Penetrationstest
Die professionelle IT-Sicherheitsuntersuchung

Die Durchführung eines Penetrationstest deckt bestehende Sicherheitslücken auf und unterstützt Sie dabei diese zu schließen. Eine Rufschädigung zu verhindern, Zertifizierungen abschließen zu können und Datenschutzverstöße zu vermeiden sind beispielhafte Ziele der Untersuchung.

Sind wir sicher gegen Angriffe aus dem digitalen Raum?

Diese oder ähnliche Fragen stehen häufig am Beginn Ihres Engagements Ihre IT-Infrastruktur. Bei einem Penetrationstest gehen unsere Sicherheitsforscher vor wie ein Angreifer. So können unwirksame Schutzmechanismen oder Schwachstellen aufgedeckt werden. Dadurch werden Ihre Systeme besser einschätzbar in Bezug auf Ihre Sicherheit und Sie können die Eignung Ihrer bisherigen Schutzmaßnahmen überprüfen. Insbesondere ein Information Security Management System (ISMS) kann bei der Bestimmung von Schutzbedarfen helfen.

MEHRWERT

Sie können mit unseren Penetrationstests bestimmte regulatorische Anforderungen erfüllen, beispielsweise im Rahmen einer ISO27001 Zertifizierung, der BAFIN oder dem BSI Grundschutz.

Weiterhin erhalten Sie ausführliche Dokumentationen und priorisierte Handlungsempfehlungen. Gefundene Schwachstellen werden kategorisiert nach standardisierten Rahmenwerken und Klassifikationsschemata, dadurch können Sie Ihre Ergebnisse vergleichen.

UNSERE VORGEHENSWEISE

In einem kostenlosen Erstgespräch sprechen wir den Umfang und den Schutzbedarf Ihres Vorhabens ab. Bei Bedarf unterzeichnen wir nun bereits eine Geheimhaltungsvereinbarung, sollten Sie ein komplexes System testen lassen wollen und keine seriöse Angebotserstellung ohne weitere Informationen möglich wäre.

Haben wir uns auf Ressourcen und Vorgehen geeinigt werden Testtiefe und Umfang im Kick Off Gespräch festgelegt. Hier lernen Sie die Projektverantwortlichen kennen und definieren Kontaktpunkte im Laufe des Penetrationstests.

Im Anschluss erfolgt dann der eigentliche Test und das Team nimmt seine Arbeit auf. Im Anschluss an den Test werden alle gefundenen Schwachstellen in einem Abschlussbericht zusammengefasst.

AUFWAND

Die Durchführung eines Penetrationstest ist immer ein Kompromiss zwischen Kosten und Aufwand. Eine effiziente Ressourcen- und Durchführungsplanung mit einem abgesteckten Umfang ist daher unerlässlich für einen erfolgreichen Penetrationstest.

Die Kosten sind immer davon abhängig, wie umfangreich der Test sein soll und wieviel Zeit das Team in einen erfolgreichen Angriff stecken soll. Bis zu 40% der Zeit können in die Erstellung eines Abschlussberichtes fließen.

Die Dauer eines seriösen Penetrationstests beginnt bei einfachen Webapplikationen mit zwei Tagen und kann bei komplexen Systemen mehrere Wochen beanspruchen. 67% unserer Penetrationstests dauern zwischen 5 und 8 Personentagen an.

KURZFAKTEN

Erfüllen Sie IT-Sicherheitsanforderungen mit der Durchführung eines Penetrationstests

Professionelle Einschätzung der IT-Sicherheit von Außen ohne Gefahr eines Vertrauensverlustes.

Vorgehensweise

1. Erstgespräch (kostenlos)
2. Durchführung
3. Abschluss

Jede Sicherheitsuntersuchung ist individuell. 67% unserer Pentest Projekte dauern zwischen 5 und 8 Personentage.

Vom Erstgespräch bis zur Durchführung sollten ca. vier Wochen einkalkuliert werden.

Die Dokumentation verlangt bis zu 40% der Projektzeit. Benötigen Sie ausführliche Berichte, Management Summarys und eine Abschlusspräsentation?

In der Regel folgt 4 - 6 Wochen nach dem Pentest ein Nachtest um die Wirksamkeit der getroffenen Maßnahmen zu überprüfen.

AWARE7
full service awareness agency

Jetzt unverbindlich Kontakt aufnehmen

Matteo Große-Kampmann
Geschäftsführer

matteo@aware7.de
https://aware7.de

+49 (0) 209 8830 676 - 2