Penetration Testing

Sicherheitsanalysen als aktives Risikomanagement

Sicherheitslücken in IT-Systemen sind bedrohlich für vertrauliche Daten. Durch Penetrationstests können Schwachstellen und Sicherheitslücken frühzeitig erkannt und geschlossen werden.

Die Herausforderung

Unternehmen sehen sich heute vielfältigen Cyber-Risiken ausgesetzt: Industriespionage von Konkurrenten, Angriffe durch Aktivisten, interne Täter, Angriffe auf den Zahlungsverkehr durch das organisierte Verbrechen oder sogar Hacking durch Staaten. Werden Schwachstellen und Sicherheitslücken in IT-Systemen und Anwendungen nicht frühzeitig erkannt und geschlossen, dann werden sie zur Bedrohung für die Vertraulichkeit, Integrität und Verfügbarkeit sensibler Unternehmensdaten.

Es besteht aber nicht nur ein vitales Eigeninteresse an einem wirksamen Schutz kritischer Daten – auch Geschäftspartner erwarten heute einen hohen Sicherheitsstandard. In Zeiten der alle Unternehmensprozesse durchdringenden Digitalisierung wird dies zu einer großen Herausforderung. Schnellere Entwickkungszyklen und agile Entwicklungsmethoden erschweren darüber hinaus den klassischen Penetrationstest. In diesem Spannungsfeld müssen Daten effektiv und effizient geschützt werden, um zukunftsfähig zu bleiben.

Unsere Leistung – Ihr Nutzen

Im Rahmen eines Penetrationstests analysiert KPMG Ihre Systeme und Anwendungen auf Schwachstellen und Sicherheitslücken. Unsere Global KPMG Security Testing Methodology sorgt dafür, dass das Qualitätsniveau eines Penetrationstests weltweit reproduzierbar hoch ist – überall da, wo unsere Kunden uns benötigen. Eine stringente Methodik ist dabei die Basis für eine strukturierte Erkennung, Auswertung und Risikobewertung aller festgestellten Sicherheitslücken. Vom Vulnerability Scan bis zum hochspezialisierten manuellen Penetrationstest, ob Black, Grey oder White Box oder von der Eigenprogrammierung bis zur Standardsoftware – unsere Spezialisten finden gemeinsam mit den IT-Experten unserer Kunden den für das jeweilige Unternehmen geeigneten Testansatz.

Im Vorfeld eines Penetrationstests wird dabei immer genau abgestimmt, wie weit wir bei der Ausnutzung einer Lücke gehen. Stellen wir im Rahmen unserer Tests fest, dass bereits eine Kompromittierung stattgefunden hat, unterstützen unsere Forensik-Spezialisten Sie gerne bei der Behebung und Aufarbeitung.

Im Nachgang eines Penetrationstests erarbeitet KPMG geeignete Umsetzungsmaßnahmen, mit denen die identifizierten Schwachstellen und Sicherheitslücken geschlossen werden können. Die Maßnahmen sind dabei immer so beschrieben, dass sie von einem sachkundigen IT-Mitarbeiter des Unternehmens umgesetzt werden können. Darüber hinaus enthält unser Bericht zu jeder Feststellung eine auf das Unternehmen angepasste Risikoeinschätzung und Kritikalitätseinstufung, die eine risikoorientierte Priorisierung ermöglicht. Eine Übersicht für das Management rundet unsere Ergebnisdokumentation ab.

Penetration Testing as a Service

Nachhaltiger als ein einmaliger Test ist eine kontinuierliche Überwachung. KPMG bietet Penetrationstests auch als dauerhaften Managed Service an, der einmal vereinbart und dann als regelmäßiger Check durchgeführt wird. Gemeinsam mit unseren Kunden bestimmen wir relevante Systeme und Anwendungen, die dann beispielsweise im Laufe eines Jahres getestet werden. Ihre Mitarbeiter werden so von dauerhaft wiederkehrenden Verwaltungsaufgaben befreit und erst dann wieder tätig, wenn aktuelle Sicherheitslücken dies erfordern.

Diese Services entlasten Ihre Mitarbeiter und ermöglichen zusätzlich eine preiswerte Kostenstruktur. Ferner entsteht so ein kontinuierliches Lagebild über Sicherheitslücken und Schwachstellen.

Bestens für Sie aufgestellt

Allein in Deutschland beschäftigen sich über 170 KPMG-Mitarbeiter mit Cyber Security. Dies ist nur einer der Gründe, warum Forrester Research das KPMG-Netzwerk als Global Leader in der Cyber- Security-Beratung sieht. KPMG hat in über 20 Jahren viele tausende Penetrationstests durchgeführt. Zudem verfügen wir über ein globales Pentesting-Netzwerk, in dem sich über 800 Mitarbeiter der verschiedenen KPMG-Mitgliedgesellschaften tagtäglich über die neuesten Sicherheitslücken, über Exploits und APTs austauschen. Diese umfangreiche Expertise ermöglicht es uns, individuelle Sicherheitstests für jedes Unternehmen durchführen und auf einen weltweit einmaligen Erfahrungsschatz zurückgreifen zu können.

KPMG ist selbstverständlich zertifiziert gemäß ISO/IEC 27001:2015 – wir beraten nicht nur zur Cyber Security, wir leben sie auch selbst.

Sie haben Fragen? Sprechen Sie uns gerne an.

Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft
Alfredstraße 277
45133 Essen

Uwe Bernd-Striebeck
Partner, Head of Cyber Security
T +49 201 455-6870
uberndstriebeck@kpmg.com

Wilhelm Dolle
Partner, Cyber Security
T +49 30 2068-2323
wdolle@kpmg.com

www.kpmg.de

www.kpmg.de/socialmedia