Penetrationstests

Sicherzustellen, dass die IT-Infrastruktur umfassend vor potenziellen Cyberattacken geschützt ist, ist für jedes Unternehmen eine ständige Herausforderung – insbesondere jedoch für Großunternehmen mit Tausenden von Mitarbeitern, Hunderten von Informationssystemen und einer Vielzahl von Standorten weltweit.

Ein Penetrationstest ist eine praktische Demonstration möglicher Angriffsszenarien, in denen versucht wird, die Sicherheitskontrollen Ihres Unternehmensnetzwerks zu umgehen und Zugriff auf wichtige Systeme zu erlangen.

Unsere Penetrationstests vermitteln Ihnen ein genaues Verständnis der Sicherheitslücken in Ihrer Infrastruktur, indem wir die möglichen Konsequenzen unterschiedlicher Angriffsarten analysieren, die Effektivität Ihrer aktuellen Sicherheitsmaßnahmen bewerten und Abhilfe- und Verbesserungsmaßnahmen vorschlagen.

Penetrationstests

Dank unserer Penetrationstests können Sie:

- **Schwachpunkte in Ihrem Netzwerk identifizieren,** um eine fundierte Entscheidung darüber zu treffen, wie finanzielle Mittel am besten einzusetzen sind, um das Risiko in Zukunft zu verringern.
- **Finanzielle und betriebliche Verluste sowie Rufschädigungen durch Cyberangriffe vermeiden**, indem Sie diese durch frühzeitige Erkennung und Schließen von Schwachstellen verhindern.
- **Behördliche Auflagen und Branchen- bzw. unternehmensinterne Normen erfüllen**, die diese Art von Sicherheitsprüfung vorschreiben (z. B. der Datensicherungsstandard für Kreditkartentransaktionen, PCI-DSS).

Serviceumfang und Optionen

Abhängig von Ihren Anforderungen und der bestehenden IT-Infrastruktur können Sie beliebige oder alle der folgenden Services in Anspruch nehmen:

- **Externer Penetrationstest:** Über das Internet vorgenommene Sicherheitsprüfung durch einen „Angreifer" ohne Vorkenntnisse über Ihr System.
- **Interner Penetrationstest:** Szenarien mit einem internen Angreifer, z. B. einem Besucher, der nur physischen Zugang zu Ihren Büroräumen hat, oder einem Dienstleister, der nur eingeschränkten Zugriff auf Ihre Systeme hat.
- **Social-Engineering-Test:** Assessment des Sicherheitsbewusstseins Ihrer Mitarbeiter durch Simulation von Social-Engineering-Angriffen, z. B. Phishing, schädliche Links in E-Mails, verdächtige Anhänge usw.
- **WLAN-Sicherheitsassessments:** Unsere Experten besuchen Ihren Standort und analysieren Ihre WLAN-Sicherheitskontrollen.

Welche Teile Ihrer IT-Infrastruktur Sie testen lassen, bleibt Ihnen überlassen, wir empfehlen jedoch, entweder das gesamte Netzwerk oder zumindest die größten Segmente einzubeziehen, da die Testergebnisse aussagekräftiger sind, wenn unsere Experten unter denselben Bedingungen arbeiten wie potentielle Eindringlinge.

Ergebnisse der Penetrationstests

Penetrationstests sollen Sicherheitslücken aufdecken, die ausgenutzt werden könnten, um Zugriff auf wichtige Netzwerkkomponenten zu erlangen. Dies beinhaltet u. a.:

- Anfällige Netzwerkarchitektur, unzureichender Netzwerkschutz
- Schwachstellen, die das Abfangen und Umleiten des Netzwerkverkehrs ermöglichen
- Unzureichende Authentifizierungs- und Autorisierungsmechanismen von unterschiedlichen Diensten
- Schwache Benutzeranmeldedaten
- Konfigurationsfehler inklusive zu umfangreicher Benutzerberechtigungen
- Schwachstellen durch Fehler im Programmcode (Code-Injektionen, Manipulation von Pfadangaben, Schwachstellen auf Clientseite usw.)
- Schwachstellen durch veraltete Hardware und Software ohne aktuelle Sicherheitsupdates
- Bereitstellung der Ergebnisse

Die Ergebnisse werden in einem abschließenden Bericht zusammengefasst, einschließlich detaillierter technischer Informationen zum Testvorgang, Ergebnissen, den entdeckten Schwachstellen und Empfehlungen für Korrekturmaßnahmen sowie einer Kurzübersicht über die Testergebnisse und die möglichen Angriffsvektoren. Auf Anfrage können auch Videos und Präsentationen für Ihre technische Abteilung und die Geschäftsführung bereitgestellt werden.

Informationen zur Vorgehensweise von Kaspersky Lab bei Penetrationstests

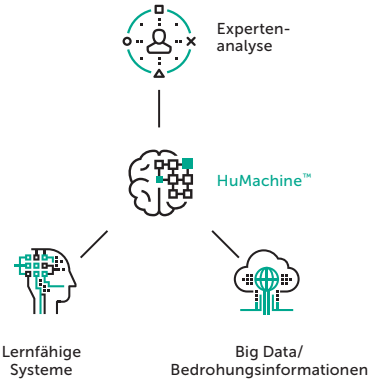
Obwohl bei Penetrationstests echte Hacker-Angriffe simuliert werden, werden diese Tests streng kontrolliert. Sie werden von Sicherheitsexperten bei Kaspersky Lab unter vollständiger Wahrung von Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Systeme ausgeführt und halten sich streng an internationale Normen und Best Practices, darunter:

- Penetration Testing Execution Standard (PTES)
- NIST Special Publications 800-115 „Technical Guide to Information Security Testing and Assessment“
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)
- Web Application Security Consortium (WASC) Threat Classification
- Open Web Application Security Project (OWASP) Testing Guide
- Common Vulnerability Scoring System (CVSS)

Bei den Mitgliedern des Projektteams handelt es sich um erfahrene Profis mit einem tiefgreifenden und aktuellen Praxiswissen auf diesem Gebiet, die als Sicherheitsberater von Branchenführern wie Oracle, Google, Apple, Microsoft, Facebook, PayPal, Siemens und SAP anerkannt sind.

Bereitstellungsoptionen

Je nach Art des gewünschten Sicherheitsassessments und ihrer speziellen Systembedingungen und Arbeitsabläufe können die Services entweder remote oder am Standort geleistet werden. Die meisten Services lassen sich per Fernzugriff ausführen und selbst die internen Penetrationstests können per VPN-Zugriff durchgeführt werden. Einige Services (z. B. WLAN-Sicherheits-Assessments) können jedoch nur vor Ort ausgeführt werden.



Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.de/enterprise**
Neues über Cyberbedrohungen: **https://de.securelist.com**
IT-Sicherheitsnachrichten: **www.business.kaspersky.com**

#truecybersecurity
#HuMachine

www.kaspersky.de