Herausforderungen und Lösungen im Detail.

IDENTITÄTSMISSBRAUCH

Sind Sie sicher, dass die Richtigen Zugriff haben?

Identity & Access Management für die Cloud

- Multi-Faktor-Authentifizierung
- Directory Federation und Single Sign-on
- Conditional Access
- Mobile-Device-Management
- Endgerätesicherheit

SHADOW IT

Haben Sie noch die Kontrolle?

Cloud Usage Assessment und Cloud Governance

- Cloudnutzungsanalyse
- Cloud-Strategie, -Richtlinien und -Konzepte
- Cloud-Governance-Lösungen (CASB) zur Umsetzung der Richtlinien

DATENABFLUSS

Wissen Sie, wer Ihre kritischen Daten nutzt?

Data Loss Prevention in der Cloud

- Datenverschlüsselung, on-premise, in-transit und in-cloud
- Datenklassifizierung
- Digital Rights Management
- DLP-Gateways

UMGEHUNG VON KONTROLLMASSNAHMEN

Wer schützt Sie in der Cloud?

Umsetzung der Detect-Schicht in der Cloud

- Cloud-SIEM-Integration
- UBA / Anomalieerkennung

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

r-tec cyber security

CLOUD-NUTZUNG

Nicht ohne Security

Cloudnutzung.

Der Weg in die Cloud

Unternehmen setzen heute auf eine Vielzahl von Cloud-Lösungen, sei es für einzelne Anwendungen (SaaS) oder die Auslagerung kompletter Infrastruktur (PaaS, IaaS). Die Vorteile liegen auf der Hand: Es wird weniger Kapital in Hardware und Software gebunden, obwohl gleichzeitig die Infrastruktur jederzeit flexibel an neue Anforderungen angepasst werden kann. Die Bereitstellung und der Betrieb der IT-Systeme werden an Spezialisten übertragen. Die Unternehmen können sich auf ihr Kerngeschäft konzentrieren.

Der Datenzugriff kann mobil von unterschiedlichen Orten und unterschiedlichen Personengruppen erfolgen, Mitarbeiterinnen und Mitarbeiter können flexibel von jedem Ort der Welt arbeiten.

Und wie sicher ist die Cloud?

Die Cloud an sich bietet Ihnen nicht automatisch die erforderliche Sicherheit. Auch Cloud-Sicherheit erfordert den Schutz der Daten, Anwendungen und Infrastrukturen im Rahmen des Cloud-Computings. Viele Herausforderungen für die Sicherheit von Cloud-Umgebungen sind daher mit denen der lokalen IT-Architektur identisch. Sicherheitslücken, Datenverluste und Datenlecks, Missbrauch von Zugangsdaten, Angriffe auf Verfügbarkeit, Sabotage und Spionage betreffen sowohl die traditionellen IT- als auch Cloud-Systeme. Sicherheit in der Cloud ist deshalb ohne effizienten Schutz nicht zu gewährleisten. Gleichzeitig unterscheiden sich die Möglichkeiten zur Integration von Sicherheitslösungen in Cloud-Umgebungen deutlich von denen der lokalen IT. Umfassender Schutz lässt sich nur mit einem ganzheitlichen Ansatz erreichen, der alle Blickwinkel der Informationssicherheit berücksichtigt.

Mit der Zahl der Cloud-Anwendungen steigt darüber hinaus auch die Anzahl der unabhängigen Cloud-Provider, deren Reifegrad im Hinblick auf Sicherheit sehr unterschiedlich ausgeprägt ist. Entscheidungen für eine Cloud-Anwendung treffen jedoch häufig die Business-Bereiche autark, ohne Einbindung der IT. In der Folge fehlt es an einer übergeordneten Cloud-Strategie und einem Cloud-Sicherheitskonzept.

