IT Security Management

Penetrationstests

Die Sicherheit von Systemen, die über Verbindungen zu öffentlichen oder privaten Netzen verfügen und damit von außen bzw. von innen erreichbar sind, wird durch unautorisierte, meist anonyme Zugriffsversuche gefährdet. Diese Problematik erfordert Sicherheitstests unter möglichst realen Bedingungen aus dem Blickwinkel eines Angreifers. Eine dafür geeignete Methode ist der Penetrationstest. Hierbei handelt es sich um einen kontrollierten Versuch, in ein IT-System einzudringen. So decken Sie nicht nur technische, sondern auch organisatorische und konzeptionelle Schwachstellen Ihrer IT-Infrastruktur zuverlässig auf.

Typen

Penetrationstests lassen sich je nach Zielsetzung sehr individuell gestalten. So wird z. B. die Menge an Informationen, die der Tester vorab erhält, oder die Aggressivität, mit der er vorgeht, an Ihre konkreten Anforderungen angepasst, um eine effektive und effiziente Durchführung mit kalkulierbarem Risiko sicherzustellen. Als Basis dienen das „Open Source Security Testing Methodology Manual“ (OSSTMM), das „Open Source Web Application Security Project“ (OWASP) sowie die Konzepte des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Nähere Informationen dazu finden Sie im Internet unter folgenden Adressen:

- http://www.isecom.org/osstmm/
- http://www.owasp.org/
- http://www.bsi.de/

Vorgehensweise

Der Penetrationstest gliedert sich in fünf Phasen:

1. **Vorbereitung** – Zu Beginn definieren wir gemeinsam mit Ihnen Ziele, Umfang, Typ, Vorgehensweise sowie Prüfobjekte des Penetrationstests. Darüber hinaus informieren wir Sie über potenzielle Risiken und entsprechende Notfallmaßnahmen.
2. **Informationsbeschaffung und -auswertung** – Ziel dieser Phase ist es, eine möglichst vollständige und detaillierte Übersicht der installierten Systeme inklusive potenzieller Angriffspunkte zu erlangen. Die Module in dieser Phase umfassen u. a. die Auswertung öffentlich zugänglicher Daten wie DNS oder WHOIS, verschiedene Port- und Anwendungsscans, OS Fingerprinting, Sammlung von FTP- und Webserver-Dateistrukturen, Untersuchung von Cookies, Web Server Session Handling und Schwachstellenrecherche.

   Bei einem White-Box-Test kommen weitere Komponenten hinzu, wie z. B. die Untersuchung von Patch-Ständen und sicherheitsrelevanten Konfigurationsdateien der Betriebssysteme bzw. Anwendungen.
3. **Bewertung der Informationen/Risikoanalyse** – Die in Phase 2 gesammelten Informationen werden analysiert und ausgewertet. Dies dient als Grundlage für die Angriffsversuche in Phase 4.
4. **Aktive Eindringversuche** – Die ausgewählten Systeme werden, ausgehend von den Ergebnissen der vorherigen Phasen, aktiv angegriffen. Dabei kommen u. a. folgende Module zum Einsatz: Password Cracking, Ausnutzung von Buffer Overflows, Cross-Site Scripting, SQL Injection, Übernahme von Web-Sessions und Social Engineering.
5. **Abschlussanalyse** – Die Ergebnisse aller Phasen fassen wir in einem Bericht zusammen, der auch eine Bewertung der gefundenen Schwachstellen in Form potenzieller Risiken sowie Empfehlungen zur Behebung der Schwachstellen beinhaltet.

Ergebnis

Mithilfe der im Abschlussbericht dokumentierten Maßnahmen können Sie die identifizierten Schwachstellen in der IT-Infrastruktur beheben und damit die IT-Sicherheit in Ihrem Unternehmen erhöhen.

plan42

plan42 ist ein Beratungsunternehmen, das sich auf die Bereiche IT Service Management, IT Security Management & Business Solutions spezialisiert hat. Von der Prozessanalyse über die Beratung und Konzeption bis hin zur Realisierung – plan42 verbindet technische Expertise mit praxisbewährten Konzepten aus den Bereichen IT Service & Security Management.