
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

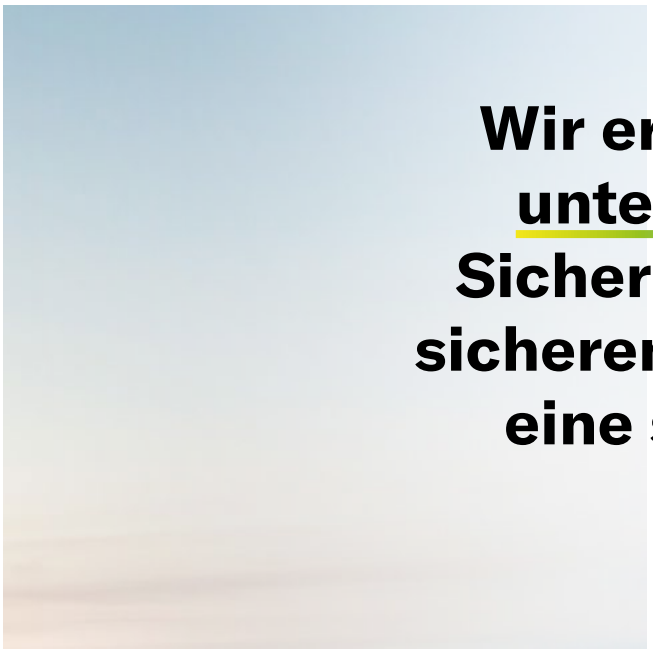
- Datenverlust bzw. Informationsabfluss
- Ausfall der Internet- oder Netzwerkverbindung, der den Zugriff auf Daten bzw. Anwendungen unmöglich macht
- Denial-of-Service-Angriffe auf Cloud-Anbieter, die sicher noch zunehmen werden
- Fehler in der Cloud-Administration durch den Anbieter
- Hohe Abhängigkeit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

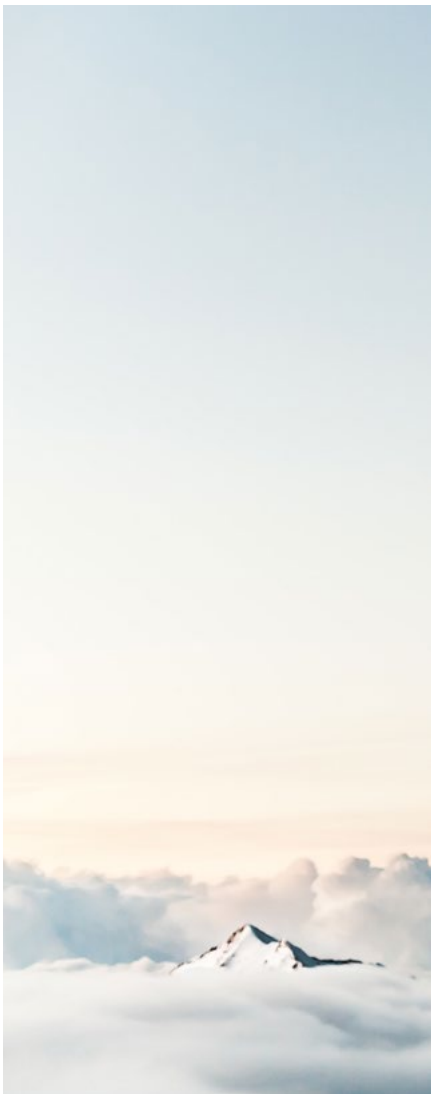
- Mangelhafter Einführungsprozess: Kritische Elemente werden übersehen, etablierte Sicherheitskontrollen entfallen, neue Risiken entstehen
- Vielzahl an Cloud-Anwendungen und damit Vertragspartnern mit jeweils individuellen Bedrohungen und Risiken
- Abhängigkeit vom Cloud-Anbieter, keine schnellen Fallback-Möglichkeiten 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!«