Nicht ohne Sicherheitskonzept

Die Nutzer eines Cloud-Dienstes sind unterschiedlichen Bedrohungen ausgesetzt. Zum einen besteht immer die Gefahr der externen Bedrohungen auf die Cloud-Infrastruktur und zum anderen ist auch der Einführungsprozess einer Vielzahl von Bedrohungen ausgesetzt.

Bedrohungen der Cloud-Infrastruktur

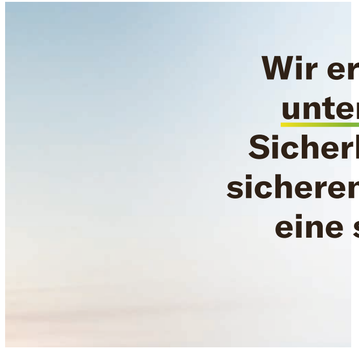
- Datenverlust bzw. Informationsabfluss
- Ausfall der Internet- oder Netzwerkverbindung, der den Zugriff auf Daten bzw. Anwendungen unmöglich macht
- Denial-of-Service-Angriffe auf Cloud-Anbieter, die sicher noch zunehmen werden
- Fehler in der Cloud-Administration durch den Anbieter
- Hohe Abhängigkeit vom Cloud-Provider – Daten können nur noch schwierig migriert werden

Bedrohungen bei der Nutzung von Cloud-Diensten

- Identitätsdiebstahl bzw. Missbrauch von Accounts
- Datendiebstahl/Datenüberwachung auf dem Übertragungsweg und in Shared-Cloud-Umgebungen, z. B. durch Provider, andere Kunden, Behörden
- Ungenügende Sicherheit der zugreifenden Endgeräte
- Verletzung geltender Vorgaben und Richtlinien (z. B. Datenschutzanforderungen) oder Kundenanforderungen

Bedrohungen bei der Einführung von Cloud-Diensten

- Mangelhafter Einführungsprozess: Kritische Elemente werden übersehen, etablierte Sicherheitskontrollen entfallen, neue Risiken entstehen
- Vielzahl an Cloud-Anwendungen und damit Vertragspartnern mit jeweils individuellen Bedrohungen und Risiken
- Abhängigkeit vom Cloud-Anbieter, keine schnellen Fallback-Möglichkeiten auf lokale Lösungen oder alternative Provider
- Unkontrollierter Einsatz von Unterauftragnehmern gerade bei kleineren Cloud-Anbietern (z. B. Administration oder Back-up von Daten)
- Fehlender Notfallplan – »Die Cloud ist doch immer da!«



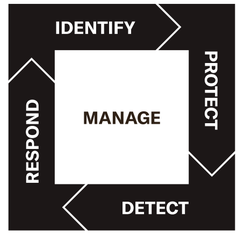
Wir erarbeiten mit Ihnen ein unternehmensspezifisches Sicherheitskonzept für einen sicheren Weg in die Cloud und eine sichere Cloudnutzung.

Unsere Vorgehensweise

- Entwicklung einer Cloud-Strategie, Ableitung von Cloud-Richtlinien und -Konzepten für einzelne Anwendungsfälle
- Erstellung von Expertisen für einzelne Cloud-Services, z. B. Office365, Dropbox
- normkonforme Cloud-Nutzung, im Hinblick auf gängige Anforderungen, insbesondere KRITIS, 27001, TISAX
- Architekturreview der Cloud-Anbindung
- Absicherung von SaaS-Cloudanwendungen (SaaS), z. B. über Zugangskontrollen, übergreifende Multifaktor-Authentifikation und Kontrolle der Nutzung
- Absicherung von Cloud-Infrastrukturen (IaaS) und Cloud-Plattformen (PaaS) mit Cloud-integrierten Security-Lösungen (Firewall, Applikationskontrolle, Verschlüsselung, Authentifikation)
- Absicherung der zugreifenden Endgeräte und der Datenübertragung in die Cloud
- Überwachung der Cloud-Anwendungen auf Anomalien, Angriffe und kritische Ereignisse

Unser Ansatz.

