TÜV TRUST IT
TÜV AUSTRIA Group

Cyber Security

Red Teaming Assessments

Ein Red Teaming Assessment ist ein fortgeschrittener, simulierter Cyber-Angriff gegen die Infrastruktur eines Unternehmens, der die Widerstandsfähigkeit (Cyber Resilience) und Verteidigungsmechanismen gegen professionelle Cyber-Angriffe, die Advanced Persistent Threats (APT), prüft.
Die Angreifer (Red Team) versuchen mit allen möglichen verfügbaren (und ethisch vertretbaren) Mitteln Zugang zum Netzwerk des Ziels zu erhalten. Dem entgegen wirken in der Regel Verteidigungstechniken und Verteidiger (Blue Team) des Unternehmens.

Unterschied zu klassischen Penetrationstests

Red Teaming Assesments und klassische Penetrationstest haben viele Gemeinsamkeiten, beide durchlaufen diverse Phasen und simulieren (in unterschiedlichen Detailgraden die Rolle eines Angreifers), sie weisen jedoch auch wichtige Unterschiede auf. Die folgende Tabelle stellt tabellarisch einige Unterschiede dar.

Klassischer Penetrationstest	Red Teaming Assessment
• Test wird auf Seiten des Auftraggebers angekündigt, Beteiligte sind informiert	• Nur ein sehr kleiner Personenkreis ist über die Durchführung informiert (GF, CIO, Betriebsrat)
• Konkrete Zielsetzung, zum Beispiel eine Webanwendung oder ein bestimmter Server	• Keine klare Vorgabe, Ziel in der Regel Infiltration des Unternehmensnetzwerks oder Extraktion von sensitiven Informationen
• Überwiegende Nutzung von vorhandenen Penetrationstester-Frameworks	• Entwicklung von eigenem Code
• Methodik vorabgestimmt (Technik, Social Engineering, physikalischer Zugang)	• Keine Vorgaben hinsichtlich Methodik, alle (ethisch vertretbaren) Methoden erlaubt
• Kurze, auffällige, einfach zu detektierende (sind im Monitoring eindeutig zu identifizieren) Tests	• Länger anhaltende, unauffällige, schwer zu detektierenden Tests
• Durchführung zu Hauptgeschäftszeiten	• Durchführung zu allen Zeiten, auch an Wochenenden oder in der Nacht
• Tests erfolgen gegen Produktiv- oder Testsysteme	• Tests erfolgen überwiegend gegen Produktivsysteme

TÜV TRUST IT
TÜV AUSTRIA Group

Cyber Security

Phasen eines Red Teaming Asssessments

Wie auch ein klassischer Penetrationstest besteht ein Red Teaming Assessment aus mehreren Phasen:

- **Reconnaissance:** Sammlung von möglichst vielen Informationen über das Ziel (unter anderem Unternehmensstruktur, Mitarbeiter, IT-Systeme, IP-Adressen, Domains, Standorte)
- **Weaponization:** Der Angriff wird vorbereitet, beispielsweise durch Präparierung eines mit Schadsoftware ausgestattetes Office- oder PDF-Dokuments.
- **Delivery:** Der Schadcode wird in die Infrastruktur des Ziels übermittelt, zum Beispiel per Phishing-Mail, externem Datenträger oder dem Download über eine Webseite
- **Exploitation:** Nach erfolgreicher Auslieferung des Schadcodes wird dieser „getriggert“
- **Installation:** Einrichtung eines persistenten Zugangs („Backdoor“)
- **Command & Control:** Kommunikation zwischen einem Server unter der Kontrolle des Angreifers und der Schadsoftware
- **Actions on Objective:** Umsetzung des ursprünglichen Ziels (finanziell, Spionage, Zerstörung von Daten, Infiltration weiterer Ziele).

Mehrwert für den Kunden

- Etablierung und Coaching eines Blue Teams
- Simulation von realitätsnahen Cyber-Angriffen
- Messung und Wirksamkeit der Verteidigungsmechanismen
- Prüfung der Reaktion auf Seiten des Unternehmens (Blue Team)
- Intensiver Austausch zwischen dem Red Team und Blue Team zur kontinuierlichen Steigerung der Sicherheitsmaßnahmen
- Ausführlicher Bericht mit detaillierter Beschreibung zur schrittweisen Nachvollziehbarkeit des Vorgehens
- Kontinuierliche Verbesserung der IT-Sicherheit

TÜV TRUST IT GmbH
Unternehmensgruppe TÜV AUSTRIA

Waltherstraße 49–51
D-51069 Köln
Tel.: +49 (0)221 969789 - 0
Fax: +49 (0)221 969789 -12

TÜV TRUST IT
TÜV AUSTRIA GmbH

TÜV AUSTRIA-Platz 1
A-2345 Brunn am Gebirge
Tel.: +43 (0) 5 0454 - 1000
Fax: +43 (0) 5 0454 - 76245

info@tuv-austria.com
www.it-tuv.com