r tec
cyber security

DATA-CENTER

Infrastruktur kosteneffizient und sicher betreiben

Datacenter.

Neue Strukturen

Das traditionelle Rechenzentrum hat ausgedient. Software Defined Infrastructure, Cloud und Edge Computing stehen auf der Agenda deutscher IT-Entscheider. Datenverarbeitungsprozesse finden heute nicht allein im Datacenter statt, hinzu kommen die zwischen den vernetzten Geräten im Internet of Things und dem Rechenzentrum ablaufenden Prozesse. Software Defined Infrastructure ersetzt wiederum die Abbildung der realen Wirtschaft und der betriebsinternen Abläufe im eigenen Datencenter. Cloud-Konzepte haben sich etabliert. Rund sechs von zehn Unternehmen werden mittelfristig zwei bis drei Cloud-Plattformen nutzen.

Je beweglicher die Grenzen klassischer Rechenzentren werden, desto deutlicher rückt das Thema Informationssicherheit in den Fokus.

Der Dynamik und Flexibilität auf der einen Seite stehen ständig wachsende und neue Herausforderungen an adäquatem Schutz der Technologie- und IT-Infrastruktur gegenüber. Dabei konkurrieren die Ziele maximale Verfügbarkeit und Schutz der Daten mit den Ansprüchen an Leistung und Effizienz.

Angepasste Lösungen

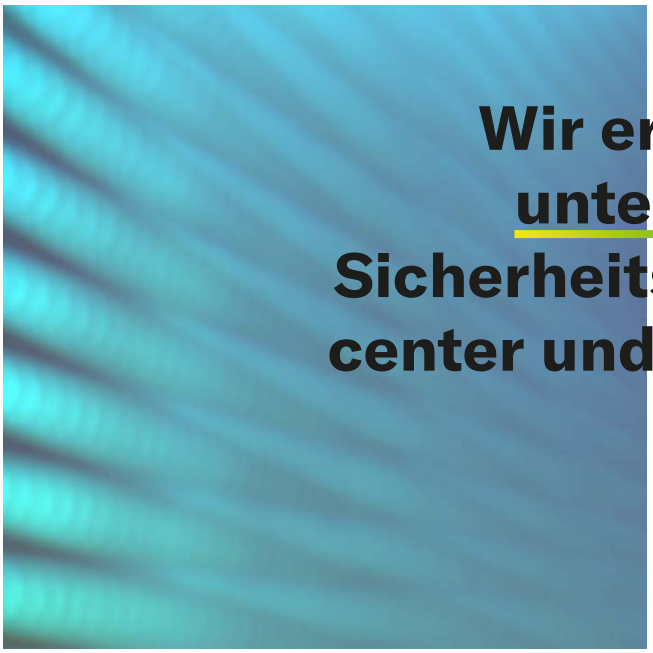
Unternehmen, die ihre Daten, Infrastrukturen und IT-Services effizient schützen wollen, sollten daher zunächst eine genaue Analyse ihrer Risikosituation durchführen. Die Basis dafür ist die Betrachtung der gesamten IT-Architektur und ihrer Bedrohungslage, sowohl der privaten als auch der öffentlichen Infrastrukturen. Nur ein Unternehmen, das weiß, wie Bedrohungen auf seine Infrastruktur einwirken und was es im Schadensfall verlieren kann, kann eine gezielte Cyber Security Strategie planen und implementieren. Aber auch dieser Plan muss in regelmäßigen Abständen überprüft werden, um die Infrastruktur kosteneffizient und sicher betreiben zu können.

Nicht jedes Datacenter weist die erforderlichen Qualitätsstandards auf. Ausfallsicherheit und Hochverfügbarkeit ist deshalb oberste Zielsetzung.

Die vier Grundbausteine für ein sicheres Datacenter bestehen aus

- Analysewerkzeugen, die bestehende und neue Bedrohungen identifizieren und gezielte Entscheidungen ermöglichen,
- geeigneten Schutzlösungen, die die Anforderungen von privaten und öffentliche Infrastrukturen vereinen, wie Segmentierung, Zugriffsregelung und -kontrolle und Absicherung der virtuellen Endpunkte,
- einer Infrastruktur-übergreifenden Überwachung auf Vorfälle und Anomalien über eine Event-Management-Lösung mit den entscheidenden Usecases und
- einer etablierten Organisation und geprüften Abläufen zum Umgang mit Vorfällen.

