CISCO
SECURE

NIS-2 Richtlinie Anforderungen erfüllen mit Cisco

CISCO SECURITY WHITE PAPER

NOVEMBER 2023

Haftungsausschluss

Dieses Dokument bietet Anleitungen für das Erfüllen der NIS-2 Richtlinie (NIS-2-RL). Die vorgestellte Hardware, Software und Produkte sind zum Zeitpunkt des Verfassens dieses Artikels die am meisten empfohlenen. Die in diesem Dokument vorgeschlagenen Produkte können sich in Zukunft ändern.

Kunden und Partner sind dafür verantwortlich, zu bestätigen, dass die Hardware- und Softwarekonfiguration alle erforderlichen Komponenten enthält, um die Lösungsanforderungen zu erfüllen. Bitte beachten Sie die Links in diesem Dokument.

Alle gedruckten Kopien und Duplikate dieses Dokuments gelten als unkontrolliert. Siehe die aktuelle Online-Version für die neueste Version.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS DESCRIBED IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. THIS DOCUMENT IS PROVIDED “AS IS.”
ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS, IMPLIED, OR STATUTORY INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, PUNITIVE, EXEMPLARY, OR INCIDENTAL DAMAGES UNDER ANY THEORY OF LIABILITY, INCLUDING WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OF OR INABILITY TO USE THIS DOCUMENT, EVEN IF CISCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Aus dem Englischen übersetzt, beitragende Autoren:

Andreas Hack | Technical Solutions Architect | Cybersecurity
Clemens Geyer | Technical Solutions Architect | Collaboration
Version 30.11.2023

Cisco Systems Austria GmbH

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

1. Executive Summary

Das vorliegende Whitepaper ist ein Appendix zum bestehenden “Die NIS-2-RL und ihre Anforderungen an Unternehmen – White Paper“ von Schiefer Rechtsanwälte GmbH. Die Kapitel sind zur leichteren Lesbarkeit analog gehalten und ergänzen einander. Dieses Cisco Whitepaper hat den Fokus auf die technische Machbarkeit und deren Umsetzung, den Stand der Technik sowie auf Referenzarchitekturen, Standards und Normen zu referenzieren. Ferner soll dieses Cisco Whitepaper Kunden helfen, die NIS-2-RL Anforderungen technisch einzuordnen und umzusetzen.

2. Ausgangssituation sowie Zweck und Struktur des White Papers

Als anerkannter Innovator und Marktführer im Bereich Cybersicherheit bietet Cisco umfassende Architekturen, Lösungen, Produkte und Dienstleistungen an, die auf die lokale Umsetzung der Richtlinie in verschiedenen Ländern abgestimmt sind. Bezugnehmend auf die in Österreich geltende NIS-2 Richtlinie, sind in den folgenden Abschnitten Maßnahmen und Referenz Architekturen beschrieben, wie Cisco Sie unterstützen kann diese zu erfüllen.
Die Struktur ist analog zum White Paper „Die NIS-2-RL und ihre Anforderungen an Unternehmen“ von Schiefer Rechtsanwälte GmbH, ergänzt die rechtlichen Anforderungen um die Bereiche in denen Cisco Ihnen einen technologischen Mehrwert bieten kann. Kapitel, in denen Technologie keine Rolle spielt, wurden freigelassen.

3. Bisherige Rechtslage: NIS-1-RL und das NISG

3.1 NIS-1-RL: Erste Schritte in der Cybersicherheit

Die benutzerfreundliche Sicherheitsreferenzarchitektur Secure Access for Everyone (SAFE) kann Ihnen dabei helfen, Ihre Sicherheitsstrategie und -bereitstellung zu vereinfachen.

Secure Access for Everyone (SAFE)

Diese Cisco-Referenzarchitektur für Sicherheit bietet benutzerfreundliche visuelle Symbole, die Ihnen beim Entwerfen einer sicheren Infrastruktur für Edge, Zweigstelle, Rechenzentrum, Campus, Cloud und WAN helfen. Das Framework umfasst operative Bereiche wie Management, Sicherheitsinformationen, Compliance, Segmentierung, Bedrohungsabwehr und sichere Dienste. SAFE-Lösungen wurden bei Cisco bereitgestellt, getestet und validiert und bieten Anleitungen, Best Practices und Konfigurationsschritte.