Mit unserem Cyber Security Framework stellen wir Ihnen den aktuellen Standard zur Bewältigung Ihrer Cyber Security Herausforderungen vor. Wir bestimmen Stärken und Schwächen und liefern Ihnen die Services für Ihre Strategie und Sicherheitsarchitektur.



INDUSTRIE 4.0

CLOUD

DATACENTER

ENDPOINT

IDENTIFY_ Identifizierung der Bedrohungen und geschäftskritischer Anwendungen, Systeme und Daten. **PROTECT_** Design und Implementierung von Schutzmaßnahmen. **DETECT_** Überwachung zur frühzeitigen Erkennung drohender Vorfälle. **RESPOND_** Vorfallsanalyse, Angriffsabwehr, Wiederherstellung des Betriebs. **MANAGE_** Governance, Risk and Compliance umfassen alle Bausteine für ein erfolgreiches Cyber Security Management.

Warum r-tec.

Unsere Kernkompetenz

- Technisch voraus, menschlich auf Augenhöhe
- Passgenaue Servicelösungen, kurze Reaktionszeiten, schnelle Terminierung, direkter Expertenkontakt
- Schnelle Hilfe im Angriffsfall
- Spezialisiertes Cyber Security Unternehmen mit ausgeprägter Service-Struktur
- 20 Jahre Erfahrung in Konzeption, Aufbau und Betrieb von Cyber Security Lösungen
- Zertifiziert nach ISO 9001 und ISO 27001

Herausforderungen und Lösungen im Detail.

MALWARE

Wie stark ist Ihr Immunsystem?

Malwareschutz

- Architekturreview Malwareschutz und Ransomware
- Endpoint Next Generation (EDR, Threat Intelligence, Threat Emulation)
- Device und Application Control
- Cyber-Threat-Analyse

SICHERHEITSLÜCKEN

Kennen Sie Ihre Verwundbarkeiten?

Schwachstellenmanagement

- Security Ratings
- Vulnerability Scan
- Threat Information Service
- Remediation Manager
- Pentest

IDENTITÄTSMISSBRAUCH

Sind Sie sicher, dass die Richtigen Zugriff haben?

Identity & Access Management

- Multi-Faktor-Authentifizierung
- Directory Federation und Single Sign-on
- Mobile Device Management
- Zero-Trust-Architektur
- Passwortmanagement

DATENVERLUST UND SPIONAGE

Haben Sie Ihre Daten unter Kontrolle?

Datensicherheit

- Datenklassifizierung
- DLP am Perimeter und in der Cloud
- Digital Rights Management
- Datei- und Geräteverschlüsselung
- Secure Data Exchange

SICHERHEITSLÜCKE MENSCH

Kennen Sie jeden Enkeltrick?

Security Awareness

- Social-Engineering-Kampagnen
- Schulungen und Live-Hacking
- Awareness-Plattform
- Vorgaben- und Richtlinienerstellung

