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 auftreten oder weitere beliebige Geräte mit unterschiedlichen Schwachstellen betreffen. 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 - Was steckt dahinter?

Das 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 Reifegrade. Anhand dieses Reifegrad lassen sich Verbesserungsmöglichkeiten und Ziele definieren, die technisch umgesetzt werden können. Auf den folgenden Seiten gehen wir weiter auf das SCALTEL Cyber Security Assessment ein. Zuerst definieren wir die einzelnen Schritte, danach die Themengebiete und im Anschluss können Sie einen Kurzcheck machen.

CYBER SECURITY ASSESSMENT IM KONTEXT VON ZERO TRUST

Ein Cyber Security Assessment im Rahmen des Zero-Trust-Modells umfasst eine umfassende Bewertung der aktuellen Sicherheitslage einer Organisation. Dies beinhaltet die Identifizierung und Bewertung von Risiken, Schwachstellen und potenziellen Bedrohungen in der IT-Infrastruktur. Ziel ist es, ein klares Verständnis der Sicherheitslage zu erlangen und Bereiche zu identifizieren, in denen Verbesserungen erforderlich sind.

KERNKOMPONENTEN EINES CYBER SECURITY ASSESSMENTS:

Identifizierung von Assets und Ressourcen:
Erfassung und Klassifizierung aller IT-Assets, einschließlich Hardware, Software, Daten und Netzwerkkomponenten. Bewertung der Wichtigkeit und des Wertes dieser Assets für die Organisation.

Bedrohungs- und Risikoanalyse:
Analyse potenzieller Bedrohungen, einschließlich externer Angriffe (wie Phishing und Ransomware) und interner Bedrohungen (wie Insider-Bedrohungen). Bewertung der Risiken basierend auf der Eintrittswahrscheinlichkeit und den potenziellen Auswirkungen auf die Organisation.

Schwachstellenbewertung:
Durchführung von Sicherheitsüberprüfungen und Penetrationstests, um Schwachstellen in der IT-Infrastruktur zu identifizieren. Bewertung der Auswirkungen identifizierter Schwachstellen und Priorisierung der Behebung.

Überprüfung der Sicherheitskontrollen:
Bewertung der Wirksamkeit bestehender Sicherheitskontrollen und -prozesse. Überprüfung der Konformität mit Sicherheitsstandards und gesetzlichen Vorschriften.

Erstellung eines Maßnahmenplans:
Entwicklung eines Plans zur Verbesserung der Sicherheitslage, basierend auf den Ergebnissen des Assessments. Priorisierung von Maßnahmen, wie die Implementierung von Zero Trust-Prinzipien, die Stärkung der Endpunktsicherheit und die Verbesserung der Incident Response-Prozesse.

CHECKLISTE FÜR DIE IMPLE-MENTIERUNG VON ZERO TRUST:

Der hier beschriebene Kurzcheck ist lediglich ein Ausschnitt unseres umfangreichen Cyber Security Assessments und dient primär dazu, eine Tendenz aufzuzeigen, wie weit ein Unternehmen in seiner IT-Sicherheitsstrategie fortgeschritten ist. Er beinhaltet nur einen kleinen Teil der Fragen, die in unserem vollständigen Assessment gestellt werden. In unserem detaillierten Cyber Security Assessment fokussieren wir uns auf acht zentrale Schwerpunkte, um eine tiefgreifende und ganzheitliche Analyse Ihrer IT-Sicherheitslage zu ermöglichen:

SOC (Security Operations Center):
Hier prüfen wir die Effektivität Ihres Security Operations Centers und die Fähigkeit zur Erkennung und Reaktion auf Sicherheitsvorfälle.

Identity Management:
Dieser Bereich konzentriert sich auf die Verwaltung von Benutzeridentitäten und Zugriffsrechte, ein Schlüsselelement zur Sicherung Ihrer IT-Infrastruktur.

Devices:
Hier bewerten wir die Sicherheit aller Geräte in Ihrem Netzwerk, einschließlich Computer, Mobilgeräte und anderer vernetzter Hardware.

Network Security:
In diesem Abschnitt liegt der Fokus auf der Sicherheit Ihres Netzwerks, um potenzielle Schwachstellen zu identifizieren und die Abwehrfähigkeit zu stärken.