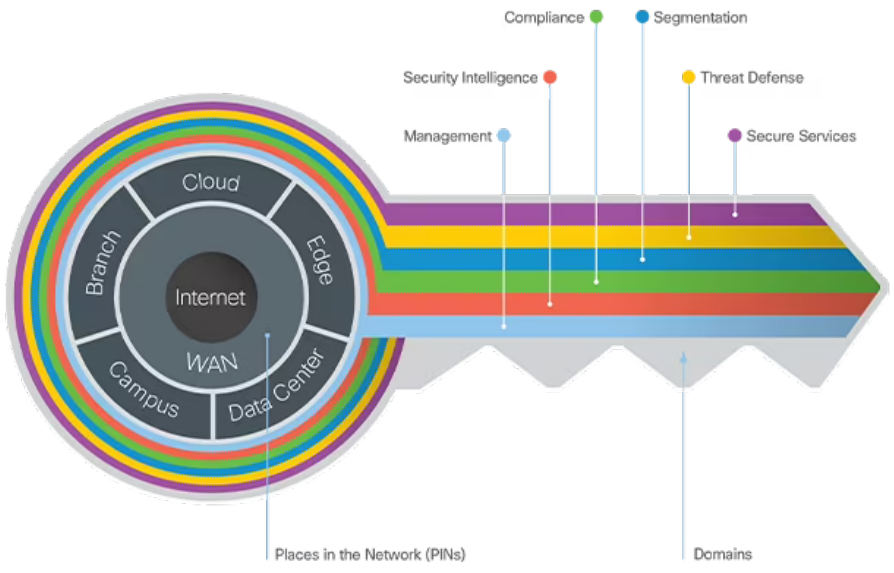

Abbildung 1: Cisco Secure Access for Everyone (SAFE)

Der SAFE-Schlüssel organisiert die Sicherheit mithilfe von zwei Kernkonzepten: Orte im Netzwerk (PINs) und sichere Domänen.

PINs verweisen auf Beispiele für Standorte, die in Netzwerken zu finden sind, und auf die Infrastruktur, die für deren Erstellung erforderlich ist:

- Rechenzentrum
- Zweigstelle (Branch)
- Campus
- WAN
- Internet-Edge
- Cloud

Sichere Domains sind Einsatzbereiche zum Schutz dieser Standorte. Dabei handelt es sich um Sicherheitskonzepte, die ein ganzes Netzwerk durchziehen:

- Management
- Sicherheitsinformationen
- Einhaltung
- Segmentierung
- Bedrohungsabwehr
- Sichere Dienste

SAFE Overview Guide
https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_safe.html
bzw. auch als PDF verfügbar:
https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-overview-guide.pdf

SAFE Secure Cloud Architecture Guide

Die Secure Cloud ist ein Ort im Netzwerk (PIN), an dem ein Unternehmen Daten zentralisiert und Dienste für Unternehmen erbringt. Cloud-Dienstanbieter hosten Rechenzentrumsdienste in der Secure Cloud. Dieser Leitfaden befasst sich mit sicheren Cloud-Geschäftsabläufen und der Sicherheit, die zu ihrer Verteidigung eingesetzt wird. Der Schwerpunkt dieses Leitfadens liegt auf den Sicherheitskontrollen, die erforderlich sind, um „Sicherheit für die Cloud“ bereitzustellen.

Die Secure Cloud ist einer der sieben Orte im Netzwerk von SAFE. SAFE ist ein ganzheitlicher Ansatz, bei dem sichere PINs die physische Infrastruktur modellieren und sichere Domänen die betrieblichen Aspekte eines Netzwerks darstellen.

Der Leitfaden zur Secure Cloud-Architektur bietet:

- Geschäftsabläufe für die Cloud
- Cloud-Bedrohungen und Sicherheitsfunktionen
- Business-Flow-Sicherheitsarchitektur
- Designbeispiele und vorgeschlagene Komponenten

SAFE bietet den Schlüssel zur Vereinfachung der Cybersicherheit in Secure Places in the Network (PINs) für die Infrastruktur und Sichere Domains für die Betriebsführung.

SAFE vereinfacht die Sicherheit, indem es mit Geschäftsabläufen beginnt und dann ihre jeweiligen Bedrohungen mit entsprechenden Sicherheitsfunktionen, Architekturen und Designs angeht. SAFE bietet ein ganzheitliches und verständliches Framework an.

