TÜVRheinland®
Genau. Richtig.

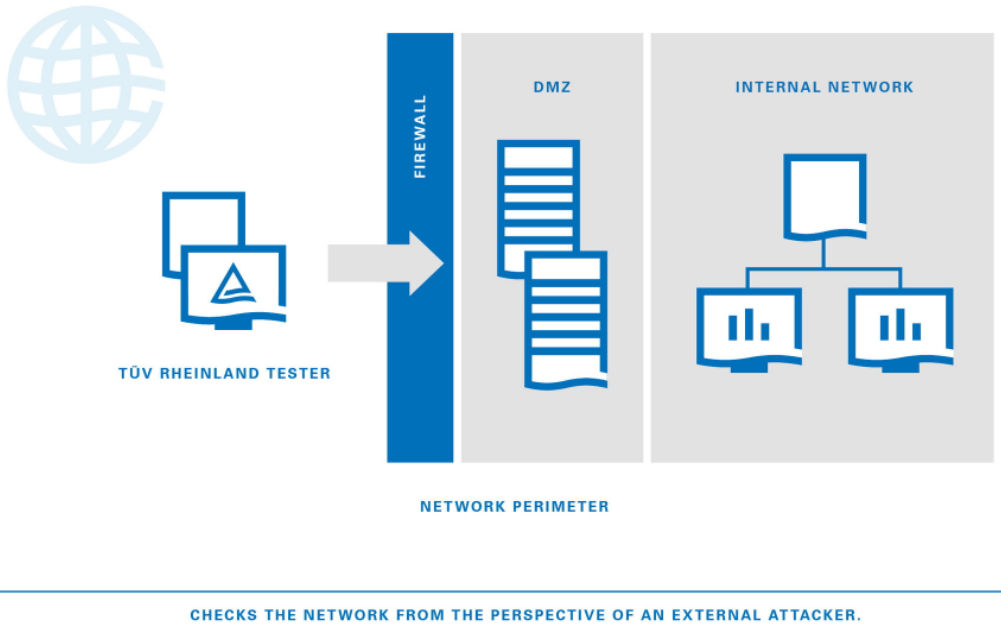
Öffentlich erreichbare Systeme

Bei einem externen Penetrationstest wird die im Geltungsbereich befindliche IT-Infrastruktur (bspw. Mailserver, VPN-Gateways oder DNS-Server) mit einer strukturieren Vorgehensweise auf Schwachstellen untersucht, die die Vertraulichkeit, Integrität oder Verfügbarkeit der Systeme negativ beeinflussen könnten. Schwachstellen werden sowohl mit Hilfe von automatischen Schwachstellenscannern als auch auf Basis von manuellen Tests und Analysen identifiziert.

Leistungsbeschreibung und Prüfumfang

In einem externen Penetrationstest werden öffentlich erreichbaren Systeme auf Schwachstellen überprüft, die ein Angreifer nutzen kann, um die Vertraulichkeit, Integrität oder Verfügbarkeit der Systeme und der darauf zu verarbeitenden Daten negativ zu beeinflussen. Ein Beispiel für eine solche Schwachstelle wäre ein FTP-Server, der einem Angreifer erlaubt, Daten unautorisiert auf dem System zu löschen.

Bei einem externen Penetrationstests, im folgenden Pentest genannt, wird also von einem Angriff von außen ausgegangen, bei dem Angreifer versuchen, Ihr Unternehmen über die aus dem Internet erreichbaren Systeme anzugreifen. Dies wird in dem folgenden Bild skizziert:



Der Umfang eines externen Pentest wird primär durch die Anzahl der öffentlich erreichbaren Systeme bestimmt, dessen Sicherheit überprüft werden sollen.

Vorgehensweise bei einem externen Penetrationstest

Der externe Pentest teilt sich insgesamt in 5 Phasen auf, die in der nachfolgenden Abbildung schematisch dargestellt sind.

Diese Phasen sind:

- Vorgespräch
- Informationssammlung
- Identifikation von Schwachstellen
- Ausnutzen von Schwachstellen
- Berichtserstellung

Im Folgenden werden die einzelnen Phasen beschrieben.

Schritt 1: Vorgespräch

Im Rahmen eines Vorgesprächs werden der Ablauf der Untersuchung sowie die aus dem Untersuchungsbereich auszunehmenden Systeme und Netzbereiche mit dem Auftraggeber abgestimmt. Falls bestimmte Systeme nicht in den Geltungsbereich der Untersuchung aufgenommen werden sollen, muss dies zu diesem Zeitpunkt mitgeteilt werden. Die betroffenen Systeme werden anschließend im Bericht als nicht geprüft vermerkt.

