
r tec
cyber security
Sicherheitsanalysen
+ Pentests
Licht ins Dunkel
bringen.

Sicherheitsanalysen und Pentests

Wie sicher sind Sie?

Wir testen die Wehrhaftigkeit Ihrer Sicherheitslandschaft gegen die unterschiedlichsten Angriffe – sowohl gegen externe als auch interne Attacken. Geprüft wird in der Cloud, in Anwendungen, Rechenzentren oder auch kritischen Infrastrukturen. Dabei finden wir Schwachstellen, die andere nicht finden: So erlangen wir beispielsweise bei über 90 Prozent unserer Pentests die volle Kontrolle über das gesamte Unternehmensnetzwerk des Kunden. Kürzeste Zeit vom Start bis zur Systemübernahme: 5 Minuten.

Darüber hinaus sind 80 Prozent der von uns untersuchten Webanwendungen bei Kunden für mindestens eine hoch kritische Schwachstelle anfällig. Unsere Erfahrung hat gezeigt, dass bei unseren Phishing-Angriffen im Schnitt 50 Prozent der Empfänger einen Link zu einer gefälschten Webseite öffnen. Von diesen 50 Prozent geben im Schnitt 80 bis 90 Prozent der Personen Ihre Zugangsdaten auf der gefälschten Webanwendung ein.

Im Anschluss entwickeln wir gemeinsam mit Ihnen im Rahmen unserer Sicherheitsanalysen eine individuelle Strategie und Handlungsempfehlungen zur Erhöhung des aktuellen Sicherheitsniveaus – und zwar ohne die bestehenden Geschäftsprozesse zu gefährden. Sie erhalten Erkenntnisse über kritische Schwachstellen, ein tiefes Verständnis für die Vernetzung Ihrer Infrastruktur und für schützenswerte Geschäftsabläufe.

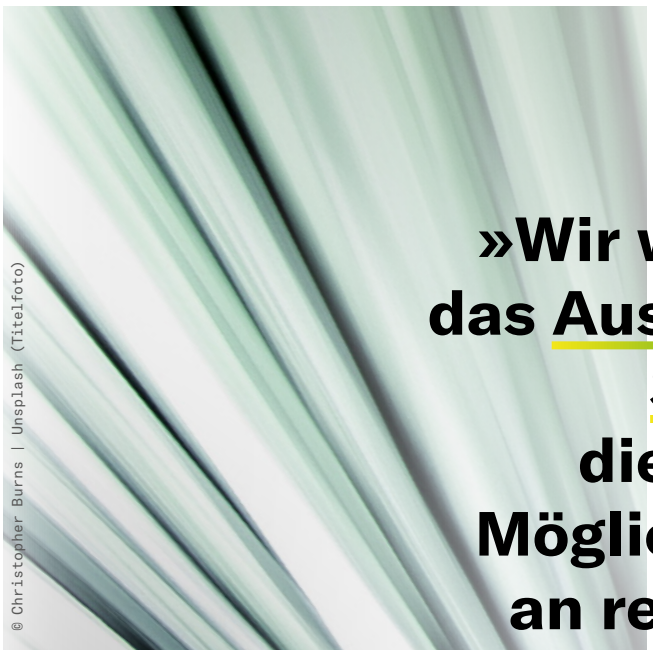
Nach der Durchführung der Pentests bekommen Sie von uns eine Zusammenfassung für Führungskräfte, einen detaillierten, technischen Bericht für Ihre IT-Abteilung, eine faktenbasierte Risikoanalyse entdeckter Sicherheitslücken im Kontext Ihrer Unternehmensumwelt sowie Empfehlungen für dringende Maßnahmen für eine langfristige Verbesserung des Reifegrads Ihrer IT-Sicherheit. Auf diese Weise sorgen wir dafür, dass Ihre Verfügbarkeit erhalten bleibt und Sie stets die Kontrolle haben.

Tief. Kontrolliert. Erfolgreich.

Mit mehr als 20 Jahren Erfahrung finden wir Schwachstellen, die andere nicht finden. Anschließend können wir Ihnen individuelle Maßnahmenempfehlungen liefern.