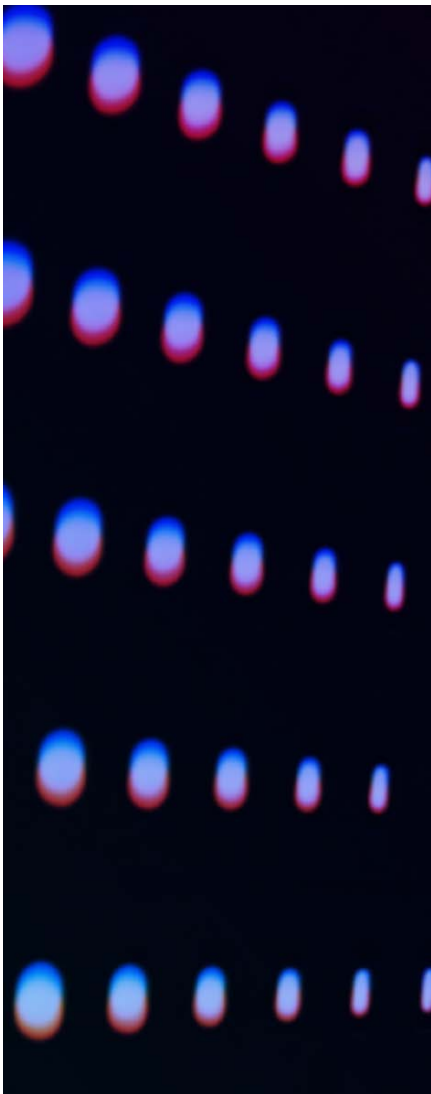
Die Implementierung und der Betrieb eines Information Security Management Systems (ISMS) sowie die Qualifikation und sicherheitstechnische Sensibilisierung der Mitarbeiter liefern den organisatorischen Überbau.



Wir erarbeiten mit Ihnen ein unternehmensspezifisches Sicherheitskonzept für Ihre Datacenter und Hybrid-Cloud-Lösung.

Unsere Vorgehensweise

- Analyse des Ist- Zustandes und Erstellung eines Cyber Security Plan Datacenter/Hybrid Cloud passend zu externen und internen Anforderungen und bereits vorhandenen Lösungen
- Design und Implementierung der Schutz- und Monitoring-Lösungen (und Einbindung vorhandener Lösungen)
- Absicherung von Cloud-Infrastrukturen (IaaS) und Cloud-Plattformen (PaaS) mit Cloud-integrierten Security-Lösungen (Firewall, Applikationskontrolle, Verschlüsselung, Authentifikation)
- Erstellung Vorgehensweise für den Umgang mit Vorfällen
- Betrieb der Gesamtlösung oder einzelner Komponenten gem. verschiedener Supportvarianten
- Überwachung der Datacenter und Hybrid-Cloud-Umgebungen auf sicherheitsrelevante Hinweise, Angriffe und kritische Ereignisse
- Aufbau und Betrieb eines zertifizierungsfähigen Information Security Management Systems mit Schwerpunkt auf die Anforderungen eines Rechenzentrumsbetriebs



Herausforderungen und Lösungen im Detail.

CYBER SECURITY LAGEBILD

Kennen Sie die aktuellen Gefahren für Ihre IT-Infrastruktur?

Identifikation der Bedrohungen

- Architekturreview Datacenter
- Cloud Usage und Compliance Assessment
- Pentest hybrider Infrastrukturen
- Threat Information Service

HYBRIDE INFRASTRUKTUREN

Sind Sie ausreichend abgesichert?

Schutzmaßnahmen implementieren und betreiben

- Containersecurity/Virtual Server Protection/ Secure VDI
- Privileged Account Management
- Network Access Control
- Datacenter und Cloud Security Gateways, Cloud-Governance-Lösungen (CASB)

SCHNELLE BEDROHUNGSERKENNUNG

Sehen Sie Angriffe rechtzeitig?

Überwachung der hybriden Infrastruktur auf sicherheitsrelevante Ereignisse

- Datacenter und Cloud Security Monitoring (SIEM)
- Vulnerability Scan
- Threat Emulation und Threat Intelligence

INCIDENT RESPONSE

Wie reagieren Sie auf Vorfälle und Angriffe?

Vorfälle analysieren, Angriffe stoppen, Normalbetrieb wiederherstellen

- Incident Response Team
- Cyber-Threat-Analyse
- Remediation Manager

CYBER SECURITY MANAGEMENT

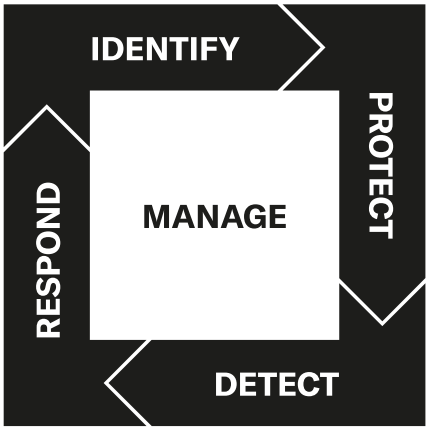
Halten Sie alle Fäden in der Hand?

IT-Infrastrukturen sicher und anforderungs-konform implementieren und betreiben

- Cloud-Strategie
- ISMS
- Risiko- und Notfallmanagement
- Audit-Services
- Awareness-Trainings

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

For your objectives.

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 9001:2000 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