisseurs. Oft ist es die Phishing Mail, die angeklickt wird. Der noch immer für Aufsehen sorgende Equifax-Hack zeigt, dass eine technische Sicherheitslücke genügt, um umfangreiche Daten abfließen zu lassen [9]. Im Rahmen einer fortschrittlichen, vollautomatisierten Reconnaissance-Phase mit einem DRM-System wäre dieser kritische Zustand des Systems aufgefallen. Die Ausnutzung der Schwachstelle sowie deren Kritikalität hätten Verantwortliche bereits vor der Ausnutzung dazu gebracht, diese Lücke zu schließen. Einstieg für den spektakulären Hack war eine Sicherheitslücke in Apache Struts. Für diese gab es zwar bereits ein Patch, aber offensichtlich wurde dieser nicht ausreichend schnell eingespielt.

Cyberkriminelle greifen jedoch beim Großteil von Attacken auf den Vektor Mensch zurück. Bis zu 95 Prozent der Sicherheitslücken gehen dabei auf Fehler von Mitarbeitenden zurück. Doch auch die letzten fünf Prozent dürfen unter keinen Umständen vernachlässigt werden. Die vollautomatisierte Ausnutzung von technischen Schwachstellen macht diesen Vektor, auch wenn es nur eine von zwanzig Attacken ist, so kritisch. Wer sein Unternehmen langfristig schützen will, muss beide Aspekte, den Menschen und die Technik, berücksichtigen.

Ein professionelles DRM-Tool richtet sich stets nach den Bedrohungen, ausgehend von Cyberkriminellen, und nutzt die gleichen Informationen, Ansätze und Vorgehensweisen (Bild 1). Eine fortschrittliche Technologie aus dem DRM-Umfeld hat den Anspruch, den Kriminellen einen Schritt voraus zu sein. Dieses Ziel verfolgt sie mit folgenden Schritten:

1. Erfassung aktueller Angriffspotenziale

- Welche Mitarbeiter*innen sind in welchem Umfang in Datendiebstählen eigener und anderer Portale aufgelistet und welche Gefahr der dort verfügbaren sicherheitsrelevanten Informationen ergeben sich hieraus?
- Welche IT-Systeme werden in- und extern eingesetzt, sind für einen Angreifer erreichbar, verwundbar und werden aktiv gescannt?
- ...

2. Beseitigung und Verfälschung von sensiblen Informationen

- Anträge zur Löschung von Daten, Einträgen und Informationen, die ein Risiko darstellen
- Platzierung und Verfälschung Honey Pots mit Falschinformationen
- ...

3. Prävention und Verhinderung von potenziellen Angriffsvektoren

- Zielgerichtete Awareness-Schulungen von besonders erkannten Risiken
- Optimierung der Cybersicherheitsmaßnahmen, die einen hohen Widerstand gegen wahrscheinliche Angriffe haben
- Registrierung von Domains mit hohem Verwechslungs- und Täuschungscharakter, um Angriffe zu verhindern
- Aktive Unterstützung der IT-Abteilung bei sicherheitsrelevanten Ereignissen

Ein Penetrationstest, ein Phishing-Training oder die Durchführung eines Cyber-Security-Days sind allesamt geeignete Cybersicherheitsmaßnahmen zur Erhöhung des Cybersicherheitsniveaus. Doch der Effekt dieser Cybersicherheitsmaßnahmen sollte stets datengetrieben analysiert, berechnet, umgesetzt und nachgehalten werden. Zielgerichtete Kampagnen mit individualisierten Inhalten, die zugeschnitten auf das Unternehmen und dessen besondere Risiken sind, lassen sich entsprechend der fortlaufend erfassten Daten priorisieren. Diese Situation ist für Verantwortliche und Führungskräfte gleichermaßen erstrebenswert und führt zu einem höheren Schutz gegen Angriffe. Der erste Ansatz für die Durchführung von Cybersicherheitsmaßnahmen zur Erhöhung des Cybersicherheitsniveaus sollte stets mit dem Blick von außen auf das Unternehmen abgeglichen werden. Dieser Blick ist auch der der Angreifer, die potenziell auf der Welt verteilt sitzen können – und das unabhängig von Land und Uhrzeit (Bild 1).