- Bei über 90 % der Pentests erlangen wir die volle Kontrolle über das gesamte Unternehmensnetzwerk
- Bei einem Passwort-Audit erhalten wir im Schnitt zwischen 50 und 95 % aller in einem Unternehmen genutzten Klartextpasswörter
- Kürzeste Zeit vom Start bis zur Systemübernahme: 5 Minuten

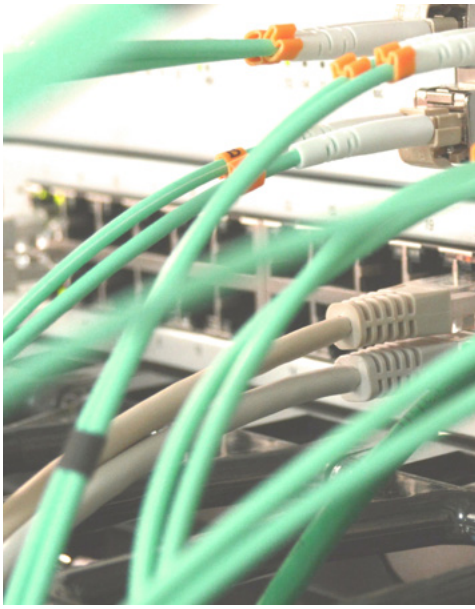
© Sharon McCutcheon | Unsplash



© Christopher Burns | Unsplash (Titelfoto)

»Wir waren überrascht über das Ausmaß der vorhandenen Sicherheitslücken und die daraus entstehenden Möglichkeiten für Angreifer, an relevante Informationen und Daten heranzukommen und kritische Systeme zu übernehmen. Wir wissen nun, welche insbesondere auch strukturellen Verbesserungen wir vornehmen müssen.«

Pentest Industrie, Kundenzitat



Ihr Nutzen

- Identifizierung physischer, menschlicher sowie hard- und softwarebedingter Schwachstellen
- Stets die Kontrolle behalten: Jeder Test kann sofort über das r-tec Emergency Stop System abgebrochen werden
- Gewinn eines praxisnahen Verständnisses des Risikos für Ihr Unternehmen
- Adressierung und Behebung aller identifizierten Sicherheitsschwachstellen

Unsere Vorgehensweise

01 Vorbereitung

In einem Kick-off-Termin vereinbaren wir mit Ihnen gemeinsam die Rahmenbedingungen für den Pentest.

02 Informationsbeschaffung

Zu den gemeinsam definierten Zielen bzw. Systemen und Anwendungen sammeln wir Informationen aus unterschiedlichen Quellen durch passive sowie aktive Verfahren.

03 Penetration

Die Eindringversuche erfolgen dann auf Basis der ermittelten Informationen sowie einer individuellen Angriffsmodellierung, um Schwachstellen und Fehlkonfigurationen aufzudecken und deren Gefahrenpotenzial zu ermitteln.

04 Bericht

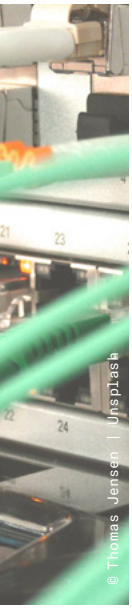
Sie erhalten eine umfassende Dokumentation der identifizierten Schwachstellen mit einer individuellen Risikobewertung und einem priorisierten Maßnahmenplan.

05 Präsentation

Die Ergebnisse des Penetrationstests werden durch r-tec vorgestellt. Offene Fragen werden diskutiert und die nächsten Schritte bestimmt.

06 Reaudit

Nach Umsetzung der empfohlenen Maßnahmen wird die Wirksamkeit der Behebung durch r-tec überprüft.



Unsere Pentests im Überblick

RED TEAM

Wir simulieren einen echten Angriff ohne oder mit einem vordefinierten Umfang und ohne vorherige Information der IT–Abteilungen, sodass wir Ihr Unternehmen aus dem gleichen Blickwinkel sehen wie ein Hacker. Gegenstand der Überprüfung sind die technischen Schutzmaßnahmen für ihre Systeme und Daten, die laufende Überwachung, Ihre Prozessabläufe bei der Angriffserkennung und die Sensibilität und das Know-how Ihrer Mitarbeiter.

INTERNE SICHERHEITSANALYSEN

Wir nehmen hier die Sicht eines in Ihrem Netzwerk befindlichen Täters ein und prüfen die Sicherheit interner Systeme, Dienste und Applikationen gegenüber Angriffen und nicht regelkonformer Nutzung.

Die Sicherheitsanalysen können für das komplette interne Netz, für bestimmte Anwendungsumgebungen, definierte Benutzerkonten oder auch kritische Anwendungen wie SAP oder Datenbanken durchgeführt werden.