Environment:
Wir betrachten die physischen und virtuellen Umgebungen, in denen Ihre IT-Systeme operieren, einschließlich aller Aspekte der Sicherheit in Rechenzentren und Cloud-Infrastrukturen.

Application Security:
Hier untersuchen wir die Sicherheit Ihrer Anwendungen und Software, um Anfälligkeiten aufzudecken und Verbesserungsmöglichkeiten aufzuzeigen.

CHECKLISTE FÜR DIE IMPLE-MENTIERUNG VON ZERO TRUST:

Data Protection:
Dieser Teil des Assessments widmet sich dem Schutz und der Integrität Ihrer Daten, um sicherzustellen, dass sensible Informationen angemessen geschützt werden.

ISMS (Information Security Management System):
Schließlich bewerten wir Ihr Informationssicherheitsmanagementsystem, um die Effektivität Ihrer Sicherheitsrichtlinien, -prozesse und Compliance-Maßnahmen zu überprüfen.

Unser umfassendes Cyber Security Assessment bietet Ihnen somit nicht nur eine Momentaufnahme Ihrer aktuellen Sicherheitslage, sondern liefert auch wertvolle Einblicke und Empfehlungen, um Ihre IT-Sicherheitsstrategie kontinuierlich zu verbessern und an die sich ständig ändernden Bedrohungslandschaften anzupassen.

Identitäts- und Zugriffsmanagement (IAM):
- ☐ Implementierung von MFA.
- ☐ Fortlaufende Überprüfung der Zugriffsrechte.

Netzwerkarchitektur:
- ☐ Umsetzung von Mikrosegmentierung.
- ☐ Einführung fortschrittlicher Netzwerküberwachungstools.

Endpunktsicherheit:
- ☐ Einrichtung von Endpoint Detection and Response (EDR) Systemen.
- ☐ Regelmäßige Updates und Patches für alle Endgeräte.

Datenschutz:
- ☐ Umsetzung von Datenverschlüsselung.
- ☐ Entwicklung von Richtlinien für das Datenmanagement.

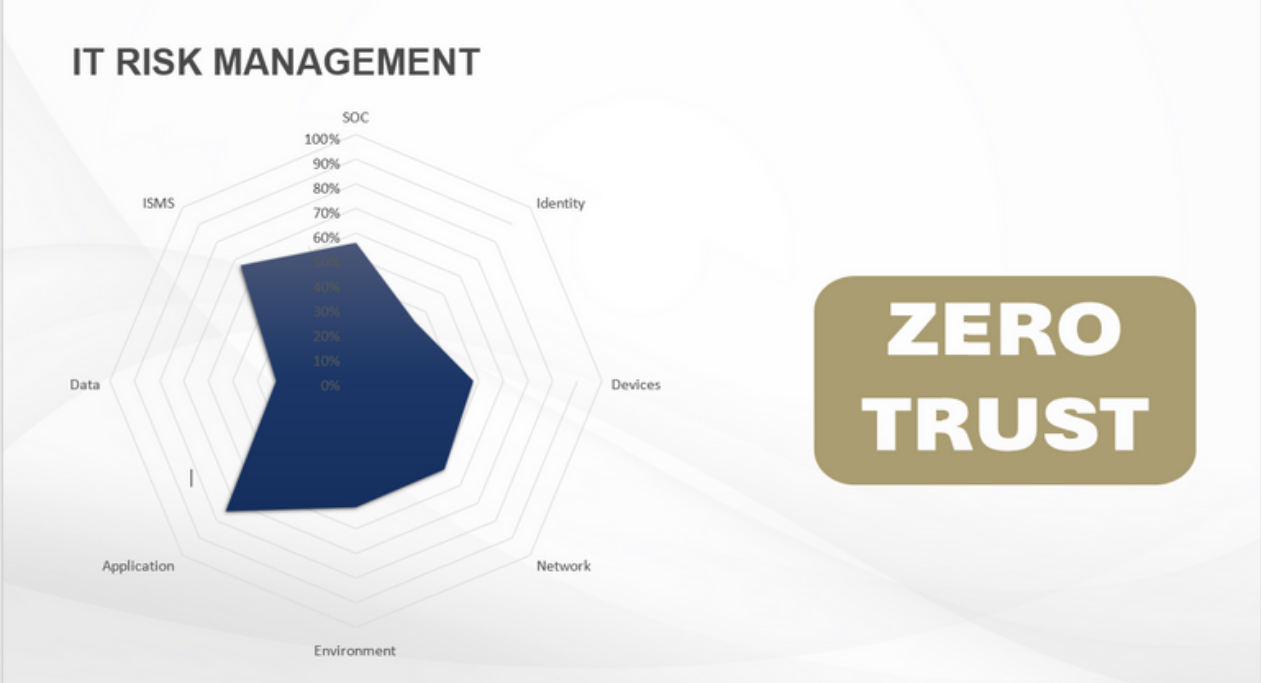
Verhaltensüberwachung und -analyse:
- ☐ Implementierung von Systemen zur Erkennung anomalen Verhaltens.
- ☐ Einsatz von KI-basierter Analytik für fortgeschrittene Bedrohungserkennung.

