CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Cyber Security im Unternehmens-umfeld

CloudCommand GmbH chr.schumacher@gmx.tm

Penetration Tests

Definition Penetrations Tests

“Ein Penetrationstest, kurz Pentest, beschreibt ein Verfahren, um die **aktuelle Sicherheit eines IT-Landschaft** oder einer (Web-)Anwendung **festzustellen**. Er gilt als **Sicherheitscheck** von IT-Systemen jeder Größenordnung und ist besonders für Unternehmen relevant. Für diese Sicherheitsüberprüfung bedient sich der Durchführende den Mitteln und **Methoden, die ein Hacker anwenden würde**, um in das **System einzudringen** – es zu penetrieren. Mithilfe des Pentest wird festgestellt, **wie empfindlich das System** auf derartige Angriffe reagiert.”

Phasen

Reconnaissance:

- Sammlung von Information über das Zielunternehmen

Scanning:

- Scannen des Netzwerks auf Schwachstellen und mögliche Zugänge

Vulnerability Assessment:

- Analyse und Be-/Auswertung der Scanergebnisse

Exploitation:

- Ausnutzung identifizierter Schwachstellen zum Aufzeigen des Risikos

Reporting:

- Berichterstattung anhand detaillierter Dokumentation an Auftraggeber

Arten von Penetration Tests

Externer Test:

- Zielt auf Assets des Unternehmens ab, die über das Internet erreichbar sind, wie Webanwendungen und externe Netzwerkdienste

Interner Test:

- Simuliert einen Angriff von einem Insider mit Zugang zum internen Netzwerk

Blind Test:

- Der Tester hat nur sehr begrenzte Informationen über das Ziel, ähnlich einem echten Angreifer

Arten von Penetration Tests

Doppelblind Test:

- Weder die Sicherheitsteams noch die Tester haben vorab Informationen, testet die Reaktionsfähigkeit und das Erkennungsvermögen des Sicherheitsteams

Zielgerichteter Test:

- Auch bekannt als "Red Team-Übungen", bei denen ein realistisches Szenario eines Cyberangriffs nachgestellt wird

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm