



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!



Warum eine gesamtheitliche Security-Strategie wichtig ist



Zero Trust – Ursprung und Bedeutung



Cyber Security Assessment - Warum wird es benötigt?

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



UNSER WEG ZU ZERO TRUST

Zero Trust		60 Prozent der Unternehmen werden bis 2025 Zero Trust als Ausgangspunkt für Ihre Sicherheit einführen. (Gartner)			Functions
© SCALTEL					Prevention / Detection / Response
SOC		<div style="border: 2px solid blue; padding: 5px; text-align: center;"> <p>Visibility</p> <p>Establish Trust</p> <p>Enforce Trust-Based Access</p> <p>Continuously Trust Verification</p> <p>Response to Change in Trust</p> </div>			Visibility & Analytics Automation & Orchestration
#1 Identity					Authentication Identity Stores
#2 Devices					Asset Management Data Access
#3 Network & Environment	Perimeter				Network Segmentation Threat Protection
	Network				
Campus					
#4 Application		Threat Protection Application Security			
#5 Data		Encryption Data Protection			
Organisational Measures		Governance			

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:

Zero Trust		60 Prozent der Unternehmen werden bis 2025 Zero Trust als Ausgangspunkt für Ihre Sicherheit einführen. (Gartner)				Functions								
© SCALTEL						Prevention / Detection / Response								
SOC		<div style="border: 2px solid blue; padding: 5px; text-align: center;"> <table border="1"> <tr> <td>NAC</td> <td>MFA</td> </tr> <tr> <td>Firewalls</td> <td>SD-WAN</td> </tr> <tr> <td>EDR/XDR</td> <td>SASE</td> </tr> <tr> <td>SOC</td> <td>Backup</td> </tr> </table> </div>				NAC	MFA	Firewalls	SD-WAN	EDR/XDR	SASE	SOC	Backup	Visibility & Analytics Automation & Orchestration
NAC	MFA													
Firewalls	SD-WAN													
EDR/XDR	SASE													
SOC	Backup													
#1 Identity		Authentication Identity Stores												
#2 Devices		Asset Management Data Access												
#3 Network & Environment	Perimeter	Network Segmentation Threat Protection												
	Network													
	Campus													
#4 Application		Threat Protection Application Security												
#5 Data		Encryption Data Protection												
Organisational Measures		Governance												

Zero Trust		60 Prozent der Unternehmen werden bis 2025 Zero Trust als Ausgangspunkt für Ihre Sicherheit einführen. (Gartner)			Functions
© SCALTEL					Prevention / Detection / Response
SOC		Vulnerability Management	Event Management	Incident Response	Visibility & Analytics Automation & Orchestration
#1 Identity		Multi Faktor Authentication	Identity Management	Access Management	Authentication Identity Stores
#2 Devices		Visualisation	Classification	Device Control	Asset Management Data Access
#3 Network & Environment	Perimeter	Secure Web Access	Secure Mail Communication	Secure Company Connect	Network Segmentation Threat Protection
	Network	Network Access Control	Macro Segmentation	Micro Segmentation	
	Campus	Building Access Control	Building Protection	Video Surveillance	
#4 Application		Endpoint Protection	Vulnerability Management	Web Service Protection	Threat Protection Application Security
#5 Data		Encryption	Retention Lock	AIR Gap	Encryption Data Protection
Organisational Measures		Information Security	Privacy	Employee Awareness	Governance

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 beachtet 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](#)

