SCALTEL

ZERO TRUST
Network

Inhalte

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

Rückblick - Warum ist eine gesamtheitliche Security-Strategie wichtig?

Never Trust, always verify - Der aktuelle Stand der Technik und praktikable Migrationspläne.

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.

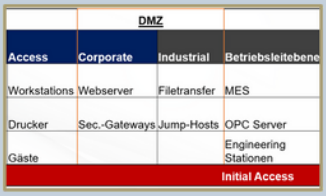
Zero Trust – eine Security-Strategie

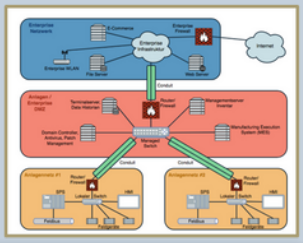
Zero Trust beschreibt einen Sicherheitsanspruch, der diverse Zugriffe auf ein Unternehmen bewacht und vor unbefugtem Zugriff schützt. Dies zeigt eine Haltung, wie ein Netzwerk geführt werden kann. Jede Unternehmung definiert hier einen eigenen Startpunkt und geht einen individuellen Sicherheitsweg, welcher 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





Visibility

Wir können nur das schützen, was wir sehen

Ergebnis: Asset Inventory

Classification

Wir müssen Risiken bewerten und Schutzmaßnahmen definieren

Ergebnis: Workbook für Projekte

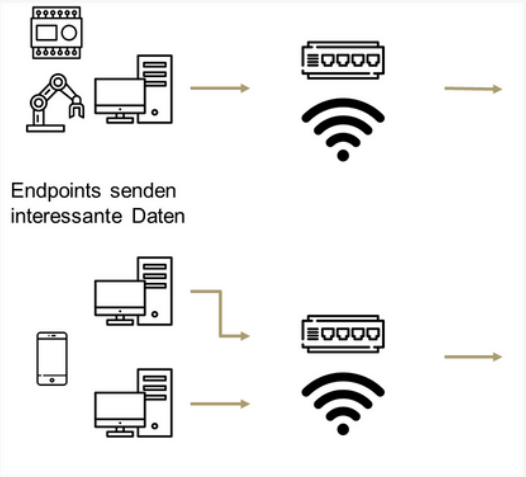
Segmentation

Eine Segmentierung reduziert die Angriffsfläche und ermöglicht eine schnelle Reaktion bei Angriffen

Ergebnis: Projektumsetzung in Reifegradmodellen

Endpoint profiling - visibility

Data Collection	Visibility - autom. Erkennung



Network Access Control – Visibility:
Authentifizierung von Benutzer und/oder Geräten für einen sicheren Netzwerkzugriff

OT-Monitoring – Visibility:
Passive Detection:
Analyse des Netzwerkverkehrs ohne Beeinflussung des Endpoints, um Endpoints und Verkehrsmuster zu identifizieren.

UNSER WEG ZU ZERO TRUST

Classification - Grundlage Risikobewertung

Risikobewertung
Entwicklung einer Übersicht zur Klassifizierung

INITIAL ACCESS
- Internetzugang
- E-Mail
- Aus dem Internet erreichbar

LATERAL MOVEMENT
- Managed/unmanaged
- Potenzielles Ziel für Berechtigungserweiterung
- Bekannte Sicherheitslücken

SCHUTZMECHANISMEN
- Mit Endpoint Security
- Ohne Endpoint Security

Asset Identity:

WIN10 Workstation:
- Internetzugang: **Ja**
- E-Mail: **Ja**
- Bekannte Sicherheitslücken: **keine**
- Endpoint Security: **vorhanden**

Asset Identity:
Controller 5069-L330ERM/A
Beispiel Asset OT:
- Internetzugang: **Nein**
- E-Mail: **Nein**
- Bekannte Sicherheitslücken: **Ja**
- Endpoint Security: **Nein**