ABLAUF EINES CYBER SECURITY ASSESSMENTS:

Das Cyber Security Assessment ist ein umfassender Prozess, der alle acht oben benannte Bereiche umfasst. In einem ca. dreistündigen Termin Remote oder bei Ihnen Vorort, werden alle Bereiche ausführliche analysiert, besprochen und Fragen beantwortet. Anschließend analysieren unsere Spezialisten die Antworten und stellen die Ergebnisse in einem Spinnendiagramm dar. Dieses Diagramm zeigt, wie gut Ihr Unternehmen in jedem der acht Bereiche aus Sicht der Cybersecurity abschneidet.

Abschließend werden spezifische Problemstellungen aufgedeckt, die es ermöglichen, den Reifegrad der Cybersecurity in jedem Unternehmen präzise zu definieren. Diese Erkenntnisse sind entscheidend, um gezielte Handlungsempfehlungen und dringende Maßnahmen zu entwickeln, die auf Ihre individuellen Bedürfnisse und Herausforderungen zugeschnitten sind.

Die Identifizierung von Schwachstellen und die Bewertung des Reifegrads sind wesentliche Schritte, um eine effektive und nachhaltige Sicherheitsstrategie zu entwerfen. Dies beinhaltet nicht nur die Behebung aktueller Sicherheitslücken, sondern auch die Planung langfristiger Verbesserungen, um auf zukünftige Bedrohungen vorbereitet zu sein.



UNSERE ERGEBNISSE AUS DEN ERSTEN 100 CYBER SECURITY ASSESSMENTS LAUTET:

1. Unvollständige Umsetzung von Zero Trust:
Die Implementierung von Zero Trust-Ansätzen in vielen Unternehmen bleibt hinter ihrem Potenzial zurück, was auf hohe Kosten, Implementierungsschwierigkeiten und Bedenken hinsichtlich der Beeinträchtigung des Geschäftsbetriebs hindeutet. Dies lässt vermuten, dass der Markt noch nicht vollständig bereit für eine umfassende Anwendung von Zero Trust ist.

2. Sicherheitsbedenken und Komplexität:
Trotz bedeutender Investitionen in IT-Sicherheit bleiben Zweifel an der Wirksamkeit traditioneller Sicherheitslösungen. Unternehmen erkennen, dass herkömmliche Methoden wie VPNs oder Firewalls nicht ausreichend auf moderne Cyberbedrohungen abgestimmt sind.

3. Mangelnde strategische Integration:
Ein wiederkehrendes Problem ist die mangelnde Abstimmung der Sicherheitsinitiativen mit den übergeordneten Geschäftszielen, was auf eine unzureichende Integration von Zero Trust als Kernelement der Geschäftsstrategie hindeutet.

4. Der Weg zu Zero Trust durch das NIST Framework:
Um Unternehmen effektiv in Richtung Zero Trust zu führen, erscheint das NIST (National Institute of Standards and Technology) Framework als geeigneter Weg. Es bietet strukturierte Leitlinien, um Unternehmen schrittweise an Zero Trust heranzuführen und die nötige Reife für diese Technologie zu entwickeln.

