SCALTEL

ZERO TRUST

Der Weg in eine sichere Zunkunft!

Inhalte

Wir freuen uns, Ihnen nach unserer Sommerpause einen Überblick über das erste Halbjahr unserer Webinar Reihe "Zero Trust" präsentieren zu dürfen. In den vergangenen Monaten haben wir mit höchster Sorgfalt 30 Cyber-Security Assessments analysiert und sind nun bereit, Ihnen unsere Erkenntnisse zu präsentieren. Jedes dieser Assessments wurde in einem Spinnendiagramm visualisiert, das die unzähligen Facetten der Cybersicherheit beleuchtet.

ZERO TRUST

Im Fokus stehen folgende Schlüsselbereiche:

SOC (Security Operation Center):

- Schwachstellenmanagement
- Sicherheitsereignismanagement
- Incident Response

Environment:

- Zugangskontrolle zu Gebäuden
- Gebäudesegmentierung
- Physikalisches Sicherheitsinformations-managementsystem

Identity (Identität):

- Authentifizierung
- Netzwerkzugriff
- Cloudzugriff

Applikation

- Sicheres Web-Gateway
- Sicheres E-Mail-Gateway
- Anwendungssicherheit – 2024

Devices:

- Sichtbarkeit
- Klassifizierung
- Endpunktschutz

Data:

- Graduierung
- Verschlüsselung
- Sichere Datensicherung

Netzwerk:

- Architektur
- Makrosegmentierung
- Mikrosegmentierung

ISMS (Informationssicherheits-managementsystem):

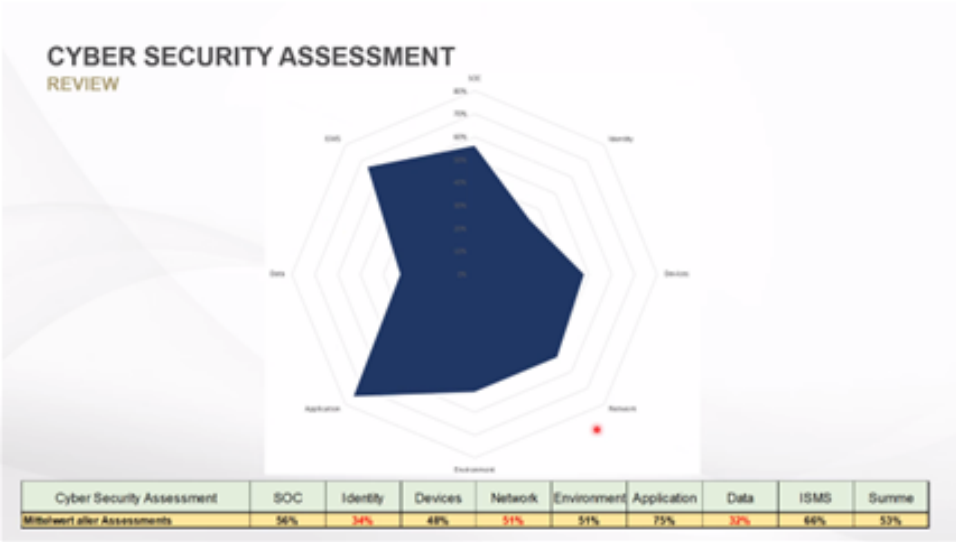
- Informationssicherheit
- Datenschutz
- Sensibilisierung der Mitarbeiter

UNSER WEG ZU ZERO TRUST

Unabhängig von der Branche wurden folgende Schlüssel-erkenntnisse gewonnen:

- Unternehmensgröße als Investitionsfaktor in die Cybersicherheit
- Unternehmen, die nach z.B. ISO27001, TISAX o.Ä. mit einem ISMS arbeiten, sind besser auf Cyber-Angriffe vorbereitet und arbeiten bereits mit Erkennungs- und Automatisierungs-Systemen
- Kaum ein Unternehmen kann eine Cyber Security Strategie mit getroffenen Maßnahmen ohne deren Umsetzung und Wirksamkeit darstellen
- Oftmals muss vorerst die Basis geschaffen werden, um die Umsetzung von Zero-Trust-Maßnahmen überhaupt anzugehen
- Je größer das Unternehmen ist, desto intensiver wurden die einzelnen Aspekte der Cybersicherheit beleuchtet.