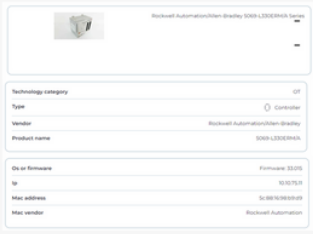
Classification - Übersicht

Unternehmensebene				DMZ		OT/ Industrial Control Systems			
Tier 0	Tier 1	Tier 2	Access	Corporate	Industrial	Betriebsleitebene	Prozessleitebene	Steuerungsebene	Feldebene
Domaincontroller	Appl.-Server	Terminalserver	Workstations	Webserver	Filetransfer	MES	SCADA	SPS	Sensoren
Exchange	Jump-Hosts		Drucker	Sec.-Gateways	Jump-Hosts	OPC Server	Local HMI	RTUs	Aktoren
	Management		Gäste			Engineering Stationen		IPCs	
Lateral Movement				Initial Access			Lateral Movement		

Asset Identity:

Beispiel WIN10 Workstation:
Internet Access: ja
Email Client: ja
→ Risiko: Initial Access
Maßnahmen: Endpoint Security
Client-Internet-Policy
Patch-MGMT
Software-Verteilung
Support: Nur über Client Admin Account

Asset Identity:



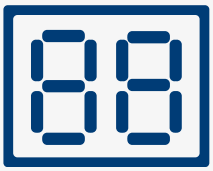
Gruppe: Steuerungsebene
Internet Access: nein
Email Client: nein
Schwachstellen OS: ja
→ Risiko: Lateral Movement
Maßnahmen: Micro Segmentierung
Policy: Zugriff nur auf Prozessleit- und Feldebene

UNSER WEG ZU ZERO TRUST

Segmentation

Macro Segmentation

Macro Segmentation bezieht sich auf die Teilung eines Netzwerks in große, logische Segmente, die jeweils mit eigenen Sicherheitsrichtlinien und Zugriffskontrollen ausgestattet sind. Das Ziel der Macro Segmentiation ist es, den Netzwerkzugriff mittels einer Next Generation Firewall auf ein Minimum zu beschränken, indem nur autorisierte Benutzer oder Anwendungen Zugang zu den jeweiligen Segmenten des Netzwerks haben.



Micro Segmentation

Durch die Verwendung von Mikrosegmentierungstechniken können Netzwerke in kleinere, isolierte Segmente unterteilt werden, wodurch die Angriffsfläche reduziert wird und eine bessere Kontrolle darüber besteht, wer auf welche Ressourcen zugreifen kann. Dies bedeutet, dass Benutzer oder Geräte nur Zugriff auf die Ressourcen erhalten, die für ihre Rolle im Netzwerk relevant sind. Dadurch wird die Möglichkeit von Netzwerkangriffen reduziert, da nur autorisierte Benutzer Zugriff auf bestimmte Netzwerkressourcen haben.

