Red-Team-Engagements.

Cyber-Resilienz erhöhen und Abwehrkräfte stärken - durch realistische Simulationen fortschrittlicher Bedrohungen und professionellen gezielten Angriffen.

www.tuv.com/pentest

TÜVRheinland®
Genau. Richtig.

UNSER SERVICE

- In einer intensiven Planungsphase bestimmen Sie gemeinsam mit unseren Experten die für Sie kritischsten Angriffsvektoren realer Angreifer gemäß Ihrer Threat-Intelligence-Landschaft und auf Grundlage des TIBER-DE-Frameworks.
- Mit einer klaren Struktur für die beteiligten Stakeholders werden alle Aspekte in Bezug auf Umfang, Kommunikation, Risikomanagement und Rules-of-Engagement besprochen und festgelegt.
- Basierend auf dem Bedrohungsbericht werden gemeinsam Angriffsziele festgelegt, die sogenannten Kampagnenzielen. Anhand des Bedrohungsberichts und dem Kampagnenziel passt unser Red-Team seine Techniken und Taktiken entsprechend an und simuliert dabei Cyberkriminelle und APT-Gruppen. Jeder Angriff und jede ausgenutzte Schwachstelle wird sorgfältig vorbereitet, um die IT-Sicherheitsabteilung nicht zu alarmieren.
- Mit diesem Ansatz werden fortgeschrittene Cyberangriffe simuliert und Schwachstellen in den Überwachungssystemen, Erkennungsregeln und -verfahren aufgedeckt.
- In einem strukturierten und detaillierten Bericht erläutert unser Red-Team Schritt für Schritt, wie es die Kampagnen durchgeführt hat, welche Entscheidungen getroffen wurden und gibt schließlich einen Einblick in die positiven Aspekte sowie in die Optimierungspotentiale.

UNSERE KOMPETENZ

- Eines der größten Cyber-Testing-Services-Teams Deutschlands mit Praxiserfahrung aus ca. 1.000 Penetrationstests pro Jahr in allen denkbaren IT-Sicherheitsfeldern. Unsere OSCP, OSCE, OSCE3, CRTO oder äquivalentzertifizierte Red-Teamer nutzen Ihre umfassenden Kenntnisse, um der hohen Kompetenz globaler Angreifergruppen gerecht zu werden.
- Als einer der führenden unabhängigen Anbieter für Cybersecurity weltweit verfügen wir über Teams an allen wichtigen Standorten – u.a. in Europa, den USA, China, Indien, Singapur und Oman.

IHRE VORTEILE

- Ganzheitliche Betrachtung Ihrer IT-Landschaft: Aus der Perspektive hochqualifizierter und bestens ausgestatteter Angreifer durch eine Attacke unter realen Bedingungen. Maßgeschneiderte Angriffsszenarien und Ausgangssituationen, die Ihren Bedürfnissen entsprechen.
- In unserem ausführlichen Bericht stellen wir die genutzten Angriffsvektoren vor und zeigen auf, wo Schwachstellen in den organisatorischen Abläufen, in den IT-Systemen und in der User-Awareness zu finden sind. Natürlich geben wir auch Empfehlungen, wie diese behoben werden können. Seien Sie den Cyber-Kriminellen einen Schritt voraus!
- Falls Sie von der DORA betroffen sind, erfüllen sie mit diesem Test die Anforderungen an das Threat-Led-Penetration-Testing (TLPT).

Elemente eines Red-Team-Engagements

BEDROHUNGSDESIGN

Ist ein Threat-Intelligence (TI)-Report nicht vorhanden? Je nachdem welches typische Angriffsschema zu Ihrem Unternehmen passt, gestalten wir gemeinsam mit Ihnen die Angriffsszenarien: Ist es ein Ziel, Entwicklungsdaten zu entwenden oder Zugriff auf ein bestimmtes System zu erlangen? Wird die IT-Abteilung vorab eingeweiht? Wird der Angriff als „Assumed-Breach"-Szenario durchgeführt?

ANGRIFFSPHASE

TÜV Rheinland nutzt in einem klassischen Red-Team-Engagement alle zur Verfügung stehenden Angriffsmethoden. Mit einem „Black-Team"-Szenario kann sogar ein noch höherer Grad an Realismus erzielt werden: In diesem Fall wird lediglich ein grober Zeitrahmen – z.B. ein halbes Jahr – abgesteckt, in dem der Angriff erfolgen soll. Hierdurch wird der IT-Sicherheitsabteilung jede Möglichkeit zur Vorbereitung genommen.

Ist vor allem die Sicherheit von Daten im internen Netz zu prüfen, kann in einem sogenannten „Assumed-Breach"-Szenario ein Brückenkopf im Unternehmensnetz platziert werden. Über diesen hat TÜV Rheinland direkten sicheren Zugang zum internen Netzwerk und versucht die definierten Ziele zu erreichen. Eine aufwendige Suche nach einem Zugang zum internen Netz entfällt, was den finanziellen Aufwand erheblich reduzieren kann. Auch andere Teilziele können als eigenständiges Projekt umgesetzt werden.

TÜV Rheinland hält auf Wunsch engen Kontakt zu Ihrem Projektverantwortlichen und spricht anzugreifende Ziele und weitere Schritte mit diesem ab – eine effektive und reibungslose Durchführung ist garantiert.

REPORTING

Aufgefundene relevante Sicherheitslücken werden klassifiziert, in den Gesamtkontext eines Red-Team-Engagements eingeordnet und in Form eines detaillierten TÜV Rheinland Prüfberichts übergeben. Dabei zeigen wir auf, welchen Schaden ein erfolgreicher Angreifer in Ihrem Unternehmen verursachen könnte, und wir schlagen Ihnen geeignete Gegenmaßnahmen vor.
Mögliche IOCs und Änderungen an den betroffenen Systemen/Konfigurationen werden sorgfältig dokumentiert und gemeldet, damit sie am Ende des Engagements rückgängig gemacht werden können.

Jetzt unverbindlich anfragen FRAGEN SIE UNS!

TÜV Rheinland i-sec GmbH
Am Grauen Stein · 51105 Köln
Tel. +49 221 806-0
cybersecurity@tuv.com
www.tuv.com/pentest

TÜVRheinland®
Genau. Richtig.