TÜV TRUST IT
TÜV AUSTRIA Group

Cyber Security

Assume Breach

Der Ansatz setzt voraus, dass es Angreifern gelungen ist, erste Sicherheitsvorkehrungen zu überwinden und Schadsoftware auf einen Rechner zu bekommen (z. B. per Phishing-Mail oder Datei-Download). Im nächsten Schritt wird versucht, die Schadsoftware auf dem Rechner zur Ausführung zu bringen.

Zielsetzung

- Bestandsaufnahme und Bewertung der technischen Sicherheit
- Test der Widerstandsfähigkeit gegenüber Cyber-Angriffen
- Steigerung der Resilienz
- Transparenz, wie weit ein Angreifer in der eigenen Infrastruktur kommen könnte

Vorgehensweise

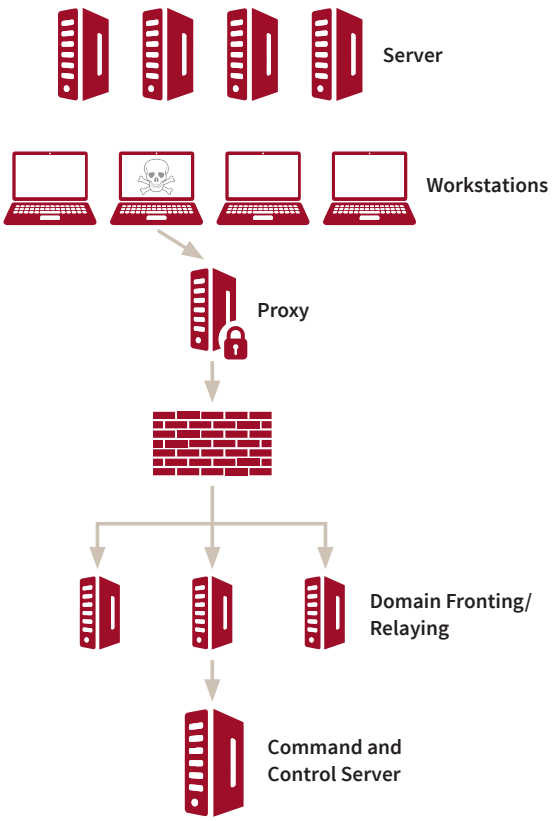
Mit dem Assume Breach Ansatz lassen sich diverse Szenarien-Abbildungen, beispielsweise:

- Test der Endpoint Detection auf die Erkennung bekannter und unbekannter Schadsoftware (statische und dynamische Analyse)
- Ermittlung der Angriffsfläche (z. B. durch Office-Makros oder PowerShell-Code)
- Netzwerkanalyse (Lateral Movement, Internal Reconaissance)
- Ausweitung der Rechte (Privilege Escalation)
- Analyse der Domäne
- Zugriff auf schützenswerte Daten wie Passwörter oder Passwort Hashes (Credential Access)
- Ransomware-Simulation (Krypto-Ransomware oder Datenexfiltration)
- Schaffung einer Persistenz
- Test der Protokollierungs- und Alarmierungsprozesse (Blue Team)

Die konkret zu testenden Szenarien werden gemeinsam abgestimmt.

In dem Assessment wird unter anderem das Command-and-Control (C2) Framework Cobalt Strike eingesetzt. Bei Cobalt Strike handelt es sich um ein Adversary Simulation Framework, welches in realen Angriffskampagnen zum Einsatz kommt. Das Assessment wird realitätsnah simuliert.

Die folgende Abbildung veranschaulicht beispielhaft ein mögliches Setup des Assessment:



Cyber Security

Jede Aktion wird zeitgenau protokolliert, sodass die Aktivitäten möglichen Events in Sicherheitsprodukten zugeordnet werden können. Zudem können die Ereignisse genutzt werden, um Detektionsmechanismen zu optimieren. Das Assessment orientiert sich vollständig am MITRE ATT&CK ATT&CK Framework, einem international anerkannten Industriestandard.

Ihr Nutzen

- Realitätsnahe Angriffssimulation (individuell auf die Kundeninfrastruktur angepasst)
- Identifizierung von Einfallstoren
- Optimierung von Detektionsmechanismen
- Identifizierung von Schwachstellen (technisch und organisatorisch)
- Purple Teaming (Training des Blue Teams)
- Erfüllung von regulatorischen Anforderungen (z. B. DORA)

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