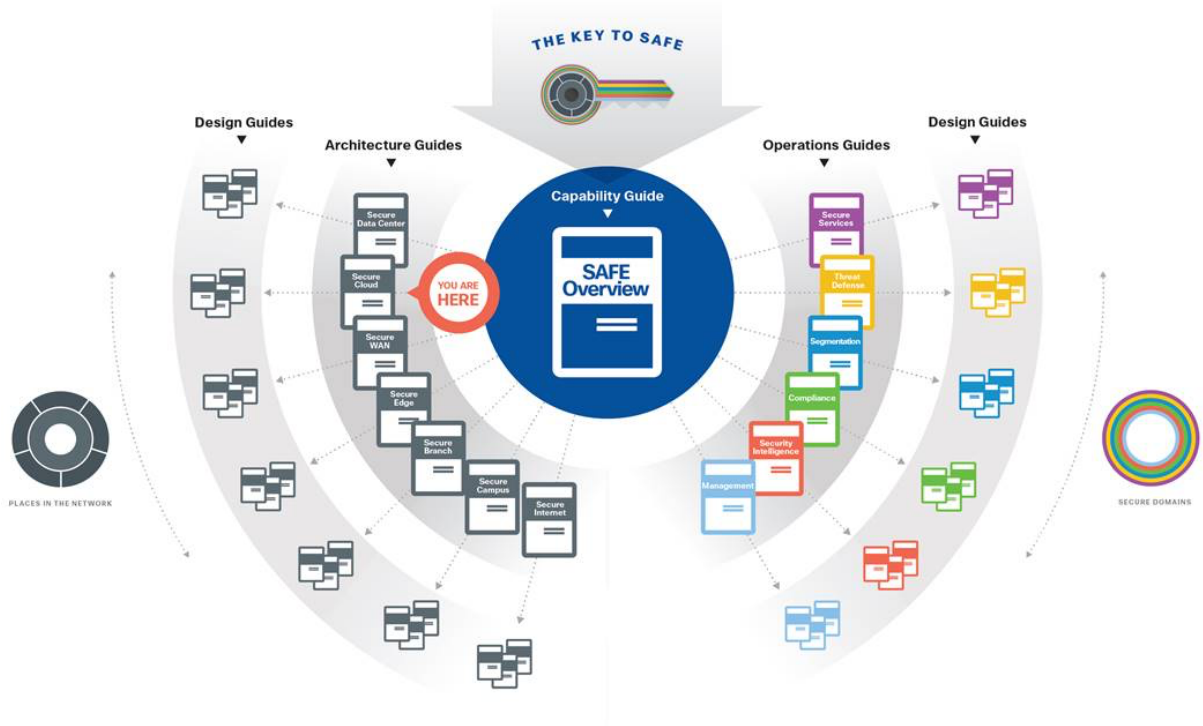

Abbildung 2: SAFE Guidance Hierarchy

Die SAFE Guidance Hierarchy referenziert im Wesentlichen auf:

- Capability Guide
- Architecture Guides sowie die referenzierenden Design Guides
- Operations Guides sowie die referenzierenden Design Guides

Cloud-Verantwortung

Der Kunde wählt das Cloud-Service-Modell aus, das den Geschäftsanforderungen am besten entspricht. Die folgende Abbildung stellt das Verantwortungsmodell zwischen dem Cloud-Dienstanbieter und dem Kunden dar.

SaaS (Software as a Service)	FaaS (Functions as a Service)	PaaS (Platform as a Service)	CaaS (Container as a Service)	IaaS (Infrastructure as a Service)	On-Prem (private cloud)
Functions	Functions	Functions	Functions	Functions	Functions
Applications	Applications	Applications	Applications	Applications	Applications
Runtime	Runtime	Runtime	Runtime	Runtime	Runtime
Middleware or Containers	Middleware or Containers	Middleware or Containers	Middleware or Containers	Middleware or Containers	Middleware or Containers
Operating System	Operating System	Operating System	Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking	Networking	Networking

Cloud Service Provider Responsible

Customer Responsible

Customer and Cloud Service Provider have Shared Responsibility

Abbildung 3: Cloud Verantwortung

Sicherheitsfunktionen in der Cloud

Die Angriffsfläche der Cloud wird durch die Geschäftsabläufe definiert und umfasst die vorhandenen Personen und Technologien. Die Sicherheitsfunktionen (Cloud Security Capabilities), die zur Reaktion auf die Bedrohungen erforderlich sind, sind in Abbildung 4 dargestellt. Die Platzierung dieser Funktionen wird im Abschnitt „Architektur“ erläutert.