Natürlich teilen wir Ihnen auch mit von welchen IP-Adressen wir den Pentest durchführen, damit sie entsprechende Ausnahmen in Ihren Monitoring-Systemen für die IP-adressen definieren können.

Schritt 2: Informationssammlung

Zunächst werden die aktiven Systeme im Geltungsbereich identifiziert und untersucht, welche Dienste die Systeme bereitstellen. Hier beginnt eine erste passive Analyse, in der unter anderem die folgenden Tätigkeiten ausgeführt werden:

- Analyse von Fehlermeldungen, erreichbaren Dateien und Konfigurationen, welche während der Interaktion des TÜV Rheinland Security-Experten mit den zu prüfenden Systemen auftreten.
- Erstellung von Testbenutzern für öffentlich erreichbare Webapplikationen im Rahmen einer erlaubten öffentlichen Registrierung.
- Insgesamt verfolgt die Informationssammlung das Ziel, relevante Informationen über die Systeme im Geltungsbereich herauszufinden. Dies dient der Abschätzung der Angriffsoberfläche, um anschließend die Systeme im Geltungsbereich effizient und effektiv auf Schwachstellen überprüfen zu können.

Soll zusätzlich untersucht werden, ob es öffentlich verfügbare Informationen zu den Systemen gibt, kann optional noch das Open-Source-Intelligence-Paket hinzugebucht werden. In dem Fall werden neben direkten Quellen für die Informationsgewinnung, also Informationen, die durch die Systeme selbst preisgegeben werden, auch indirekte Quellen genutzt. Zu den indirekten Quellen gehören unter anderem die folgenden Quellen:

- DNS-Einträge
- Suchmaschinen
- Webseiten mit Passwort-Leaks

Über den Weg können beispielsweise auch Systeme mit IPv6-Adressen identifiziert werden, die zwar in den zu untersuchenden Netzbereich liegen, aber beispielsweise nicht im Vorgespräch genannt wurden.

! Um ein umfassendes Bild der eigenen Verwundbarkeit aus dem Internet zu erhalten, empfehlen wir daher das Open-Source-Intelligence-Paket.

Schritt 3: Identifizierung von Schwachstellen

Gegen die im Geltungsbereich befindlichen Systeme, die ggfs. auch durch die Open-Source-Intelligence-Phase identifiziert wurden, wird ein automatisierter Schwachstellenscan mit aktuellen Signaturen durchgeführt, um potenziell bekannte Schwachstellen schnell zu identifizieren. Parallel zu dem Schwachstellenscan werden je nach identifiziertem Dienst weitere automatische oder auch manuelle Tests durchgeführt. Bei den Tests werden unter anderem die folgenden Aspekte berücksichtigt:

- Identifizierung administrativer Schnittstellen und Dienste, welche nicht öffentlich über das Internet zugänglich sein sollten;
- Identifizierung von veralteter und unsicherer Software;
- Einsatz von Protokollen ohne oder mit mangelhafter Transportsicherheit;
- Identifizierung von Schwachstellen, die durch eine unzureichende Konfiguration der Systeme entstehen und z.B. eine Umgehung von Authentifizierungs- und/oder Autorisierungsmechanismen erlauben;
- Einsatz von schwachen Authentifizierungsverfahren oder schwachen Passwörtern.

Sofern anwendbar führt TÜV Rheinland auch eine stichprobenartige Suche nach typischen Schwachstellen von den Webapplikationen im Geltungsbereich durch, die es TÜV Rheinland ermöglichen könnten, tiefer in die Systeme im Geltungsbereich vorzudringen.

! Ein externer Pentest kann keinen umfassenden Penetrationstest einer Webapplikation ersetzen. Um ein umfassendes Bild der Verwundbarkeit von Webapplikationen zu erlangen, ist ein eigenständiger Penetrationstest erforderlich.

Schritt 4: Ausnutzung von Schwachstellen

Solange nicht anderswertig spezifiziert, nutzt TÜV Rheinland identifizierte Schwachstellen aus, um in das System und die Applikationen im Geltungsbereich einzudringen. In diesem Schritt werden beispielsweise die folgenden Schwachstellen ausgenutzt:

- Verwendung von schwachen Passwörtern;
- Verwendung von Software mit bekannten Schwachstellen;
- unzureichende Authentifizierungs- und Autorisierungsmaßnahmen;
- unzureichende Eingabevalidierungen, z. B. bei SQL-Injection oder einer Remote-Code-Execution;
- unsichere Konfiguration von Systemen.

