



Penetrationstest

Was ist ein Penetrationstest?

Bei einem Penetrationstest wird die Sicherheit Ihrer Datenbestände untersucht und bewertet. Dies kann auf verschiedene Arten geschehen. Die gängigste Methode ist, die Sicherheitsmaßnahmen aktiv auf Schwächen im Design, technische Fehler und Sicherheitslücken zu prüfen.

Wozu braucht man Penetrationstests?

Es gibt verschiedene Gründe, warum Unternehmen Penetrationstests durchführen lassen sollten. Diese Gründe können sowohl technischer als auch wirtschaftlicher Natur sein, wie etwa:

- Die Gefahren für die Datenbestände Ihres Unternehmens zu identifizieren, sodass Sie die Risiken, denen Ihre Daten ausgesetzt sind, bestimmen und entsprechende Investitionen in die Informationssicherheit tätigen können.
- Die Kosten für die IT-Sicherheit in Ihrem Unternehmen zu reduzieren und eine höhere Rendite Ihrer Investitionen in die IT-Sicherheit (ROSI) zu erhalten, indem Sie Sicherheitslücken und Schwachstellen identifizieren und eliminieren. Hierbei kann es sich um bekannte Sicherheitslücken in den zugrunde liegenden Technologien, Schwächen im Design oder die Folgen mangelhafter Implementierung handeln.
- Eine gründliche und umfassende Bewertung der Informationssicherheit in Ihrem Unternehmen zu erhalten, wobei sowohl Richtlinien und Verfahrensweisen als auch Design und Umsetzung untersucht werden.
- Ihr Unternehmen dauerhaft nach einer Industrienorm zertifizieren zu lassen (ISO 17799, HIPAA usw.).
- Die Einhaltung gesetzlicher und interner Vorschriften durch Best-Practice-Methoden sicherzustellen.

Mögliche Arten von Tests

1. Externe Penetrationstests stellen den traditionellen Weg dar, die Sicherheit eines Systems zu prüfen. Bei diesen Tests werden sämtliche Komponenten des zu untersuchenden EVG-Systems untersucht, darunter die Server, die Infrastruktur und die verwendete Software. Dies kann ohne Vorkenntnisse über das System geschehen (auch als Black-Box-Methode bekannt) oder nach vollständiger Offenlegung der Systemstruktur und -umgebung (White-Box-Tests). Bei den externen Tests werden öffentlich zugängliche Informationen über den EVG eingehend analysiert. Darüber hinaus wird die Netzwerkarchitektur ermittelt, indem die einzelnen Hosts identifiziert werden, und das Verhalten von Sicherheitseinrichtungen wie etwa Routern oder Firewalls gescreent und analysiert werden. Dieser Test dient dazu, Sicherheitslücken und Fehlkonfigurationen der Hosts zu identifizieren, zu verifizieren und deren Folgen abzuschätzen.

Der Test umfasst normalerweise:

- Analyse des Netzwerks
- Portscan
- Systemidentifikation
- Identifikation der Systemdienste
- Identifikation & Verifikation von Sicherheitslücken
- Router-Test
- Firewall-Test
- IDS-Test (Intrusion Detection System)
- Cracken von Passwörtern
- DoS-Test (Denial of Service)
- Test der Schutzmaßnahmen

2. Die Methoden beim **internen Sicherheitsaudit** ähneln jenen der externen Tests, bieten aber einen vollständigeren Überblick über die Sicherheit des Systems insgesamt. Die Tests werden üblicherweise von ausgewählten Zugangspunkten im Netzwerk aus durchgeführt, sodass alle logischen und physischen Segmente abgedeckt sind. Dazu zählen beispielsweise Zonen und DMZ in der Netzwerkumgebung, das globale Firmennetzwerk oder Verbindungen zu Partnerunternehmen.

Der Test umfasst normalerweise:

- Analyse des Netzwerks
- Portscan
- Systemidentifikation
- Identifikation der Systemdienste
- Identifikation & Verifikation von Sicherheitslücken
- Route-Test
- Firewall-Test
- IDS-Test (Intrusion Detection System)
- Cracken von Passwörtern
- DoS-Test (Denial of Service)
- Test von Trusted Systems

3. Das **Sicherheitsaudit von Applikationen** zielt darauf ab, Gefahren für das Unternehmen durch eigenentwickelte Anwendungen oder Systeme zu identifizieren und abzuschätzen. Diese Anwendungen könnten Nutzern interaktiven Zugriff auf potenziell vertrauliche Materialien bieten. Ein Audit ist äußerst wichtig; erstens, um sicherzustellen, dass die Anwendungen keine Angriffe auf deren Server oder die Software ermöglichen, und zweitens, um zu verhindern, dass böswillige Nutzer auf Daten oder Dienste innerhalb des Systems



zugreifen und diese modifizieren oder zerstören können. Selbst wenn ein Unternehmen über eine optimal umgesetzte und gut geschützte Infrastruktur verfügt, stellt eine schlecht abgesicherte Anwendung ein fundamentales Risiko dar.