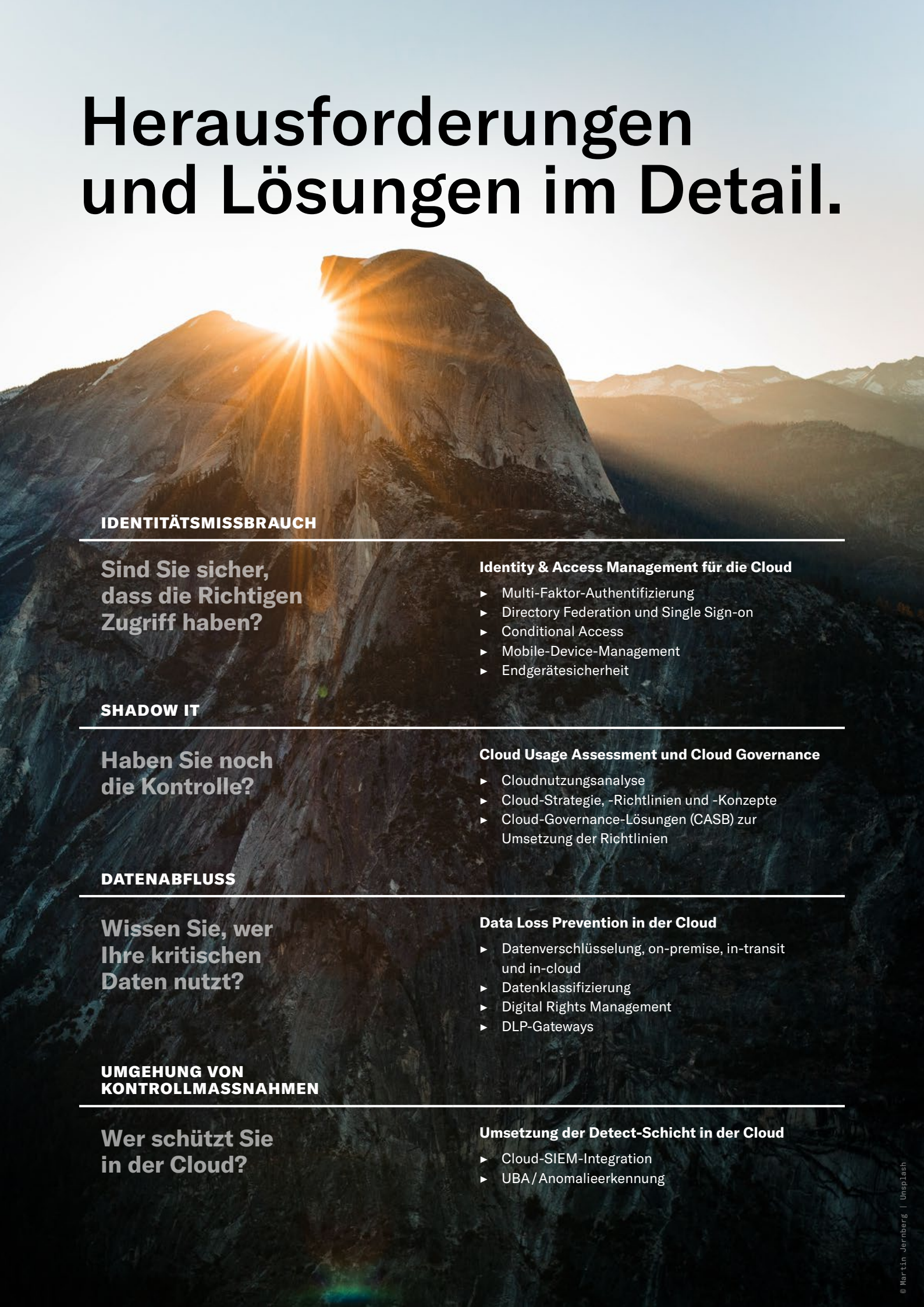
Wir erarbeiten mit Ihnen ein unternehmensspezifisches Sicherheitskonzept für einen sicheren Weg in die Cloud und eine sichere Cloudnutzung.

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



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

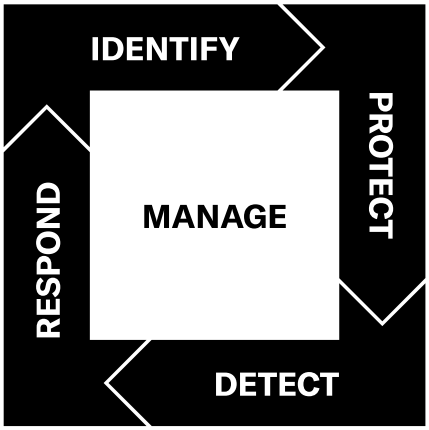
Wer schützt Sie in der Cloud?

Umsetzung der Detect-Schicht in der Cloud

- Cloud-SIEM-Integration
- UBA/Anomalieerkennung

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 9001:2015 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