Red-Team-Engagements.

IT-Sicherheit stärken – mit realistischen Simulationen Advanced Persistent Threats und professionellen Angriffen vorbeugen.

www.tuv.com/informationssicherheit

TÜVRheinland®
Genau. Richtig.

UNSER SERVICE

- In einer intensiven Planungsphase bestimmen Sie gemeinsam mit unseren Experten die für Sie kritischsten Angriffsvektoren realer Angreifer – in Bezug auf Ihre ganzheitliche IT-Umgebung und auf Ihr Personal.
- In der Umsetzungsphase simuliert unser Red-Team Angriffe von Cyber-Kriminellen oder APT-Gruppen. Innerhalb des zuvor festgelegten Rahmens kommen verschiedene Techniken zum Einsatz: von Angriffen auf die technische Infrastruktur und erreichbare Dienste über Spear-Phishing-Kampagnen bis hin zu physikalischem Zugriff auf eines Ihrer Gebäude. Ist ein Zugriff erfolgreich, versucht das Red-Team die gesetzten Ziele, z.B. den Diebstahl von Entwicklungsdaten, zu erreichen, ohne die IT-Sicherheitsabteilung zu alarmieren. So werden Sicherheitsprobleme sichtbar, die bei normalen Penetrationstests nur selten zu Tage treten.
- Wir empfehlen Ihnen abschließend ganzheitliche und strategische Verbesserungen für Ihre IT-Sicherheit und zeigen auf, wie Sie kritische Sicherheitslücken beheben.

IHRE VORTEILE

- Ganzheitliche Betrachtung Ihrer IT-Landschaft: Aus der Perspektive hoch qualifizierter und bestens ausgestatteter Angreifer durch eine Attacke unter realen Bedingungen. Sie entscheiden vorab, wie weit TÜV Rheinland gehen darf und soll.
- Ausführlicher Bericht: Welche Angriffsvektoren wurden benutzt? Wo sind Schwachstellen in den organisatorischen Abläufen, in den IT-Systemen und in der User-Awareness? Wie können Sie diese beheben?
- TÜV Rheinland zeigt auf, ob bestehende IT-Sicherheitslösungen und deren Konfigurationen die Sicherheitsanforderungen erfüllen und wo Optimierungspotentiale liegen.

UNSERE KOMPETENZ

- Eines der größten deutschsprachigen Security-Testing-Services-Teams profitiert von seinen Erfahrungen aus ca. 1.000 Penetrationstests pro Jahr in allen denkbaren IT-Sicherheitsfeldern: IoT, Office-Netze in Konzerngröße oder Applikationen. In unseren Red-Team-Engagements nutzen wir diese 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.

Elemente eines Red-Team-Engagements

BEDROHUNGSDESIGN

Je nachdem welches typische Angriffsschema zu Ihrem Unternehmen passt, gestalten wir gemeinsam mit Ihnen das Angriffszenario: 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 „Expected-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 „Expected-Breach"-Szenario ein Brückenkopf im Unternehmensnetz platziert werden. Über diesen hat TÜV Rheinland direkten 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 eingeordnet und in Form eines 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.

Fragen Sie uns!

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

www.tuv.com/informationssicherheit

TÜVRheinland®
Genau. Richtig.