Der Test umfasst normalerweise:

- Sicherheitsaudit der Anwendungen
- Code-Review

4. Beim Sicherheitsaudit für Wireless-LAN's und Remote-Zugriff werden Sicherheitsrisiken beurteilt, die aufgrund der gestiegenen Mobilität von Arbeitskräften entstehen. Das Arbeiten von zu Hause aus, ständig aktive Breitband-Internetzugänge, die drahtlose Vernetzung via 802.11 sowie die hohe Dynamik bei Technologien für den Fernzugriff setzen Unternehmen immer größeren und vielfältigeren Risiken aus als früher. Aus diesem Grund muss die Sicherheit derartiger Lösungen in Bezug auf Architektur, Design und Nutzung sowie ein effektives Risikomanagement gewährleistet werden.

Der Test umfasst normalerweise:

- Test der Drahtlosnetzwerke
- Test der Schnurloskommunikation
- Datenschutzaudit
- Test der Infrarot-Systeme

5. Das Telefonie-Sicherheitsaudit befasst sich mit der Sicherheit von Technologien, die in Unternehmen zur Sprachübertragung zum Einsatz kommen. Dies beinhaltet den Missbrauch firmeneigener Telefonanlagen durch Außenstehende, wenn diese Anrufe auf Kosten des Unternehmens weiterleiten, die Integration von VoIP-Technologien (Internet-Telefonie), die unbefugte Nutzung von Modems sowie die damit verbundenen Risiken.

Der Test umfasst normalerweise:

- Test der Nebenstellenanlage (PBX)
- Voicemail-Test
- Untersuchung des Faxdienstes
- Modem-Test

6. Social Engineering bedeutet, dass Personen in ein System eindringen möchten, ohne dabei technisches Fachwissen anzuwenden. Diese Methode baut auf der zwischenmenschlichen Kommunikation auf, wo Menschen dazu gebracht werden, übliche Sicherheitsmaßnahmen zu umgehen. Bei dieser „sozialen Manipulation“ ist normalerweise Betrug im Spiel – oft versuchen die Betrüger, das Vertrauen einer zuverlässigen Auskunftsperson zu gewinnen,

indem sie ihre natürliche Hilfsbereitschaft oder ihre Schwächen ausnutzen, ihnen schmeicheln, ihre Autorität einsetzen oder ihre Opfer belauschen. Andere Techniken bestehen etwa darin, Mülltonnen nach brauchbaren Informationen zu durchsuchen, Personen über die Schulter zu schauen und sich so ihre Zugangscodes zu merken, oder die Tatsache auszunutzen, dass Menschen von Natur aus dazu geneigt sind, einfach zu merkende und damit leicht zu erratende Passwörter zu wählen.

Der Test umfasst normalerweise:

- Stellen von Anfragen, um Zugriffsrechte zu erhalten
- Gezielte Einladungen, z. B. einem Link zu folgen („Guided Suggestion Testing“)
- Vertrauenstest

Methodik – Grundvoraussetzung für den Erfolg

Der Großteil der Tests besteht aus der systematischen Analyse der vorhandenen Sicherheitsmaßnahmen. Eine fehlende Methodik könnte dazu führen, dass die Tests nicht konsistent sind. Häufig verwendete Methoden: OSSTMM, OWASP sowie Veröffentlichungen des **National Institute of Standards and Technology** (NIST). In der Sonderveröffentlichung 800-42, die den Titel „Guideline on Network Security Testing“ (Richtlinie über das Testen der Netzwerksicherheit) trägt, befasst sich die US-amerikanische Einrichtung NIST mit dem Thema Penetrationstests. Die Umsetzung derartiger Methoden und Normen bietet dem Berater einen Überblick über die Struktur der wichtigsten Testbereiche, sodass der Test insgesamt vollständig und exakt ist.

Berichte

Die wichtigste Phase der Penetrationstests ist die Präsentation der Ergebnisse. Die einzelnen Testphasen werden dokumentiert und genau beschrieben, wobei das Endergebnis normalerweise auf zwei verschiedene Arten präsentiert wird – das Management erhält einen überblicksartigen und die Information Security Verantwortlichen einen detaillierten Bericht. Der Kernaspekt dieser Berichte besteht darin, Empfehlungen abzugeben, wie die identifizierten Sicherheitslücken geschlossen und die Risiken somit minimiert werden können.