WENN DER MENSCH IM FOKUS STEHT, WERDEN ANGRIFFE OFT ERFOLGREICH

Die zunehmende Cybersicherheit, wie die Nutzung der TLS-Verschlüsselung [10], sorgt für ein Umdenken bei den Kriminellen. Nicht zuletzt fördern Initiativen wie Lets Encrypt, die bereits eine Milliarde Zertifikate ausgestellt haben und für Anwender kostenfrei sind, eine höhere Cybersicherheit [11]. Doch bevor Hashes zurückgerechnet und moderne Authentifizierungsmethoden geknackt werden, setzen Cyberkriminelle auf menschliche Schwachstellen und bedienen sich nicht selten auch der kostenfreien, automatisierten Verfahren, die betrügerische, gefälschte Websites vertrauensvoll wirken lassen. Dabei klingt das Vorgehen so einfach wie banal. Anstatt, wie in der Vergangenheit, mit offensichtlich unseriösen Domains zu arbeiten, passen sich die Kriminellen an – schneller als sich die Betrugsmasche bei den Opfern herumsprechen kann.

BEISPIEL: Erfolgreiche Betrugsmaschen mit menschlicher Interaktion

Punycode Domains werden verwendet, um Opfer gezielt über Social Media oder Instant Messenger auf falsche Websites zu locken. Am Smartphone fällt die Prüfung der Domänen schwer. Bei guten Websites erkennt das Opfer den Unterschied nicht.

Bild 2: Punycode Domains – Beispiel 1

Nicht zuletzt werden diese professionell angelegten Domains auch per E-Mail versendet. Bis vor kurzem ist vor den sogenannten Punycode Domains noch nicht einmal gewarnt worden. Mittlerweile sind Instant Messenger nachgezogen und platzieren einen Hinweis, falls ungewöhnliche Zeichensätze in Links verwendet werden.

Bild 3: Punycode Domains – Beispiel 2

Die Beobachtung und Identifizierung von potenziell gefährlichen Domains, sei es über Punycode-Methoden oder schlichtweg über Verwechslung, ist Teil einer professionellen Digital-Risk-Management-Lösung, wie zum Beispiel RISKREX. Dabei wird im ersten Schritt automatisch ein Set an potenziell gefährlichen Domains angelegt:

ORIGINALE DOMAIN:
company-a.com

Potenziell gefährliche Domains:
com.pany-a.com, company.y-a.com, company-a.com, Company-a.com, compoany-a.com, c0mpany-a.com, +100

Gefährliche Domains zeichnen geschickte, kleine Manipulationen der Domain-Namen aus, die ein Großteil der Menschen im Alltag nicht bemerkt. Das gelingt durch Ersetzungen, unterschiedliche Zeichensätze, oder die Verwendung von Buchstabendrehern wie zum Beispiel bei poilzei.de. Eine moderne Risk Management Lösung beobachtet registrierte und freie Domains inklusive Subdomains. Getrennt bewertet werden Domains, die nicht von der eigenen Organisation registriert sind. Der Zustand, die Darstellung und potenzielle Entwicklung wird erfasst und bewertet. Treten Änderungen ein, erhalten die hinterlegten Verantwortlichen des Unternehmens umgehend eine Benachrichtigung.

Der Auslöser für die Benachrichtigung erfolgt auf mehreren Wegen. Registrierte, potenziell gefährliche Domains werden auf Erreichbarkeit untersucht. Wird die Domain auf eine baldige Live Schaltung vorbereitet, beginnt die Digital-Risk-Management-Lösung mit einem pixelgenauen Vergleich der Website. Sobald Ähnlichkeiten im unteren einstelligen Prozent-Bereich festgestellt werden oder in Subdomains ein Teil oder der ganze Firmenname erscheint, wird die Benachrichtigung versendet. Die Benachrichtigung kann dann der Auslöser sein, die Vorbereitung einer Phishing-Kampagne frühzeitig zu erkennen und Vorbereitungsmaßnahmen zu treffen. Erfolgen keine Hinweise und Warnungen vor konkreten Bedrohungen, droht die Phishing-Kampagne erfolgreich zu werden. Kosten durch Kontenwiederherstellung und Forensik sind schnell höher als die Kosten für ein Digital-Risk-Management-System.

SPÄTE ERKENNUNG, ERFOLGREICHER ABFLUSS UND LEISES VERSCHWINDEN – TECHNISCHE SCHWACHSTELLEN BILDEN DIE SARGNÄGEL

Dass jedoch eine auf Signaturen basierende Schutzfunktion nur so lange zuverlässig funktioniert, wie auch die Signatur bekannt ist, zeigten eindrucksvoll die ersten Ransomware-Wellen, von denen kleine Unternehmen und große Konzerne gleichermaßen kritisch betroffen waren. Sicherheitslücken im Betriebssystem, von denen potenziell jeder betroffen ist, sorgen für Einschläge in die Vertrauenswürdigkeit der Cybersicherheit. Dabei sind regelmäßig große Betriebssysteme, wie auch Software-Bibliotheken betroffen.