Allgemeine Rückmeldungen zu den Cyber Security Assessments



Cyber Security Assessment	#Soc:	#Identity:	#Devices:	#Network:	#Enviroment:	#Application:	#Data:	#ISMS:	Summe
Mittelwert aller Assessments	**56%**	**34%**	**48%**	**51%**	**51%**	**75%**	**32%**	**66%**	**53%**

UNSERE SCHLUSSFOLGERUNG

SOC

Hier sind bereits Bewusstsein und Maßnahmen vorhanden, die primär die Erkennung (Sercurity Event Handling) im Fokus haben. Präventive Maßnahmen, wie ein definiertes Schwachstellen-Management, werden nicht umfassend genug umgesetzt. Ein Notfallplan mit aufgeführten Verantwortlichkeiten, Incident Response-Maßnahmen oder Notfallkommunikation ist oft nur teilweise oder gar nicht vorhanden.

Environment

Obwohl im Bereich Environment grundlegende Themen wie Zutritt oder Gebäudeüberwachung weit verbreitet sind, diese Bereiche selten in der IT verankert und laufen so nicht in die allgemeine Zero Trust Strategie mit ein.

Identity

In diesem Bereich besteht erheblicher Nachholbedarf bei der generellen Erkennung von Identitäten und deren Berechtigungsreichweite.

ISMS

In den organisatorischen Maßnahmen hat sich in den letzten Jahren viel getan. Dennoch bestehen weiterhin Lücken in den Bereichen Risikomanagementdokumentation und Berichterstattung.

Devices

Ähnlich wie im SOC-Bereich wurden bereits erste Schritte unternommen. Es wird jedoch mit den Daten nicht gearbeitet, um auf Basis einer risikobasierten Klassifizierung effektive Sicherheitsmaßnahmen abzuleiten.

Netzwerk

Nach wie vor kann innerhalb eines Netzwerkes weitestgehend unkontrolliert kommuniziert werden. Die interne Segmentierung über ein Regelwerk, wie z.B. die Abtrennung des Datacenters, der (m)IoT, etc. stellt viele Unternehmen vor eine große Herausforderung; ist aber für eine effektive Angriffserkennung zwingend erforderlich.

Data

Backup-Strategien sind vorhanden, jedoch mit Fokus auf Desaster-Recovery. Besonderes Augenmerk sollte auf den Bereich Cyber Security Recovery im Vergleich zur Katastrophenwiederherstellung gelegt werden.

Applikation

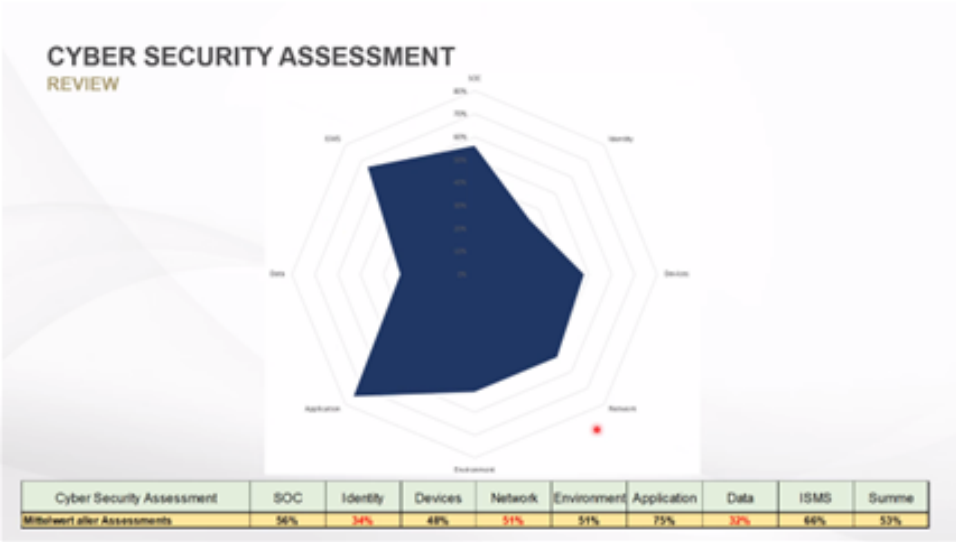
Dies ist der am weitesten entwickelten Bereich. Web- und Email-Security wird schon lange publiziert - somit sind hier die meisten Maßnahmen bereits getroffen. Im Bereich der Endpoint Security gibt es speziell beim Thema “verhaltensbasierte Analyse” Nachholbedarf.