r-tec cyber security

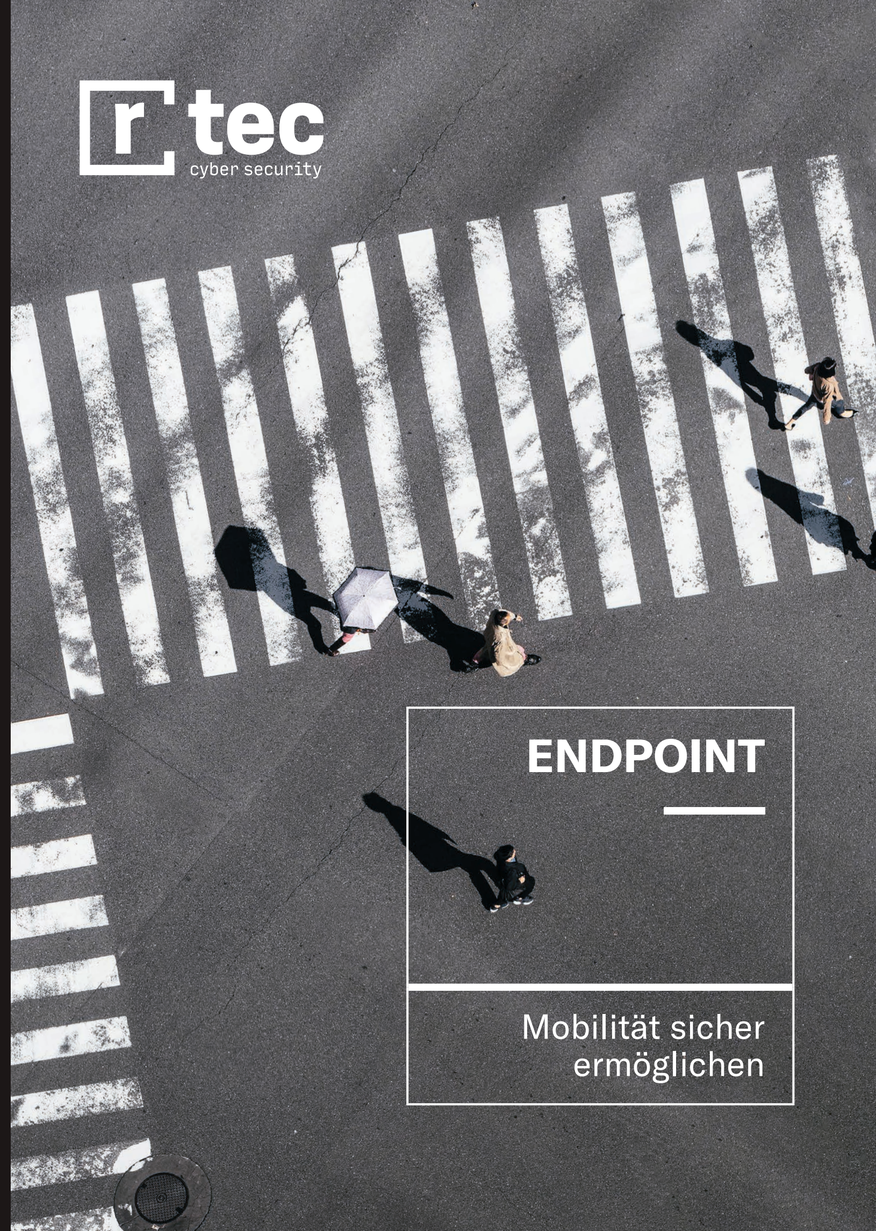
Die r-tec IT Security GmbH, mit Sitz in Wuppertal, wurde 1996 von Dr. Stefan Rummenhöller gegründet. Als Wegbereiter und Wegbegleiter schaffen wir für unsere Kunden sichere Räume für die Entwicklung ihrer Organisationen und die Verwirklichung ihrer Visionen. Unsere Kunden aus dem gehobenen Mittelstand, 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

r-tec cyber security



ENDPOINT

Mobilität sicher ermöglichen

Endpoint.

Die Realität

Tausende Geräte in hundert verschiedenen Modellen mit Dutzenden unterschiedlichen Betriebssystemen, Server, PCs, Notebooks, Smartphones, Tablets, Barcode-Scanner, Point-of-Sales Terminals, das ist in vielen Unternehmen Alltag und mit der boomenden IoT-Welt wird die Anzahl weiter rapide wachsen. All diese Endpoints sind die zentralen Einfallstore für Angriffe auf die IT-Infrastruktur von Institutionen und Unternehmen und müssen verwaltet, kontrolliert und richtig abgesichert werden.

Die Zunahme an Ransomeware-Angriffen, Phishing-Mails, APT oder gezielter Industriespionage zeigt dies drastisch. Endpoint-Schutz muss jedoch mehr können, als Viren und Malware zu erkennen. Er muss offline und online Schutz bieten, Bedrohungen erkennen und schnelle Gegenmaßnahmen ermöglichen. Eine Strategie und ein unternehmensspezifisches Sicherheitskonzept sind unerlässlich.


