SCALTEL

ZERO TRUST

Cyber Security Assessment

Inhalte

Warum brauchen Sie Zero Trust? Was ist Zero Trust? Und wo bekommt man es her? Diese Fragen wurden in unserem ersten 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 nutzten dies gerne aus und greifen an mehreren Stellen gleichzeitig an. Ein Angriff findet nicht zwangsläufig im Datacenter statt, sondern kann ebenso in Niederlassungen oder weitere beliebige Geräte mit unterschiedlichen Schwachstellen auftreten. Eine Analyse des aktuellen IST-Zustandes ordnet die Situation einem Reifegrade zu und zeigt den bestmöglichen Weg zu einer erfolgreichen Zero Trust Security Strategie auf.

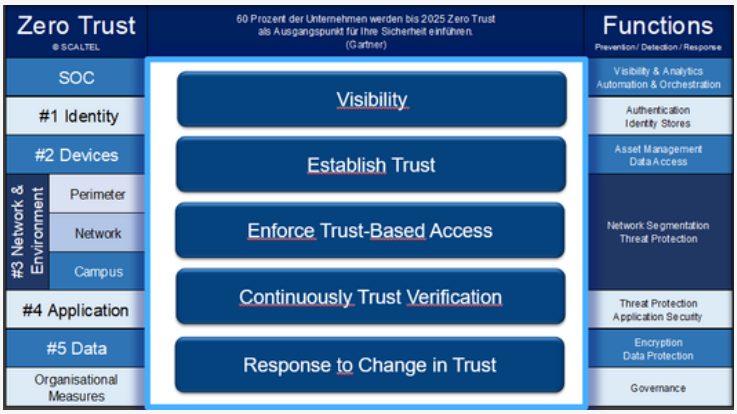
Zero Trust – Ursprung und Bedeutung

Zero Trust beschreibt einen Sicherheitsanspruch, der diverse Zugriffe auf ein Unternehmen bewacht und vor unbefugtem Zugriff schützt. Dabei gibt es entscheidende Unterschiede zwischen Zero Trust 1.0 und 2.0. Während Zero Trust in der ersten Version nur die Zugriffe auf Netzwerkebene (Layer 2) berücksichtigt hat, sind die neuen Ansätze in der zweiten Generation vielschichtiger. Sämtliche Verbindungen werden innerhalb und außerhalb, digital und physisch im Unternehmen analysiert und fortlaufend geprüft.

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 Reifegrade lassen sich Verbesserungsmöglichkeiten und Ziele definieren, die technisch umgesetzt werden können.

UNSER WEG ZU ZERO TRUST

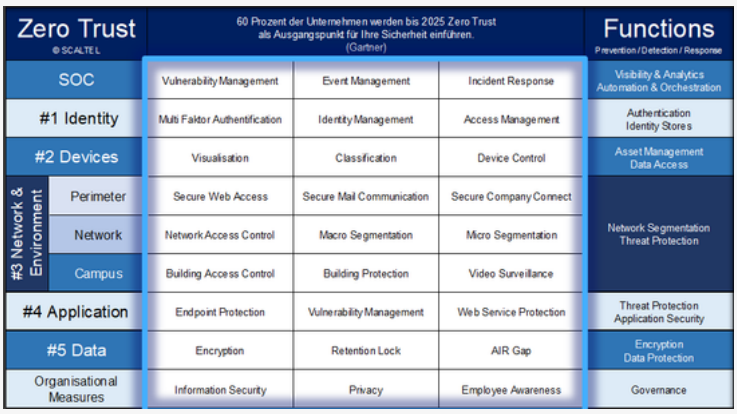


Assessment - Ziele

Um die Ziele, wie beispielsweise Visibility, zu erreichen, benötigt es mehrere Bausteine mit verschiedenen Aufgabenblöcken

Assessment - Komponenten

In unserem Portfolio umfassen wir folgende Zero Trust Bausteine:



Assessment – Maßnahmen

Hinter jedem Aufgabenblock verbergen sich Maßnahmen, die umgesetzt werden müssen.

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 müssen 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
16.02.2023	ZERO TRUST: Informationssicherheit / DSGVO
09.03.2023	ZERO TRUST: Physical Security
30.03.2023	ZERO TRUST: Perimeter
20.04.2023	ZERO TRUST: Network
11.05.2023	ZERO TRUST: Devices
25.05.2023	ZERO TRUST: Data

Zur Anmeldung

Kontakt aufnehmen