UNSER WEG ZU ZERO TRUST

Unabhängig von der Branche wurden folgende Schlüssel-erkenntnisse gewonnen:

- Unternehmensgröße als Investitionsfaktor in die Cybersicherheit
- Unternehmen, die nach z.B. ISO27001, TISAX o.Ä. mit einem ISMS arbeiten, sind besser auf Cyber-Angriffe vorbereitet und arbeiten bereits mit Erkennungs- und Automatisierungs-Systemen
- Kaum ein Unternehmen kann eine Cyber Security Strategie mit getroffenen Maßnahmen ohne deren Umsetzung und Wirksamkeit darstellen
- Oftmals muss vorerst die Basis geschaffen werden, um die Umsetzung von Zero-Trust-Maßnahmen überhaupt anzugehen
- Je größer das Unternehmen ist, desto intensiver wurden die einzelnen Aspekte der Cybersicherheit beleuchtet.

Allgemeine Rückmeldungen zu den Cyber Security Assessments



Cyber Security Assessment	#Soc:	#Identity:	#Devices:	#Network:	#Enviroment:	#Application:	#Data:	#ISMS:	Summe
Mittelwert aller Assessments	**56%**	**34%**	**48%**	**51%**	**51%**	**75%**	**32%**	**66%**	**53%**

EINFÜHRUNG IN NIS2 - DIE DRINGLICHKEIT VERSTEHEN

Die NIS2-Richtlinie (EU) 2022/2555, die am 18. Oktober 2024 in allen EU-Staaten verbindlich wird, hat das Ziel, die Cybersicherheit von Diensten in Schlüsselsektoren zu erhöhen. Dies betrifft Unternehmen, deren Produkte oder Dienstleistungen von hoher kritischer oder kritischer Bedeutung für die Öffentlichkeit sind.

GELTUNGSBEREICH VON NIS2 - FÜR WEN IST NIS2 RELEVANT?

NIS2 betrifft Unternehmen, die in zwei Hauptkategorien unterteilt sind: Sektoren mit hoher Kritikalität und sonstige kritische Sektoren. Es ist erstaunlich, wie viele verschiedene Branchen in die Kategorie der kritischen Sektoren fallen. Hier ist eine Aufschlüsselung:

Es ist wichtig zu beachten, dass die Entscheidung, ob ein Unternehmen den Anforderungen von NIS2 unterliegt, von Schwellenwerten abhängt. Das bedeutet, dass ein Unternehmen möglicherweise nicht automatisch NIS2-konform sein muss, nur weil es sich in einem der oben genannten Sektoren befindet.

Die Schwellenwerte sind daher mit entscheidend, um festzustellen, ob Ihr Unternehmen den Anforderungen von NIS2 gerecht werden muss oder nicht, da diese in den EU Staaten unterschiedlich definiert sein können. Daher empfehlen wir, die genauen Schwellenwerte und Vorschriften in Ihrem Land zu überprüfen, um sicherzustellen, dass Ihr Unternehmen ordnungsgemäß NIS2 umsetzt, wenn es dazu verpflichtet ist.

In Deutschland werden die genauen Schwellwerte und Umsetzungsrichtlinien durch die Gesetze NIS2UmsuCG und KRITIS-DachG definiert. Diese Gesetze legen fest, wie die Schwellenwerte, beispielsweise durch Branchenstandards, festgelegt werden. Es ist jedoch wichtig zu beachten, dass zum Zeitpunkt des Webinars diese Gesetze noch nicht vom Bundestag verabschiedet wurden, so dass sich hier noch Änderungen ergeben können.