Im Falle einer erfolgreichen Ausnutzung von einer Schwachstelle wird TÜV Rheinland zusätzliche Informationen sammeln, um herauszufinden, ob ein Angreifer in weitere Systeme vordringen kann. Dies beinhaltet eine erneute Informationssammlung und eine Identifizierung von Schwachstellen. Zusätzlich können noch folgende Aspekte untersucht werden:

- Identifizierung (und Extraktion) von nicht ausreichend geschützten Daten auf Festplatten oder im Arbeitsspeicher.
- Identifizierung (und Extraktion) unsicherer Konfigurationsdateien, welche Passwörter für andere Systeme beinhalten oder Zugang zu anderen Systemen erlauben.
- Erfassen der Informationen über weitere Systeme innerhalb des Netzes.
- Identifizieren unzureichender Berechtigungen, die beispielsweise eine Rechteausweitung (Privilege Escalation) erlauben.

Mit den neuen gesammelten Informationen und zusätzlich identifizierten Schwachstellen versucht TÜV Rheinland, weitere Systeme zu übernehmen oder in weitere Netzbereiche vorzudringen. Dies bedeutet, dass Schritte 2, 3 und 4 mehrfach wiederholt werden können, sofern das Projektbudget noch ausreichend Zeit aufweist. Inwieweit ein tieferes Vordringen in die Infrastruktur im Rahmen des externen Penetrationstests gewünscht ist, wird im Rahmen des Vorgesprächs definiert.

Schritt 5: Berichtserstellung

Nach dem externen Penetrationstest wird ein Bericht erstellt, der aus den folgenden Bestandteilen besteht:

- Management-Summary;
- Definition des Geltungsbereichs (z.B. Auflistung der Zielsysteme);
- Beschreibung der angewandten Methodik;
- Übersichtstabelle der gefundenen Schwachstellen;
- Informationen über die gefundenen Schwachstellen mit allgemeinen Empfehlungen, wie die gefundenen Schwachstellen adressiert werden können;
- Bewertung der Kritikalität des technischen Risikos auf Basis einer vierstufigen Skala: kritisch, hoch, mittel und gering;
- zusätzliche tabellarische Auflistung der gefundenen Schwachstellen (MS-Excel);

Optional haben Sie die Möglichkeit, dass wir Ihnen die Ergebnisse in einer Ergebnispräsentation darstellen und mit Ihnen gemeinsam die Ergebnisse besprechen.

TÜVRheinland®
Genau. Richtig.

Hinweise zur Bestimmung des passenden Umfangs

In dem Konfigurator ist die Anzahl der IP-Adressen anzugeben, die an Systeme vergeben sind. Nachfolgend sind ein paar Bespiele für die passende Bestimmung des Umfangs gegeben:

- In einem /24-Netz sind 254 IP-Adressen verfügbar, aber nur 5 IP-Adressen sind tatsächlich an Systeme vergeben. In dem Fall wären 5 Systeme auszuwählen.

- Ist ein System über eine IPv6-Adresse als auch eine IPv4-Adresse erreichbar, so zählt dieses System doppelt.

- Sie sind sich nicht 100% sicher, ob es noch einige unbekannte Systeme im IP-Bereich existieren, so ist es sinnvoll den nächstgrößeren Bereich zu wählen.

Abgrenzung der Dienstleistung

Hierbei stehen technische Schwachstellen im Vordergrund der Untersuchung. Es wird versucht, kosteneffizient möglichst viele Schwachstellen zu finden, weswegen wir während eines externen Penetrationstests voraussetzen, dass z. B. Intrusion-Prevention-Systeme (IPS) für unsere IP-Bereiche in den Monitoring-Mode versetzt werden, sodass beispielsweise Netzwerkscans nicht aktiv blockiert werden. Falls Sie die Fragestellung haben, ob Sie einen echten Cyberangriff erkennen, Ihre Systeme Sie effektiv schützen und auch die Prozesse eine zeitnahe Reaktion bei einem echten Angriff erlauben, helfen wir Ihnen auch gerne weiter. Hierfür bieten wir speziell darauf zugeschnittene Dienstleistungen an.

! **Eine vollständige Bewertung von der IT-Sicherheit aller Dienste und Anwendungen im Geltungsbereich wird aufgrund des Aufwands in der Regel nicht durchgeführt. Es handelt sich vielmehr um eine pragmatische Vorgehensweise, bei der mit überschaubarem Aufwand die technische Widerstandsfähigkeit der externen IT-Infrastruktur gegenüber Angriffen aus dem Internet geprüft wird. Dabei gilt in der Regel, je mehr Tage für einen Test genutzt werden, umso höher ist der Abdeckungsgrad.**