Cybersicherheitsverantwortlichen muss ein Werkzeug an die Hand gegeben werden, das genau die richtigen Informationen zur richtigen Zeit darstellt. So sind fehlende Records auf dem Mail Server zwar eine zu lösende Aufgabe, doch die Web Application mit einem veralteten Stand und einfach ausnutzbarer Sicherheitslücke, etwa in Form einer SQL-Injection, stellt ein Problem dar, das es schnell zu lösen gilt.

Die Aufgaben eines Cybersicherheitsverantwortlichen sind die Kontrolle, das Nachhalten, das Archivieren und das Auslesen von Logs. Das verbraucht viele Ressourcen. Diese Ressourcen lassen sich zum Großteil mit der Hilfe einer professionellen Digital-Risk-Management-Lösung einsparen. Der Blick von außen auf die eigene, technische Infrastruktur gibt den Verantwortlichen Werkzeuge mit, Schwachstellen schnell und priorisiert anzugehen. Schnell lösbare Probleme spiegeln sich im allgemeinen Cybersicherheitsniveau wider. Mittel- und langfristige Projekte können in Form von Cybersicherheitsprojekten geplant, umgesetzt und verfolgt werden.

Der Diebstahl von Daten oder das Ausnutzen von Rechten auf Plattformen Dritter kann zu erheblichen Datenschutz- und Sicherheitsproblemen führen. Informationen über Angebote, Verträge, geplante Patente und Unternehmensstrategien sowie Partnerschaften, tragen einen Großteil zum Fortbestand zahlreicher Unternehmen bei. Werden diese von Mitbewerbern gestohlen, handelt es sich um Industriespionage. Die Konsequenzen für Fehler von Drittanbietern haben Organisationen beziehungsweise Personen, wie beispielsweise Facebook [12], Boris Becker und ProSieben [13], bereits spüren müssen. Neben dem Abfluss von Daten können Kriminelle aber auch die Gelegenheit bekommen, Mails mit korrektem SPF-Record (Sender Policy Framework, ein Verfahren, mit dem das Fälschen der Absenderadresse einer E-Mail verhindert werden soll) zu versenden, falls für den gehackten Dritten ein entsprechender Eintrag im DNS hinterlegt worden ist. Ein professionelles, auf den digitalen Bereich spezialisiertes Digital Risk Management, ist so angelegt, dass es auf diese Gefahren frühzeigt vorbereitet.

BENCHMARKING DER EIGENEN UND DER ABHÄNGIGEN UNTERNEHMEN

Das Sammeln, Analysieren und Bewerten von Informationen und Daten ist der erste Schritt von Cyberkriminellen, um Attacken vorzubereiten. Im besten Fall erhalten Angreifer so wenige Informationen wie möglich. Doch welche Informationen in welchem Umfang auf welcher Plattform über die eigene Organisation erhältlich sind, ist für viele Unternehmen eine Herausforderung und häufig nur eine Bestandsaufnahme, die nach wenigen Wochen oder gar Monaten komplett neu erhoben werden muss. Die laufende Bewertung von Drittquellen und Anbietern, die Einschätzung von potenziellen, digitalen Risiken und die Bewertung der Zulieferkette wird

in Zukunft ein Schlüsselthema zur Erhöhung der allgemeinen Cybersicherheit mit Blick auf den technischen und menschlichen Faktor.

Das Darstellen und Berechnen von belastbaren, vergleichbaren und nachvollziehbaren Kennzahlen ist gerade für Cybersicherheitsprojekte, die sich häufig konkret auf das Cybersicherheitsniveau der Infrastruktur oder mitarbeitende Menschen auswirken soll, ein Vorteil für Projektleiter und Verantwortliche. Ressourcen, wie Budget und Zeit, lassen sich so konkret anhand der Verbesserung darstellen.

Der gesamte Schaden, welcher der deutschen Wirtschaft pro Jahr entsteht, beläuft sich auf etwa 102,5 Milliarden Euro. Eine Schadenssumme, die durch Sabotage, Datendiebstahl und zahlreiche andere digitale Angriffe entsteht. Um auch in Zukunft vor Angriffen auf Mensch und Technik gefeit zu sein, sind gezielte und generelle Cybersicherheitsmaßnahmen für das Vermeiden von Angriffen notwendig.

Ein Digital Risk Management hilft, diese Herausforderungen zu lösen. Über 250 Quellen (Tendenz steigend [14]) im Internet werden über offizielle und inoffizielle Wege abgerufen und sorgen für eine ausreichend große Datenbasis, um das IT-Sicherheitsniveau von Unternehmen zuverlässig und belastbar bewerten zu können. Das besondere an der Technologie, ist die Berücksichtigung der menschlichen Faktoren.