Die bisher geltenden Schwellenwerte können auf der Website des Bundesamts für Sicherheit in der Informationstechnik (BSI) abgerufen werden:

[Link zur Website](https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Sektorspezifische-Infos-fuer-KRITIS-Betreiber/sektorspezifische-infos-fuer-kritis-betreiber_node.html).

NIS2-ANFORDERUNGEN - WAS MÜSSEN SIE UMSETZEN?

Unabhängig von der Branche wurden folgende Schlüsselerkenntnisse gewonnen:

Risikomanagement im Bereich der Cybersicherheit

Hierbei geht es im Wesentlichen, um die die Einführung eines IT Risikomanagements, welches in Form eines Informationssicherheitsmanagement-system (ISMS) abgebildet wird. Die NIS2 Richtlinie nennt hier z.B. die Anwendung eines ISMS nach ISO 27000. Dies beinhaltet die Einführung eines IT-Notfall- und Riskomanagements, sowie Implementierung geeigneter technischer und organisatorischer Maßnahmen um den kontinuierlichen IT Betrieb sicherstellen zu können.

Berichtspflichten

Von der NIS2 betroffene Unternehmen müssen Sicherheitsvorfälle binnen 24 Stunden an die zuständigen Aufsichts-behörden melden, binnen 72 Stunden den Behörden einen detaillierten Bericht über Art und Umfang des Vorfalls einreichen und spätestens einen Monat nach dem Auftreten des Vorfalls einen vollständigen Abschlussbericht bei der Behörde einreichen erstellen.

KONSEQUENZ UNTERSTÜTZUNG MEHRWERT

Konsequenzen der Nichteinhaltung
Warum sollten Sie NIS2 beachten?

Die Nichteinhaltung von NIS2 kann drastische Konsequenzen haben, darunter Bußgelder von bis zu 10.000.000 € oder 2% des weltweiten Jahresumsatzes (jeweils das höhere) für Unternehmen in Sektoren mit hoher Kritikalität und bis zu 7.000.000 € oder 1,4% des weltweiten Jahresumsatzes (jeweils das höhere) für sonstige kritische Sektoren. Es besteht auch das Risiko von Sanktionen durch die Aufsichtsbehörden bis hin zur Anordnungen den kritischen Geschäftsbetrieb einzustellen.

Unterstützung durch SCALTEL SNS Systems
Ihr Weg zur Compliance

SCALTEL SNS Systems bietet umfassende Unterstützung bei der Implementierung eines Informationssicherheitsmanagementsystems (ISMS) nach ISO 27001, CISIS12, BAIT, VAIT, TISAX oder B3S. Unser bewährter 18-Punkte-Plan führt Ihr Unternehmen schrittweise zur Zertifizierungsreife. Wir bieten Expertise, Schulungen und Sensibilisierung, um sicherzustellen, dass Ihre Cybersicherheit den Anforderungen von NIS2 gerecht wird.

Mehrwerte von SCALTEL SNS Systems
Warum uns wählen?

Mit unserem 360° Informationssicherheits- und Datenschutz Check erhalten Sie eine schnelle Übersicht über Ihren Handlungsbedarf. Unsere zertifizierten Experten haben langjährige Erfahrung in den Bereichen ISMS und Datenschutz. Wir bieten Schulungen und Sensibilisierung für Ihre Mitarbeiter sowie eine beschleunigte Zertifizierungsreife durch bewährte Best Practices.

Mit unserem 360° Informationssicherheits- und Datenschutz Check erhalten Sie eine schnelle Übersicht über Ihren Handlungsbedarf. Unsere zertifizierten Experten haben langjährige Erfahrung in den Bereichen ISMS und Datenschutz. Wir bieten Schulungen und Sensibilisierung für Ihre Mitarbeiter sowie eine beschleunigte Zertifizierungsreife durch bewährte Best Practices.

Unsere nächsten Themen aus

DER ZERO TRUST WELT:

12. Oktober 2023
IT-Risikomanagement
(Fokus auf Geräten)

26. Oktober 2023
Zugangsmanagement
(Fokus auf Netzwerk)

16. November 2023
Datensicherung & Backup-Vault
(Fokus auf Daten)