© Claudia Kempf

Mobile Endgeräte bieten höchste Flexibilität in der Arbeitswelt und stellen gleichzeitig eines der größten Risiken für Datenverlust und Malwarevorfälle dar.

Die Lösung – Endpoint Data Protection

Der Schutz der Endgeräte lässt sich nicht allein durch technische Schutzmaßnahmen realisieren. Umfassender Schutz erfordert einen ganzheitlichen Ansatz, der alle Blickwinkel der Informationssicherheit berücksichtigt.

Im ersten Schritt gilt es, die möglichen Angriffstore und typischen Angriffswege sowie die businesskritischen Anwendungen, Systeme und Daten, schlicht die unternehmensspezifischen Werte, zu identifizieren, die im Fokus der Angreifer stehen. Darauf aufbauend muss ein unternehmensspezifisches Sicherheitskonzept entwickelt werden, das die Punkte

- Endpoint Management & Protection
- Endpoint Detection & Response
- Mobile Security
- Faktor Mensch: Schulung und Sensibilisierung umfasst.

Und ... wirksame Endpoint-Security sollte immer branchenspezifisch sein.

Wir erarbeiten mit Ihnen ein unternehmens- und branchenspezifisches Sicherheitskonzept für Ihre Endpoints.


© Claudia Kempf

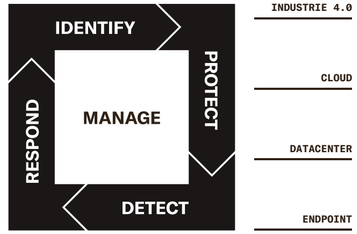
Dr. Stefan Rummenhöller, Geschäftsführer und Firmengründer

Unsere Vorgehensweise

- Analyse des Ist- Zustandes und Erstellung eines Cyber Security Konzeptes passend zum jeweiligen Industrieumfeld und der bereits vorhandenen AnlagenSicherheitsarchitektur
- Aufbau der für das Industrieumfeld, Anlagen, Steuerungen und Leitsysteme passenden Schutzmaßnahmen
- Überwachung der Anlagen-Netze und aller verbundenen Systeme auf sicherheitsrelevante Hinweise und Ereignisse
- Konzeption für den Umgang mit Vorfällen, Datensicherungskonzept, erprobtes Notfallkonzept

Unser Ansatz.

Mit unserem Cyber Security Framework stellen wir Ihnen den aktuellen Standard zur Bewältigung Ihrer Cyber Security Herausforderungen vor. Wir bestimmen Stärken und Schwächen und liefern Ihnen die Services für Ihre Strategie und Sicherheitsarchitektur.



IDENTIFY_ Identifizierung der Bedrohungen und geschäftskritischer Anwendungen, Systeme und Daten. **PROTECT_** Design und Implementierung von Schutzmaßnahmen. **DETECT_** Überwachung zur frühzeitigen Erkennung drohender Vorfälle. **RESPOND_** Vorfallsanalyse, Angriffsabwehr, Wiederherstellung des Betriebs. **MANAGE_** Governance, Risk and Compliance umfassen alle Bausteine für ein erfolgreiches Cyber Security Management.


© Pavel Ivets | Unsplash

Warum r-tec.

Unsere Kernkompetenz

- Technisch voraus, menschlich auf Augenhöhe
- Passgenaue Servicelösungen, kurze Reaktionszeiten, schnelle Terminierung, direkter Expertenkontakt
- Schnelle Hilfe im Angriffsfall
- Spezialisiertes Cyber Security Unternehmen mit ausgeprägter Service-Struktur
- 20 Jahre Erfahrung in Konzeption, Aufbau und Betrieb von Cyber Security Lösungen
- Zertifiziert nach ISO 9001 und ISO 27001

For your objectives.

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.

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

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

© Thomas Jensen | Unsplash

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.