SCALTEL

# ZERO TRUST
# Datacenter

# Inhalte

Warum brauchen Sie Zero Trust? Welche Herausforderungen warten bei der Implementierung dieser Sicherheitsstrategie auf Ihr Unternehmen? Diese Fragen wurden in unserem siebten Webinar der Online-Seminar Reihe "Zero Trust" aufgedeckt. Die wichtigsten Fragen zeigen wir hier nochmals auf!

# ZERO TRUST

## Warum eine gesamtheitliche Security-Strategie wichtig ist

Netzwerke sind heutzutage unglaublich vielschichtig, weit verzweigt und häufig unübersichtlich. Hacker nutzen dies gerne aus und greifen an mehreren Stellen gleichzeitig an. Ein Angriff findet nicht zwangsläufig im Datacenter statt, sondern kann ebenso in Niederlassungen oder in weiteren beliebigen Geräten mit unterschiedlichen Schwachstellen auftreten. Eine Analyse des aktuellen IST-Zustandes ordnet die Situation einem Reifegrad zu und zeigt den bestmöglichen Weg zu einer erfolgreichen Zero Trust Security Strategie auf.

## Zero Trust – eine Security-Strategie

Zero Trust beschreibt einen Sicherheitsanspruch, der diverse Zugriffe auf ein Unternehmen bewacht und vor unbefugtem Zugriff schützt. Dies zeigt eine Haltung, wie ein Netzwerk geführt werden kann. Jede Unternehmung definiert hier einen eigenen Startpunkt und geht einen individuellen Sicherheitsweg, welcher niemals endet. Dabei gilt: Vertrauen Sie niemanden, vergeben Sie immer nur zwingend notwendige Rechte und gehen Sie jederzeit von einem Angriff aus!

## Cyber Security Assessment - Warum wird es benötigt?

Cyber Security Assessment ist ein Modell, das den Sicherheitsansatz in einem Unternehmen kontinuierlich verbessert. Im ersten Schritt findet eine IST-Analyse statt, anschließend erfolgt die Einstufung in Reifegrad. Anhand dieses Reifegrades lassen sich Verbesserungsmöglichkeiten und Ziele definieren, die technisch umgesetzt werden können.

# UNSER WEG ZU ZERO TRUST

## GRADUIERUNG

Zero Trust Graduierung stellt sicher, dass vertrauliche Daten, während ihrer Verarbeitung und Speicherung, angemessen geschützt werden.
Die Identifizierung kritischer Daten und Dienste ist entscheidend, um eine Infrastruktur aufzubauen, die die Sicherheit dieser Assets gewährleisten kann und gleichzeitig den Betrieb wichtiger Dienste auch im Falle eines Angriffs ermöglicht.

Die wichtigsten Themen im Bereich Datengraduierung in Verbindung mit Cyber Recovery sind:

**Datenklassifizierung:**
Hierbei werden Daten auf der Grundlage ihrer Vertraulichkeit, Integrität und Verfügbarkeit kategorisiert. Die Klassifizierung kann in verschiedenen Stufen erfolgen, wie z.B. öffentlich, intern, vertraulich und streng vertraulich.

**Identifizierung kritischer Dienste:**
Die Bestimmung der geschäftskritischen Dienste und Anwendungen, die im Falle eines Cyber-Angriffs priorisiert werden müssen. Diese Dienste sind oft direkt mit den vertraulichen Daten verknüpft.

**Schutzmaßnahmen:**
Die Implementierung von Sicherheitskontrollen und -richtlinien, die auf die Graduierung der Daten und Dienste abgestimmt sind. Dazu gehören Zugriffskontrollen, Verschlüsselung, Datenverlustprävention (DLP) und regelmäßige Sicherheitsüberprüfungen.

## Graduierung - Was sollte nicht in falsche Hände geraten?

# UNSER WEG ZU ZERO TRUST

## Was brauche ich für den Restore?

### Authentifizierung, Identität und Sicherheit
- Active Directory/LDAP
- DNS-Speicherabbilder
- Zertifikate
- Ereignisprotokolle (einschließlich SIEM-Daten)

### Netzwerke
- Switch-/Router-Konfiguration
- Firewall-/Lastenausgleichseinstellungen
- Entwurf von IP-Services
- Zugriffssteuerungskonfiguration
- Firmware/Microcode/Patches

### Storage
- Backuphardwarekonfiguration
- SAN-/Arraykonfigurationen
- Storage-Abstraktionseinstellungen
- Firmware/Microcode/Patches

### Geistiges Eigentum
- Quellcode
- Proprietäre Algorithmen
- Entwicklerbibliotheken

### Host- und Build-Tools
- Aufbau physischer/virtueller Plattformen
- DevOps-Tools und Automatisierungsskripte
- Firmware/Microcode/Patches
- Anbietersoftware
  - Binärdateien (goldene Bilder)
  - Konfigurationen und Einstellungen

### Dokumentation
- CMDB-/Asset-DR und Cyber-Recovery-Runbooks und -Prüflisten
- Management-Extrakte
- HR-Ressourcen und Kontaktlisten

