SCALTEL

ZERO TRUST
Perimeter

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 - Jede Abgrenzung bildet einen Perimeter

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.

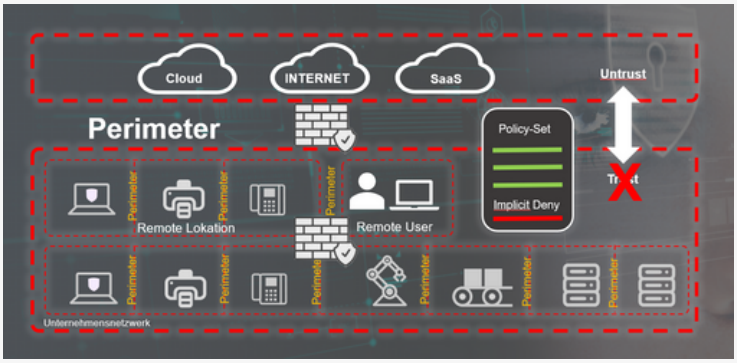
Zero Trust – eine Security-Strategie

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



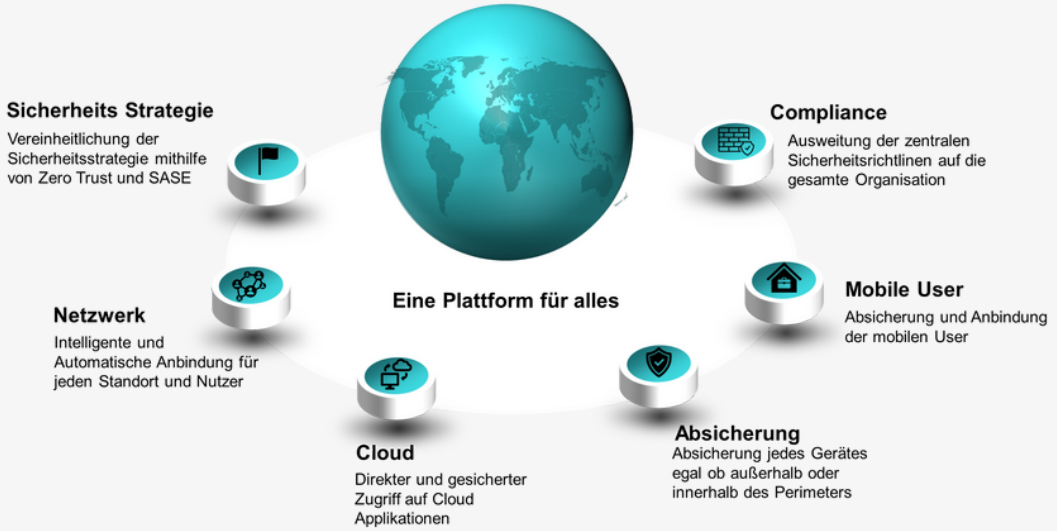
Der Begriff "Perimeter"

In der IT-Sicherheit wird der Begriff "Perimeter" als eine Art virtuelle Grenze verstanden, die ein Netzwerk oder eine IT-Infrastruktur vor unerwünschten Zugriffen und Angriffen von außen schützen soll. Der Schutz erfolgt in der Regel durch die klassische Internet-Firewall.

SASE - Plattform

Im Kontext von Zero Trust bildet nun aber jeder Segment-Übergang, innerhalb und außerhalb des Unternehmensnetzwerkes, ein Perimeter und verlangt daher die gleichen bekannten Schutzmaßnahmen wie beim Übergang zum Internet.
Dieser Ansatz verlangt nach einer kompletten Neustrukturierung der Netzwerk-kommunikation. Speziell für den WAN- Bereich ist dies mit hohen Aufwänden verbunden, da der bisherige Best-of-Breed Ansatz sehr betreuungsintensiv ist.
Realistisch umsetzbar, ohne Ausnahmeregelungen dafür mir maximaler Flexibilität, ist dies nur durch einen Plattformansatz, der sowohl die Konnektivität als auch die Sicherheit berücksichtigt - Connect IT + Secure IT.

Laut Gartner werden bis 2025 80 Prozent der Unternehmen eine Strategie verfolgen, die den Zugriff auf das Internet, Cloud-Dienste und private Anwendungen über eine SSE-Plattform (Security-Service-Edge) eines einzigen Anbieters ermöglicht.



Exklusiver Partner:
paloalto NETWORKS

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
20.04.2023	ZERO TRUST: Network
11.05.2023	ZERO TRUST: Devices
25.05.2023	ZERO TRUST: Data

Zur Anmeldung

Kontakt aufnehmen