Das Risiko, einem Cybersicherheitsangriff zu unterliegen, wird in Form eines Cybersecurity-Scores dargestellt. Konkrete, digitale Brandherde werden den Verantwortlichen mit Handlungsempfehlungen angereicht. Aber auch die Schließung beziehungsweise Reduzierung des Risikos wird darstellbar. Das Prüfen von Partnern, Zulieferern, Kunden etc. ist ebenfalls möglich. Ein modernes Digital Risk Management ist ein sehr guter Ansatz – auch im KMU-Bereich. Der datengetriebene Ansatz erlaubt ab sofort allen Beteiligten, die Erfolgswirkung diverser Kampagnen zu messen (Bild 4).

FAZIT: IST MODERNES DIGITAL RISK MANAGEMENT MÖGLICH?

Auch wenn es keine 100prozentige Sicherheit im Cyberspace gibt, so sollten Abwehrmaßnahmen, Monitoring-Tools und Ansätze zur Prävention eines Angriffs in den festen Alltag integriert werden. Diese Schritte sind heute notwendig, um langfristig am Markt bestehen zu können [15]. Eine komplexer werdende Infrastruktur, neue

WAS IST EIN DIGITAL-RISK-MANAGEMENT-SYSTEM?“

Das Digital Risik Management ist die nächste Entwicklung im Bereich der Unternehmensrisiken und Cybersicherheit, die sich bei der Führung des Geschäfts zunehmend auf digitale Prozesse verlassen. Dabei ermöglicht ein professionelles Digital-Risiko-Management-System, wie zum Beispiel RISKREX, das digitale Risikoprofil der Organisation zu ermitteln, zu verstehen und unterstützt mit Wissen die Entscheidungsfindung und Protokollierung des Erfolgs.

Angriff	Vektor	Notwendige Informationen	Schutzmaßnahmen
Ransomware	**Technik** (Arbeitsplatzrechner, Server, Datenspeicher)	▪ Eingesetzte Spam-Filter-Regeln ▪ Verfügbare CVEs & Exploits	▪ Reduzierung der verfügbaren Informationen ▪ Frühzeitige Erkennung und Bewertung von CVEs mit der Hilfe eines Digital-Risk-Management-Systems
CEO-Fraud	**Mensch** (Sekretär*in, Geschäftsführer*in)	▪ Kontaktdaten (E-Mail, Telefon etc.) ▪ Kompromittierung von Accounts ▪ Offizielle Stellenbezeichnung ▪ Aufgabenbereich ▪ Arbeitszeiten	▪ Digital-Risk-Management-Alert-System für abgeflossene und gestohlene Accounts auf Systemen und Plattformen Dritter ▪ Reduzierung von verfügbaren Kontaktmöglichkeiten ▪ Einrichtung fester Prozesse über vorher festgelegte Kanäle
Phishing-Attacke	**Technik und Mensch** (Log-in-Daten für E-Mail-Postfächer und Portale)	▪ E-Mail-Adressen ▪ Eingesetzte Software ▪ Wiederkehrende und einmalige Events (Passwortwechsel) ▪ Domain zum Versenden von E-Mails	▪ Frühzeitige Erkennung von potenziell gefährlichen Domains mit einem Digital-Risk-Management-System ▪ Zielgerichtete Schulung von Mitarbeitern mit öffentlicher E-Mail-Adresse

Tabelle 1: Übersicht über Angriffsformen, Angriffsvektoren, notwendige Informationen zur Erkennung und Schutzmaßnahmen.