EXTERNE SICHERHEITSANALYSEN UND PENTESTS

Wir testen die Sicherheit von Netzwerken, Systemen und Applikationen, die aus dem Internet erreichbar sind, aus der Sicht eines externen Angreifers. Dies ist für Sie die unverzichtbare Grundlage einer umfassenden Risikobetrachtung.

WEBANWENDUNG

Webapplikationen, Content-Management-Systeme und Portallösungen, auf denen häufig kritische Daten liegen und deren Verfügbarkeit direkte Auswirkungen auf digitale Geschäftsprozesse und -modelle hat, sind oft der verwundbarste Teil der IT-Infrastruktur.

Wir prüfen im Rahmen der Sicherheitsanalyse diese Webapplikationen, Webservices, CMS-Systeme oder Portallösungen wie auch die zugrunde liegende Infrastruktur (Web-, Applikations- oder Datenbankserver) auf Schwachstellen. Ziel ist es, gerade in diesen kritischen Bereichen die Sicherheit der Systeme und der Daten zu verbessern.

MOBILE APPS

Durch eine umfassende Analyse von mobilen Apps im Kontext des Betriebssystems erhalten Sie ein Verständnis für Risiken durch mobile Anwendungen des Unternehmens oder Dienst-Smartphones.

INTERNET OF THINGS

Wir prüfen die eingebettete Firmware auf Verwundbarkeit und geben Ihnen eine Beurteilung des Sicherheitsstatus dieses wichtigsten Bindegliedes zwischen Hard- und Software. Übernimmt ein Angreifer die Kontrolle, sind alle nachgelagerten Schutzmaßnahmen wirkungslos.

ICS/SCADA

Gerade IP-fähige Automaten, Steuer- und Kontrollsysteme (z. B. SCADA/ICS in Energiewirtschaft, Prozesstechnik, Medizin und Handel) sind besonders risikobehaftet und werden in Sicherheitsbetrachtungen häufig nicht mit einbezogen. Wir testen diese auf Zugriffsmöglichkeiten und Sicherheitslücken und zeigen die Schwachstellen in Industrieumgebungen auf, bevor sie durch Angreifer ausgenutzt werden.

WLAN-AUDIT

Wir nehmen eine Sicherheitsprüfung und -bewertung vorhandener WLAN-, Bluetooth- und Funkperipherie-Netze vor, inklusive einer Ermittlung der Netzabdeckungen. So liefern wir Informationen und die Grundlage für das Verständnis der Sicherheit der Datenübertragung in lokalen Funknetzwerken, kabellosen Tastaturen und Mäusen.

STEUERUNGS- UND LEITNETZE

Zur Analyse der Sicherheitsmaßnahmen von Steuerungs- und Leitnetzen führen wir verschiedene Pentest-Szenarien durch (physischer Zutritt, Social Engineering, Pentests Perimeter und Leitnetz, Kompromittierung Office-Client). Sie erhalten individuelle Maßnahmenempfehlungen zur Absicherung Ihrer Steuerungs- und Leitnetze. Im besten Fall führen wir die Szenarien in einer redundanten Umgebung durch, sodass keine Produktivsysteme gestört werden.

© Sharon McCutcheon | Unsplash

r-tec cyber security

Die r-tec IT Security GmbH, mit Sitz in Wuppertal, wurde 1996 von Dr. Stefan Rummenhöller gegründet. Als Wegbereiter und Wegbegleiter schaffen wir für unsere Kunden sichere Räume für die Entwicklung ihrer Organisationen und die Verwirklichung ihrer Visionen. Unsere Kunden aus dem gehobenen Mittelstand, Konzerne, kommunale Rechenzentren und Bundes- oder Landesbehörden vertrauen seit über 20 Jahren auf unsere hoch spezialisierten Experten.

Als Strategic Supplier für Cyber Security Services schützen wir die Werte unserer Kunden vor Bedrohungen und begleiten ihr Security Management von der Initiierung über die Einführung bis zum Betrieb auf allen Ebenen.

Wir leben Regeltreue, höchste Qualitätsstandards und Servicementalität. Unser Unternehmen haben wir nach den Strukturen und Richtlinien der DIN ISO 9001:2015 und der ITIL aufgebaut. Wir sind nach ISO 27001 zertifiziert.

r-tec IT Security GmbH | Hatzfelder Str. 167 | 42281 Wuppertal
www.r-tec.net | +49 (0) 202 31767–100