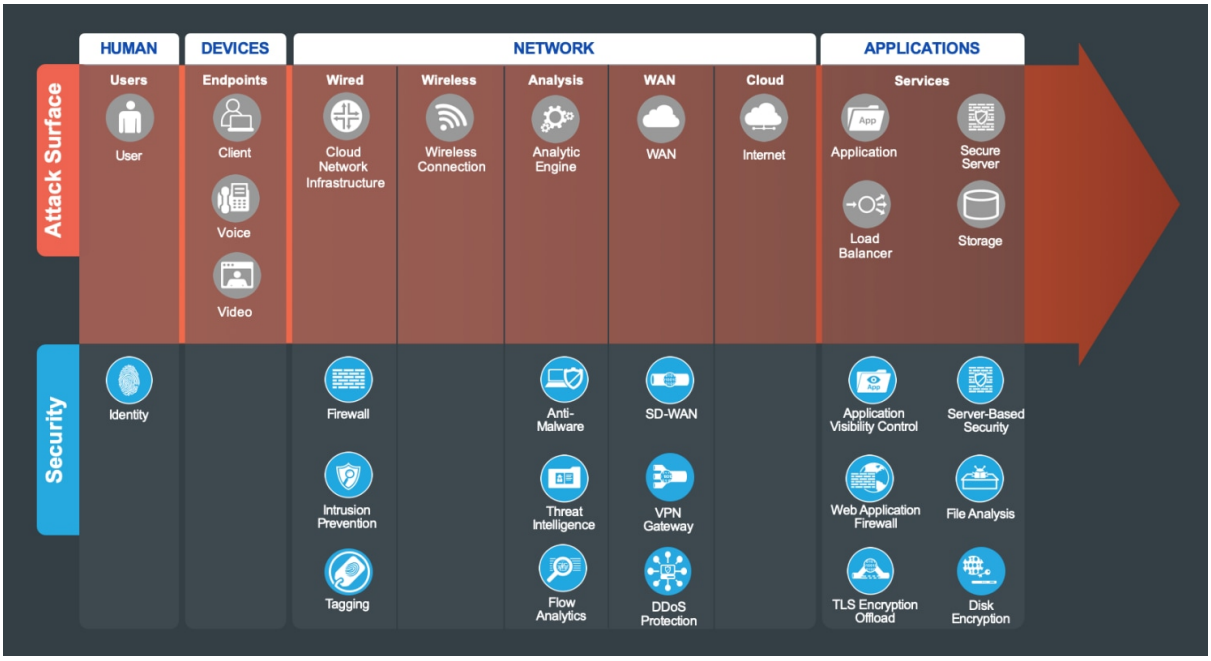

Abbildung 4: Attack Surface and Security Capabilities

Die Architektur

SAFE unterstreicht die Herausforderungen bei der Sicherung des Unternehmens. Es erweitert herkömmliche Netzwerkdiagramme um eine sicherheitsorientierte Sicht auf das Unternehmensgeschäft. Die Secure Cloud-Architektur ist eine logische Gruppierung von Sicherheits- und Netzwerktechnologie, die geschäftliche Anwendungsfälle unterstützt.

Die Sicherheitsarchitektur von SAFE Business Flow stellt einen Sicherheitsschwerpunkt dar. Eine SAFE-Sicherheitsarchitektur kann auf vielen verschiedenen Netzwerkarchitekturen beruhen.