Insgesamt offenbart sich, dass größere Unternehmen tendenziell ein höheres Sicherheitsniveau erreichen, aber selbst bei Ihnen ist ein umfassender Zero Trust-Ansatz in allen IT-Bereichen noch nicht realisiert. Dies unterstreicht, dass Zero Trust über Investitionen in Sicherheit hinausgeht und als kontinuierliche Herausforderung und strategischer Ansatz tief in die Geschäftsprozesse und -kultur integriert werden muss, um wirksam zu sein.

UNSER WEG ZU ZERO TRUST- DAS NIST FRAMEWORK:

Das NIST (National Institute of Standards and Technology) Framework bietet eine strukturierte und flexible Anleitung für Unternehmen aller Größen, insbesondere auch für mittelständische Unternehmen, um Ihre Cybersecurity zu stärken. Es besteht aus fünf Kernbausteinen, die Ihnen helfen können, sich auf den Weg zu Zero Trust zu machen:

Identifizieren (Identify):
Dieser Baustein hilft Unternehmen, Ihre Systeme, Daten, Kapazitäten und Cybersecurity-Risiken zu verstehen. Für mittelständische Unternehmen ist dies besonders wertvoll, da es Ihnen ermöglicht, Ressourcen effizient einzusetzen und sich auf die wichtigsten Risikobereiche zu konzentrieren.

Schützen (Protect):
Hierbei geht es um die Implementierung von Schutzmaßnahmen, um Services und Assets vor Cyberangriffen zu schützen. Mittelständische Unternehmen profitieren durch die Schaffung robuster Abwehrmaßnahmen, die Ihre kritischen Assets sichern und gleichzeitig den Geschäftsbetrieb aufrechterhalten.

Erkennen (Detect):
Die Fähigkeit, schnell Cybersecurity-Ereignisse zu erkennen, ist entscheidend. Für mittelständische Unternehmen bedeutet dies, dass sie schneller auf Vorfälle reagieren und Schäden minimieren können, was für die Aufrechterhaltung des Kundenvertrauens und der Geschäftskontinuität entscheidend ist.

Reagieren (Respond):
Dieser Baustein konzentriert sich auf die Entwicklung eines Plans zur Reaktion auf erkannte Cybersecurity-Ereignisse. Mittelständische Unternehmen können dadurch die Auswirkungen eines Angriffs begrenzen und eine schnellere Erholung ermöglichen.

Wiederherstellen (Recover):
Hier geht es darum, Pläne zur Wiederherstellung von Funktionen oder Services zu entwickeln, die durch Cybersecurity-Ereignisse beeinträchtigt wurden. Für mittelständische Unternehmen ist es wichtig, nach einem Angriff schnell wieder in den Normalbetrieb zurückzukehren, um wirtschaftliche Verluste zu minimieren.

IHR WEG ZU ZERO TRUST: DER ERSTE SCHRITT IN EINE SICHERERE ZUKUNFT

Das NIST Framework bietet mittelständischen Unternehmen einen erheblichen Vorteil, da es eine klare und anpassbare Anleitung bietet, um die Cybersecurity zu stärken und sich schrittweise auf Zero Trust zuzubewegen. Es hilft bei der Priorisierung von Ressourcen und Entscheidungen, die auf die spezifischen Bedürfnisse und Kapazitäten des Unternehmens zugeschnitten sind. In einer Welt, in der Cyber-Sicherheit von entscheidender Bedeutung ist, ist der Schritt zu einem Zero Trust-Modell unerlässlich. Ihr Weg dorthin ist klar und einfach:

Weg 1:

Nutzen Sie unser kostenloses Cyber Security Assessment. Tauchen Sie direkt in die Welt von Zero Trust ein und erfahren Sie, wie Sie Ihre digitale Infrastruktur effektiv schützen können. Melden Sie sich jetzt an!

+49 (0)831 540 54-321

Ganz anders:

Sichern Sie sich einen unverbindlichen Beratungstermin. Unser Expertenteam freut sich darauf, mit Ihnen gemeinsam Ihren individuellen Weg zu Zero Trust zu planen und zu realisieren.

Kontakt aufnehmen

Mit diesen Schritten sind Sie bestens aufgestellt, um Ihr Unternehmen in eine sicherere Zukunft zu führen. Wir begleiten Sie gerne auf diesem Weg.