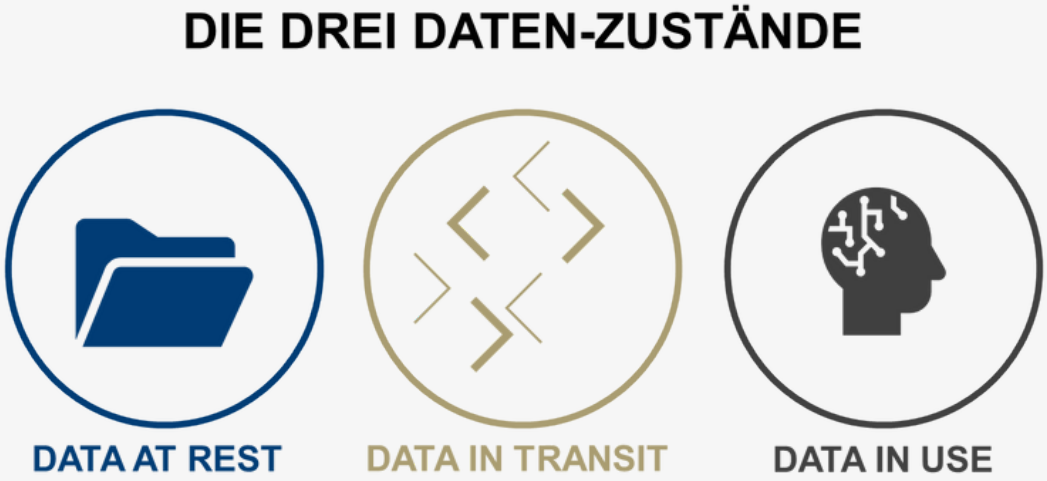
**Gaduierung**

**Encryption**

**Secure Backup**

# UNSER WEG ZU ZERO TRUST

## ENCRYPTION




Zero Trust Encryption bezieht sich auf eine Verschlüsselungsstrategie, die auf dem Zero Trust-Prinzip basiert, bei dem keinem Benutzer, Gerät oder Netzwerk automatisch vertraut wird. Bei dieser Herangehensweise werden Daten sowohl bei der Übertragung als auch bei der Speicherung verschlüsselt, um ihre Vertraulichkeit und Integrität zu gewährleisten. Durch die Implementierung strikter Authentifizierungs- und Autorisierungsmechanismen, wie Multi-Faktor-Authentifizierung und rollenbasiertem Zugriff, wird sichergestellt, dass nur berechtigte Benutzer auf die entschlüsselten Daten zugreifen können.

**DATA AT REST - Verschlüsselung von Daten im Ruhezustand:**
Das bezieht sich auf Sicherheitsmaßnahmen die ergriffen werden, um Daten, die auf Datenträgern wie Festplatten, Solid-State-Laufwerken, USB-Sticks oder in Cloud-Speicher gespeichert sind, zu schützen. Beispiele sind vollständige Laufwerksverschlüsselung, Datei- oder Ordner Verschlüsselung, Datenbank-Verschlüsselung und/oder Cloud-Speicher Verschlüsselung.

**DATA IN TRANSIT - Datenübertragungsverschlüsselung:**
Das ist ein Sicherheitsverfahren, bei dem Daten, die zwischen zwei Systemen oder Geräten übertragen werden, verschlüsselt werden (VMotion, SSL/TLS, HTTPS, S/MIME), um sie vor unbefugtem Zugriff, Manipulation oder Diebstahl zu schützen.

**DATA IN USE - Speicherverschlüsselung:**
Im Kontext der Informationssicherheit bezieht sich "Data in use" auf Informationen, die gerade geöffnet und von Systemen und Benutzern bearbeitet werden, was sie potenziell anfällig für unautorisierten Zugriff oder Datendiebstahl macht.

# UNSER WEG ZU ZERO TRUST

## DATA - BACKUP

### Disaster vs. Cyber Recovery

| Kategorie | Disaster Recovery | Cyber Recovery |
|---|---|---|
| **RTO (Recovery Time Objective)** | Möglichst sofort | Zuverlässig |
| **RPO (Recovery Point Objective)** | Möglichst fortlaufend | Letzte “gute” Backup-Kopie |
| **Art der Katastrophe** | Hochwasser, Stromausfall, Brand… | Gezielter Cyberangriff |
| **Auswirkung der Katastrophe** | Regional beschränkt | Unternehmensweite Ausbreitung |
| **Backuptopologie** | Verbundene, redundante Systeme | Zusätzliche isolierte Umgebung |
| **Datenmenge** | Alle Daten | Wichtigste Unternehmenssysteme (“Minimal viable Business”) |
| **Wiederherstellung** | Klassischer Restore (z.B. Failback) | Iterative, geplante Wiederherstellung |

### Was soll ich tun?

# UNSER WEG ZU ZERO TRUST

Neben den technischen Parametern müssen Budget und Komplexität sowie Zeitaufwand gegenübergestellt werden.

Im zweiten Schritt werden sämtliche Schutzflächen sowie Angriffsflächen identifiziert. Der Zusammenhang zwischen riskanten und zu schützenden online- sowie offline-Objekten muss unbedingt beachtetet werden!

Wir begleiten Sie gerne auf dem Weg zu Zero Trust.

**SCALTEL Zero Trust**

**Mail - Verteiler**

**Kontakt aufnehmen**