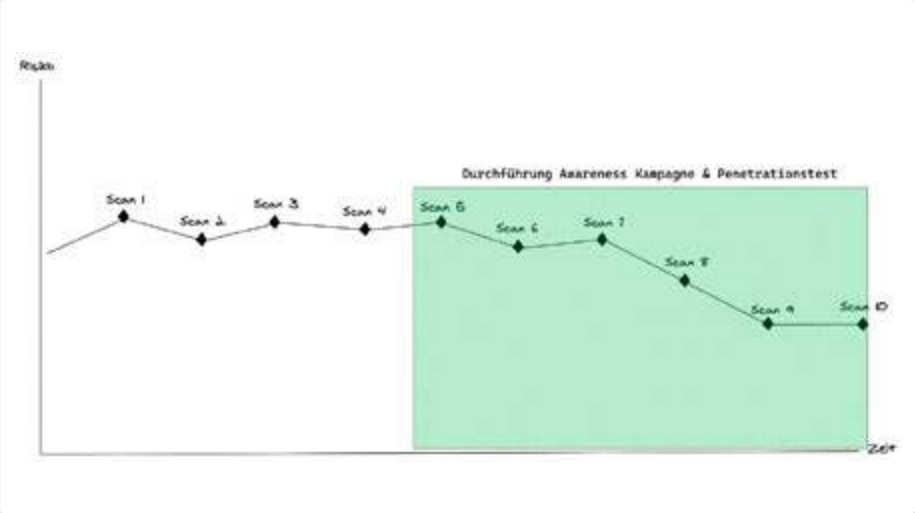

Bild 4: Das Risiko von Angriffen reduziert sich mit Digital Risk Management kontinuierlich.

Gefahren und Abhängigkeiten von Dritten, stellen Unternehmen weltweit vor die Herausforderung, potenzielle Angriffsvektoren frühzeitig zu erkennen und schließen zu können.

Mit einem modernen Digital Risk Management lassen sich neben technischen, auch menschliche Sicherheitsfaktoren ausmachen. Nur jede zwanzigste Cyberattacke findet rein technisch statt. Mit Digital-Risk-Management-Systemen besteht die Chance darauf, die anderen 19 Cyberangriffe kommen zu sehen und sich auf diese vorbereiten zu können. Die auf klein- und mittelständische Unternehmen ausgerichtete Technologie greift dabei auf mehrere Hundert Quellen zurück. IT-Abteilungen werden entlastet, IT-Security-Verantwortliche können den Erfolg von Cyber-Security-Projekten verfolgen, und auf unvermeidbare Angriffe und Risiken kann sich das Unternehmen vorbereiten.

Unternehmen ab einer Größe von zehn Mitarbeiter*innen sollten mindestens zwei Mal im Jahr einen Scan, die Ergebnisse eines Hacker-Views, durchführen. Bei einer steigenden Anzahl von Mitarbeiter*innen, mehr Werten in der IT, Abhängigkeiten von Lieferanten etc. empfiehlt sich die Durchführung kontinuierlicher, monatlicher Scans. Das IT-Sicherheitsniveau und das potenzielle Angriffsrisiko von Organisationen lässt sich mit der Hilfe von Digital-Risk-Management-System feststellen und vergleichen. ■

JAN HÖRNEMANN
studiert im Master Internet-Sicherheit am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums mit Digital Risk Management.

NORBERT POHLMANN,
Informatikprofessor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.

Quellen:

[1] *https://aware7.de/digital-risk-management/*

[2] *N. Pohlmann: „Wertschöpfung der Digitalisierung sichern – Vier Cybersicherheitsstrategien für den erfolgreichen Wandel in der IT", IT-Sicherheit – Mittelstandsmagazin für Informationssicherheit und Datenschutz, DATAKONTEXT-Fachverlag, Ausgabe 1/2020*

[3] *https://www.golem.de/news/deutscher-bundestag-persoenliche-daten-von-politikern-auf-twitter-veroeffentlicht-1901-138492.html*

[4] *https://newsroom.ibm.com/2020-02-11-IBM-X-Force-Stolen-Credentials-and-Vulnerabilities-Weaponized-Against-Businesses-in-2019*

[5] *https://arstechnica.com/information-technology/2020/02/four-plus-years-later-ashley-madison-hack-is-used-in-new-extortion-scam/*

[6] *https://www.seas.harvard.edu/news/2020/01/imperiled-information*

[7] *https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identit ProzentC3 ProzentA4ts-_und_Berechtigungsmanagement.html*

[8] *https://www.golem.de/news/ceo-fraud-autozulieferer-leoni-um-40-millionen-euro-betrogen-1608-122741.html*

[9] *https://www.heise.de/security/meldung/Equifax-Hack-Angreifer-ueber-Apache-Struts-Luecke-eingestiegen-3831905.html*

[10] *N. Pohlmann: „Cyber-Sicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung", Springer-Vieweg Verlag, Wiesbaden 2019*

[11] *https://www.golem.de/news/let-s-encrypt-1-million-freie-zertifikate-ausgestellt-1603-119643.html*

[12] *https://www.sueddeutsche.de/digital/datenmissbrauch-was-ist-eigentlich-gerade-bei-facebook-los-1.3932349*

[13] *https://www.wired.com/2012/07/yahoo-breach/*

[14] *https://awareseven.github.io/OSINTsources/*

[15] *https://www.blick.ch/news/schweiz/ostschweiz/swisswindows-ag-macht-per-sofort-dicht-170-mitarbeiter-entlassen-hacker-angriff-versetzte-den-todesstoss-id15771321.html*