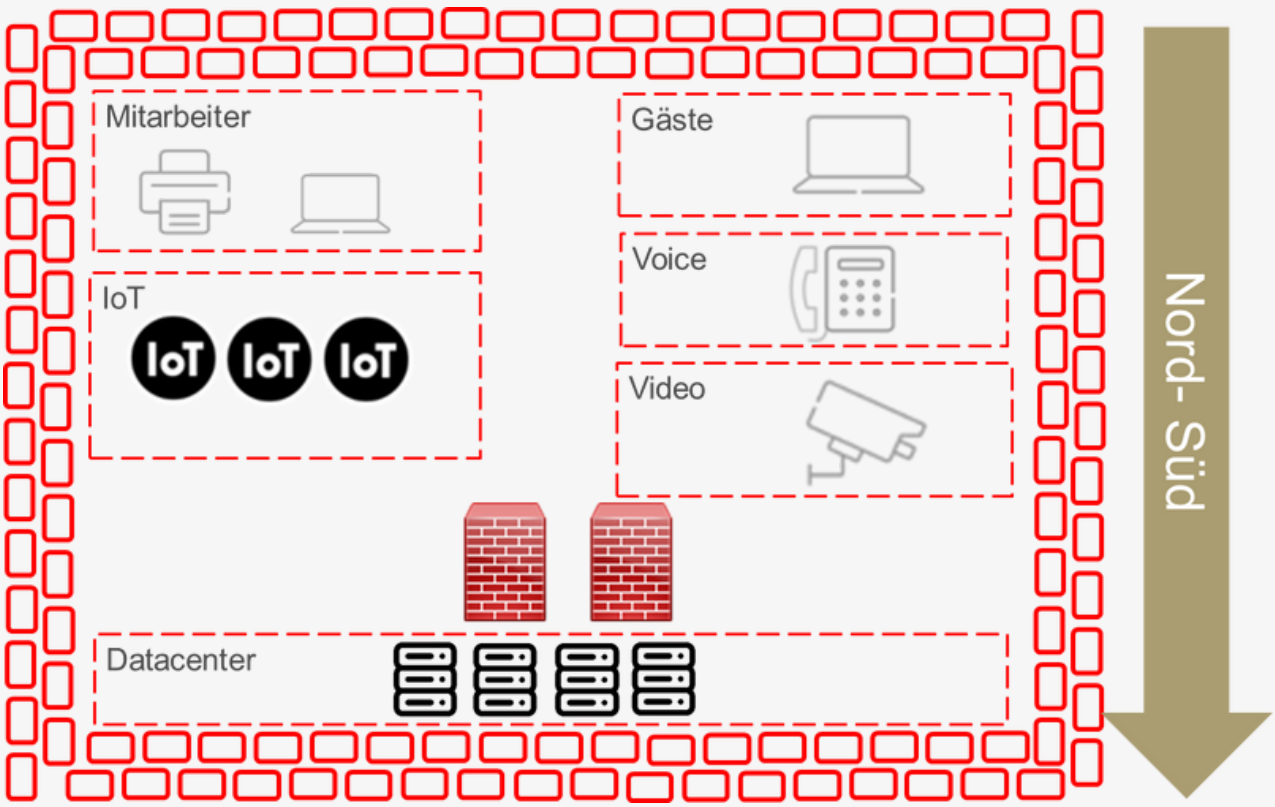
UNSER WEG ZU ZERO TRUST

Macro Segmentation

Das Ziel der Macro-Segmentierung ist es, den Netzwerkzugriff mittels einer Next Generation Firewall auf ein Minimum zu beschränken. Diese Möglichkeit wird gegeben, indem nur autorisierte Benutzer oder Anwendungen Zugang zu den jeweiligen Segmenten des Netzwerks haben.

Nachteile von Macro-Segmentierung:

- Kein Schutz innerhalb des gleichen VLANs
- Innerhalb eines Segments können die Geräte frei kommunizieren
- Keine Unterscheidung bei Zugriffsberechtigungen
- Wenn eine Malware ein System infiziert hat, breitet sich die Bedrohung im ganzen Segment aus
- Konfiguration am Switch, um den Port in das richtige Segment zu hinterlegen
- Änderungen von VLANs wirken sich auf die IP-Adresse von dem Gerät aus