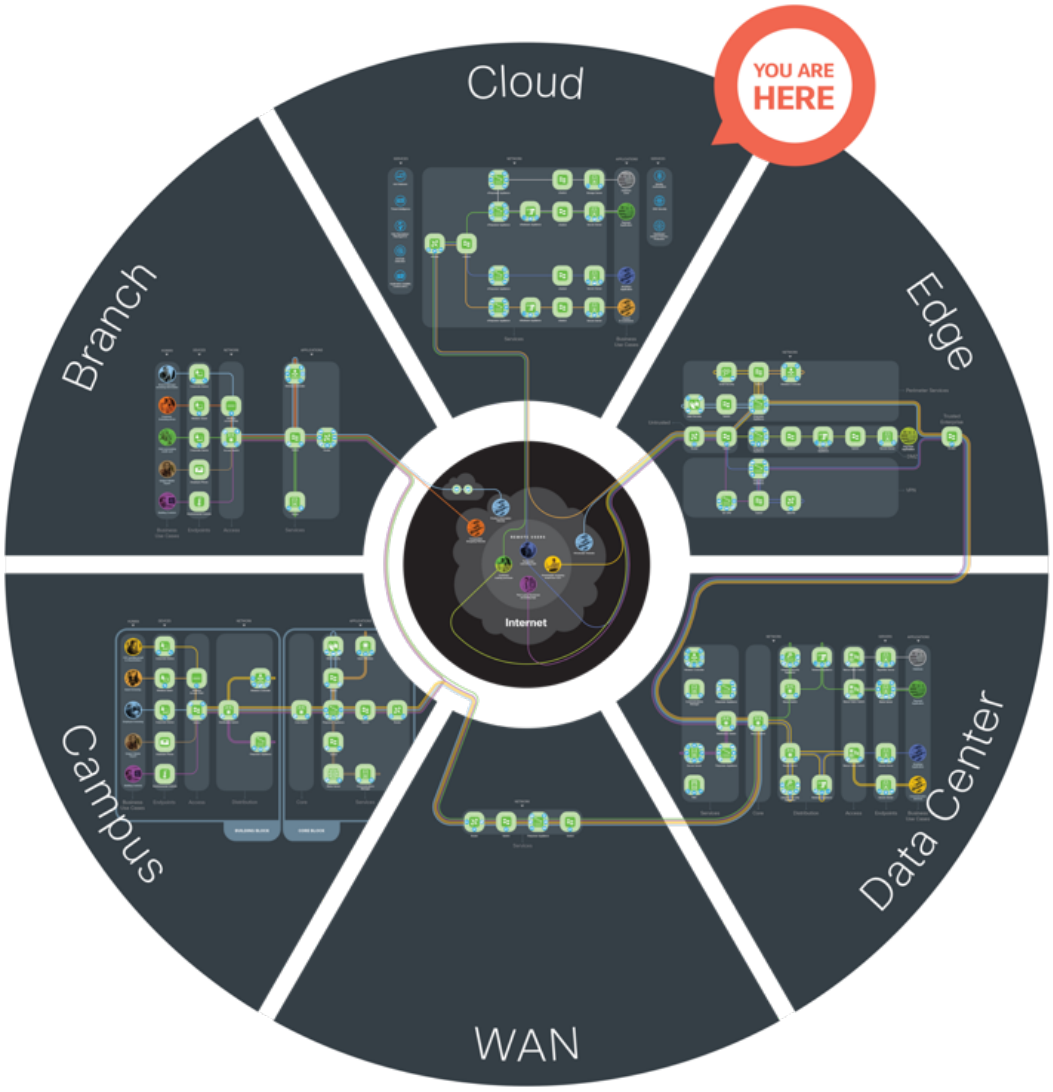

Abbildung 5: SAFE-Modell

Das SAFE-Modell vereinfacht die Komplexität im gesamten Unternehmen, indem es Orte im Netzwerk (PINs) definiert, die gesichert werden müssen.
https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/safe-secure-cloud-architecture-guide.html

Sichere Cloud

Die Secure Cloud-Architektur weist die folgenden Merkmale auf:

- Transparenz durch zentralisierte Verwaltung, Analyse und gemeinsame Dienste
- Ein Kern, der Verteilungs- und anwendungszentrierte Schichten verbindet
- Softwaredefinierte Netzwerksegmentierung
- Softwaredefinierte Anwendungssegmentierung
- Virtuelle Server, die eine sichere Netzwerkzugriffskonnektivität erfordern

Menschen und Geräte sind Teil der Angriffsfläche, aber nicht Teil der Architektur innerhalb der sicheren Cloud.

