Mike Kuketz

Vorgehensmodell Penetrationstest

KUKETZ IT-SECURITY

Penetrationstest Vorgehensweise

Penetrationstests (Pentest) sind vergleichbar mit einem **realen Angriff** auf Ihre IT-Systeme. Ich schlüpfe in die Rolle eines »Hackers« und versuche mit professionellen Werkzeugen, gezielt und individuell in die zu prüfenden IT-Systeme oder ganze Netzwerke einzudringen. Am Ende eines jeden Pentests erhalten Sie einen **umfassenden** Bericht, der die identifizierten Schwachstellen detailliert erläutert, bewertet und Empfehlungen zur Behebung aufzeigt. Auf Grundlage dieses Berichts können wir dann gemeinsam Lösungen erarbeiten und die gefundenen Schwachstellen gezielt beheben.

Ich biete Ihnen Pentests für folgende Bereiche an

IT-Systeme

Webanwendungen

Android-Apps

Mein Vorgehensmodell

Projektierung

Die Vorbereitung des Pentests erfolgt im Rahmen einer gemeinsamen Projektierung mit den technischen und organisatorischen Verantwortlichen Ihres Unternehmens. Anhand von 12 zentralen Punkten werden darin die **Rahmenbedingungen** des Pentests festgelegt. Unter anderem wird hierbei die zu prüfende IT-Infrastruktur spezifiziert, Umfang und Detailgrad der Tests abgestimmt, sowie Ansprechpartner definiert.

Informationsbeschaffung [Phase 1]

In der ersten Phase werden möglichst viele Informationen über die in der Projektierung spezifizierten Ziele gesammelt. Zu diesem Zweck werden verschiedene öffentlich verfügbare **Informationsquellen** durchsucht. Die hierbei gewonnen Erkenntnisse geben oftmals einen sehr detaillierten Einblick in die Zielsysteme und dienen als Ausgangspunkt für den weiteren Ablauf.

Kontakt

+49 (0) 721 / 467 162 17
info@kuketz-security.de

Web

www.kuketz-security.de
www.kuketz-blog.de

Penetrationstest Vorgehensweise

Angriffsvektoren [Phase 2]

Ausgehend von den im ersten Schritt gesammelten Informationen werden anschließend mögliche **Einstiegspunkte** in die zu testenden IT-Systeme erkundet. In dieser Phase wird also aktiv mit den IT-Systemen interagiert, um potenzielle Schwachstellen bzw. Angriffsvektoren zu identifizieren.

Exploitation [Phase 3]

In der dritte Phase wird versucht, die identifizierten Schwachstellen gezielt ausnutzen. Abhängig vom jeweiligen Dienst oder IT-System werden hierfür neue **Exploits** entwickelt oder bereits vorhandene verwendet, um Zugriff auf die Zielsysteme und gespeicherten Daten zu erlangen. Falls in ein IT-System eingedrungen werden kann, ergeben sich aus dem Zugriff häufig **weitere** mögliche Angriffsziele, die zuvor nicht erreichbar waren.

Report [Phase 4]

Die Ergebnisse des Pentests werden in einer dreiteiligen Dokumentation erfasst. Im ersten Teil werden kritische Schwachstellen und eine Einschätzung des allgemeinen **Sicherheitsniveaus** in einem »Management Summary« präzise zusammengefasst. Im zweiten Teil werden die jeweils gefundenen Schwachstellen detailliert erläutert und ihre Kritikalität bewertet. Dazu zählt die Art der Schwachstelle und in welcher Weise sie ausgenutzt werden kann. Komplettiert wird die Dokumentation im dritten Teil mit konkreten **Empfehlungen** zur Behebung der Schwachstellen.

OPTIONAL

Ergebnispräsentation

Auf Wunsch werden die Ergebnisse des Pentests allen Verantwortlichen präsentiert. Hierzu eignet sich eine zweiteilige Ergebnispräsentation mit »Workshop-Charakter«. Begonnen wird mit dem Briefing für die **Entscheidungsebene** mit einer Dauer von ungefähr 30 Minuten. Hier werden grundlegende Ergebnisse der Tests auf strategischer und organisatorischer Ebene besprochen. Der zweite Teil richtet sich generell an IT-Systemverantwortliche Ihres Unternehmens. An dieser Stelle besteht die Möglichkeit, tiefgreifende Fragen zu stellen und mögliche **Lösungsansätze** mit allen Beteiligten zu diskutieren.

Kontakt

+49 (0) 721 / 467 162 17
info@kuketz-security.de

Web

www.kuketz-security.de
www.kuketz-blog.de