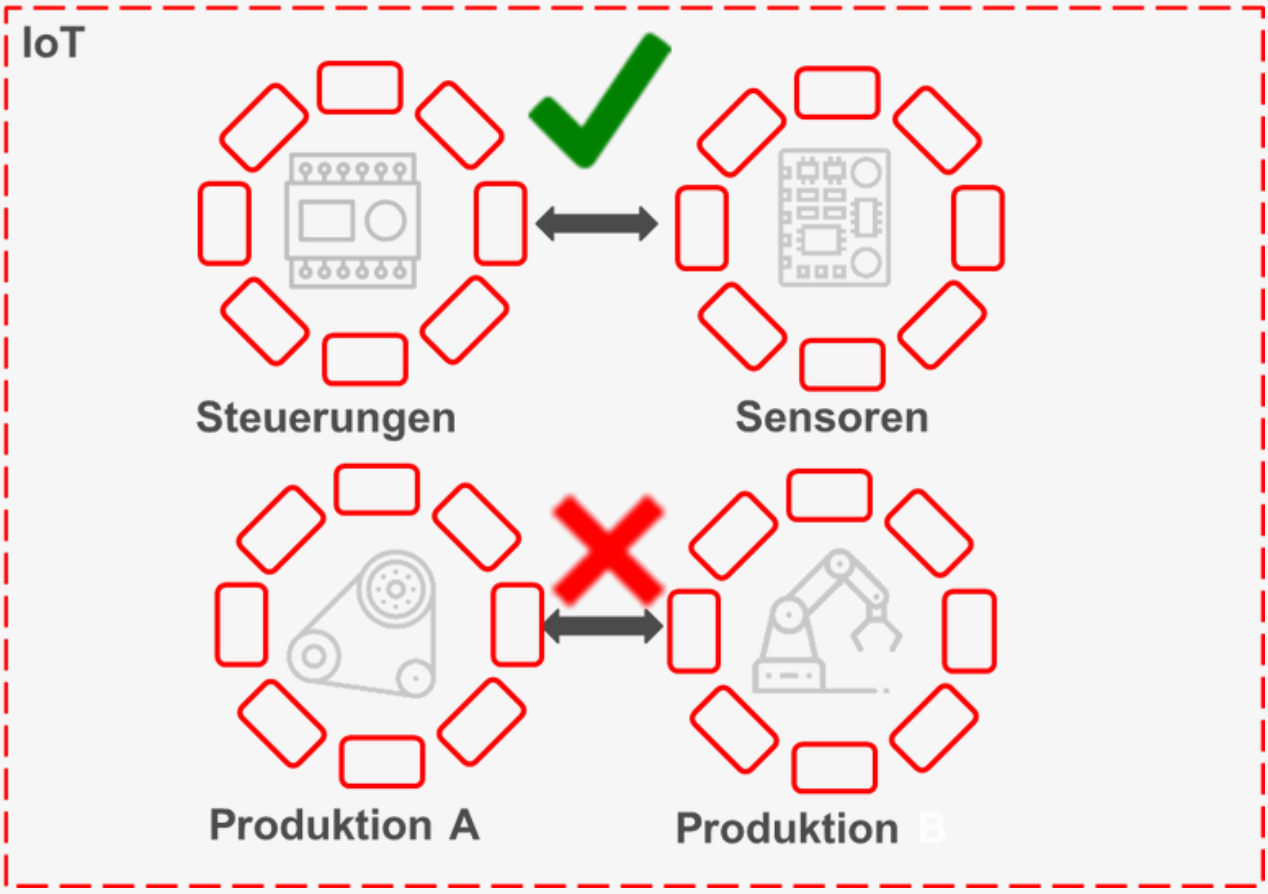


UNSER WEG ZU ZERO TRUST

Micro Segmentation

Festlegung isolierter Netzwerkports, die keine Berechtigung haben, mit anderen isolierten Ports zu kommunizieren.

- Unterteilung in kleine und isolierte Segmente, um die Angriffsfläche zu reduzieren
- Segment basiert auf einem Rollenkonzept
- Kein „Default Trust“
- Ohne Genehmigung können Segmente nicht miteinander kommunizieren
- Jede Kommunikation zwischen den Segmenten wird durch eine Firewall mit IDS und IPS überwacht



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.
Informieren Sie sich in unseren nächsten Webinaren über die weiteren Bausteine.

Unsere Termine zur Online-Seminarreihe "Zero Trust"

DATUM	THEMA
11.05.2023	ZERO TRUST: Devices
25.05.2023	ZERO TRUST: Data

Zur Anmeldung

Kontakt aufnehmen