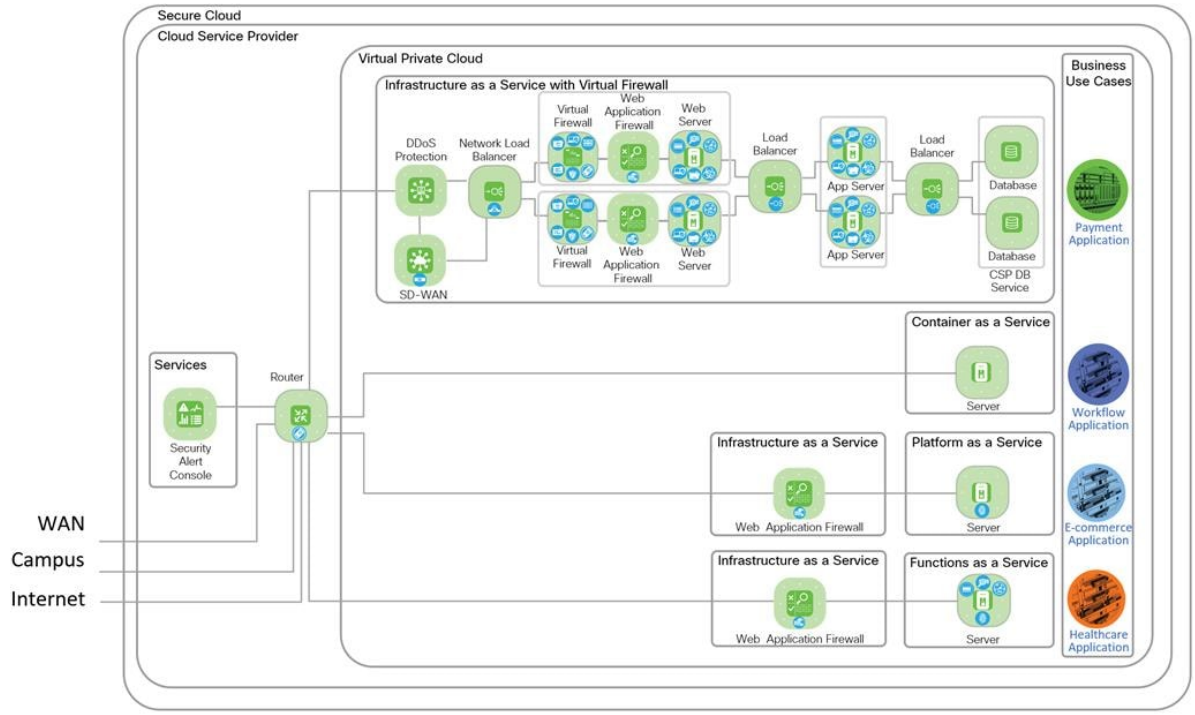

Abbildung 6: Secure Cloud-PIN

Die Geschäftsabläufe und Sicherheitsfunktionen der Secure Cloud sind in einer logischen Architektur angeordnet. Geschäftsanwendungsfälle durchlaufen die grünen Architektursymbole mit den erforderlichen blauen Sicherheitsfunktionen.

Angriffsfläche

Die Angriffsfläche der Secure Cloud (Abbildung 6) besteht aus Menschen, Geräten, Netzwerk und Anwendungen. Ein erfolgreicher Einbruch gibt einem Angreifer die „Schlüssel zum Königreich".
Zur Sicherheit gehören folgende Überlegungen:

- Menschliche Administratoren können sich überall befinden
- Für Anwendungen, die in der öffentlichen Cloud gehostet werden, ist Netzwerksicherheit erforderlich
- Anwendungen und Daten enthalten wichtige Unternehmensinformationen
- Die Anwendungsorchestrierung zentralisiert die Kontrolle über Sicherheits-, Netzwerk- und Serverelemente in einem einzigen kritischen Ziel

In den folgenden Abschnitten wird die Sicherheitsfunktion erläutert, die die mit jedem Teil der Angriffsfläche verbundenen Bedrohungen abwehrt.

Menschen

Typischerweise sind Menschen Administratoren für das sichere Rechenzentrum, die sichere Cloud und öffentliche SaaS-Anwendungen.
Keine noch so hohe Technologie kann erfolgreiche Angriffe verhindern, wenn die Administratoren selbst kompromittiert werden. Administratoren, die verärgert (gefeuert, degradiert, gemobbt, ideologisch) oder kompromittiert (Erpressung, Drohungen, Bestechung) sind oder deren Zugangsdaten gestohlen wurden (Phishing, Keylogger, Wiederverwendung von Passwörtern), stellen das größte Risiko für die Sicherheit eines Unternehmens dar.

Administratoren haben eine höhere Zugriffsebene als normale Benutzer, was zusätzliche Kontrollen erfordert:

- Multi-Faktor-Authentifizierung
- Eingeschränkter Zugriff auf die Jobfunktion
- Protokollierung von Administratoränderungen

- Dedizierte, eingeschränkte Arbeitsplätze
- Entfernung alter Administratorkonten

Die primäre Sicherheitsfunktion ist Identität. Eine der Hauptbedrohungen ist der „unautorisierte Netzwerkzugriff“. Um dieser Bedrohung entgegenzuwirken, ist eine starke Identitätslösung erforderlich.

Geräte

Das Gerät des Administrators (d. h. Laptop, Tablet) wird verwendet, um auf Tools zuzugreifen, mit denen Administratoren Systeme steuern und überwachen, die die Geschäftsanwendungen warten und sichern, unabhängig davon, ob es sich um sichere Rechenzentren, sichere Clouds oder öffentliche SaaS-Anwendungen handelt. Administratoren stellen über eine sichere Konnektivität mit starker Verschlüsselung (SSH, TLS, VPN) und Multi-Faktor-Authentifizierung von einer Vielzahl von Geräten aus eine Verbindung zu zentralen Verwaltungssystemen her.
Die primären Sicherheitsfunktionen sind clientbasierte Sicherheit und Statusbewertung für das Gerät. Client-basierte Sicherheit umfasst VPN-Client-, Anti-Malware- und Secure Internet Gateway-Funktionen.

Netzwerk

Das Netzwerk befindet sich in einer virtuellen privaten Cloud, die von einem Cloud-Dienstanbieter gehostet wird. Zum Schutz der Anwendung in der Cloud sind die grundlegenden Funktionen Firewall, Intrusion Prävention und Tagging erforderlich. Die meisten Cloud-Dienstanbieter bieten Standard-Firewall-Funktionen für die verschiedenen von ihnen angebotenen Cloud-Diensttypen. Für IaaS-Bereitstellungen wird eine virtuelle Firewall mit L4-L7-Firewall-Schutzfunktionen mit integrierter Intrusion Prävention in derselben virtuellen Maschine empfohlen. Die Tagging-Funktion variiert je nach Cloud-Dienst und kann Folgendes umfassen: VLANs, VXLANs oder Sicherheitsgruppen-Tags (TrustSec).
Zu den grundlegenden Funktionen gehören Anti-Malware, Threat Intelligence und Flow Analytics. Eine der Hauptbedrohungen ist die „Verbreitung von Malware“. Daher ist eine Anti-Malware-Erkennung des Netzwerkverkehrs erforderlich. Um dieser Bedrohung entgegenzuwirken, sollte die Anti-Malware-Lösung im Einklang mit dem Datenverkehr arbeiten.
Threat Intelligence wird für alle Lösungskomponenten empfohlen und sollte auf einen gemeinsamen Intelligence-Feed zurückgreifen, um über Cyber-Bedrohungen auf dem Laufenden zu bleiben. Die Analyse des Datenverkehrs ist der Schlüssel zur Sichtbarkeit. Sie können sich nicht schützen, wenn Sie ihn nicht sehen können. Zur Analyse des Datenverkehrs zur und innerhalb der virtuellen privaten Cloud, in der die Anwendungen gehostet werden, wird eine Cloud Analytics-Plattform empfohlen, die Analysen verschiedener CSPs sowie lokaler Rechenzentren zusammenfassen kann.

Anwendungen

Die Server sind die Endpunkte in der Cloud, die Webdienste, Anwendungen und Datenbanken hosten. Die Zugriffsmöglichkeiten, um sie zu sichern, sind serverbasierte Sicherheit und Statusbewertung. Serverbasierte Sicherheit erfordert Anti-Malware, hostbasierte Firewall, Statusbewertung und Patching, Cloud-Sicherheit und Festplattenverschlüsselung.
Um den Zugriff auf Anwendungen über die grundlegenden Funktionen und Zugriffsfunktionen hinaus zu sichern, müssen Geschäftsfunktionen bereitgestellt werden, um die durch die Geschäftspraxis verursachten Geschäftsrisiken zu verwalten. Die primären Sicherheitsfunktionen sind Application Visibility Control, Web Application Firewall, TLS Offload und File Analysis.

Zusammenfassung

Heutzutage werden Unternehmen durch immer ausgefeiltere Angriffe bedroht. Öffentliche Cloud-Dienste, die Geschäftsanwendungen hosten, geraten ins Visier, weil sie die Daten des Unternehmens speichern. Die Secure Cloud-Architektur von Cisco schützt das Unternehmen vor entsprechenden Bedrohungen mithilfe eines Architekturansatzes, der die Einschränkungen eines Einzelproduktangebots überwindet. SAFE ist die Sicherheitsreferenzarchitektur von Cisco, die die Sicherheitsherausforderungen von heute vereinfacht und sich auf die Bedrohungen von morgen vorbereitet.

Weitere Informationen zum Thema SAFE Secure Cloud Architecture finden Sie hier:
https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/safe-secure-cloud-architecture-guide.html

4. Überblick NIS-2-RL – Was ist Neu?

Siehe White Paper „Die NIS-2-RL und ihre Anforderungen an Unternehmen“ Schiefer Rechtsanwälte GmbH

5. Der erweiterte Anwendungsbereich der NIS-2-RL

5.1 Cybersicherheit: Vom Nischenthema zur „Chefsache“

5.2 Erfasste Einrichtungen

5.2.1 Kumulative Voraussetzungen

5.2.2 Einrichtungen im Sinne der Anhänge I und II der NIS-2-RL

Die Cisco Referenzarchitekturen für Betreiber wesentlicher Dienste:

- Energie
  - Elektrizität, Fernwärme und -kälte
    - ⇒ Grid Security Design Guide
      https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Grid_Security/DG/DA-GS-DG/DA-GS-DG.html
    - ⇒ Grid Security Implementation Guide
      Grid Security Requirements and Use Cases
      https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Grid_Security/IG/DA-GS-IG/DA-GS-IG.html
      Substation Automation Local Area Network and Security Cisco Validated Design
      https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Utilities/SA/2-3-2/CU-2-3-2-DIG/CU-2-3-2-DIG.html
    - ⇒ Cybersecurity for Utilities
      https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer/portfolio-explorer-for-utilities.html?s=explore-the-use-cases&u=cybersecurity
    - ⇒ Asset Visibility
      https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer/portfolio-explorer-for-utilities.html?s=explore-the-use-cases&u=asset-visibility
    - ⇒ Video Surveillance
      https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer/portfolio-explorer-for-utilities.html?s=explore-the-use-cases&u=video-surveillance
  - Erdöl, Erdgas, Wasserstoff
    - ⇒ Cybersecurity for Oil & Gas
      https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer/portfolio-explorer-for-oil-and-gas.html?s=explore-the-use-cases&u=cybersecurity
- Verkehr
  - Straßenverkehr
    - ⇒ Connected Communities Infrastructure - General Solution Design Guide
      https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/General/cci-dg/cci-dg.html
    - ⇒ Connected Communities Infrastructure - Roadways Solution Design Guide
      https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/Roadways/cci-dg_roadways/cci-dg_roadways.html
    - ⇒ Validated Design for Roadways and Intersections
      https://www.cisco.com/c/en/us/solutions/design-zone/industries/roadways-intersections.html?ccid=cc001023
  - Schienenverkehr
    - ⇒ Cisco Connected Rail Solution Brief
      https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-industry-solutions/solution-overview-c22-744756.html?dtid=oblgblg001259
    - ⇒ Connected Communities Infrastructure – Rail Solution Design Guide
      https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/Rail/cci-dg_rail/cci-dg_rail.html

        - ⇒ Connected Trackside: Delivering resilience and security https://blogs.cisco.com/internet-of-things/connected-trackside-delivering-resilience-and-security
    - Schiffsverkehr
        - ⇒ Connected Ports and Terminals reference architecture https://www.cisco.com/c/en/us/solutions/collateral/internet-of-things/terminal-ops-digitization-security-sb.html#ConnectedPortsandTerminalsreferencearchitecture
    - Luftverkehr
        - ⇒ Connected Ports and Terminals reference architecture https://www.cisco.com/c/en/us/solutions/collateral/internet-of-things/terminal-ops-digitization-security-sb.html#ConnectedPortsandTerminalsreferencearchitecture
- Bankwesen und Finanzmarktinfrastrukturen
    - ⇒ Securing a Resilient Financial Services Enterprise https://www.cisco.com/c/en/us/solutions/collateral/secure-the-enterprise/securing-fs-enterprise.html
    - ⇒ Cybersecurity for Financial Services https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer/portfolio-explorer-for-financial-services.html?s=explore-the-use-cases&u=cybersecurity
    - ⇒ Video surveillance and safety https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer/portfolio-explorer-for-financial-services.html?s=explore-the-use-cases&u=video-surveillance-and-safety&o=technical-overview
    - ⇒ E-communication compliance https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer/portfolio-explorer-for-financial-services.html?s=explore-the-use-cases&u=e-communication-compliance&o=technical-overview
    - ⇒ Secure Branch https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer/portfolio-explorer-for-financial-services.html?s=explore-the-use-cases&u=secure-branch&o=technical-overview
- Gesundheitswesen
    - ⇒ Cybersecurity Threats Top of Mind for Healthcare https://www.cisco.com/c/en/us/solutions/collateral/industries/healthcare/healthcare-cybersecurity.html
    - ⇒ Cybersecurity for Healthcare https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer/portfolio-explorer-for-healthcare.html?s=explore-the-use-cases&u=cybersecurity-for-healthcare&o=technical-overview
    - ⇒ Medical Device and IoT Security https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer/portfolio-explorer-for-healthcare.html?s=explore-the-use-cases&u=medical-device-and-iot-security
    - ⇒ Video Surveillance and Physical Security https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer/portfolio-explorer-for-healthcare.html?s=explore-the-use-cases&u=video-surveillance-and-physical-security
- Trinkwasser
    - ⇒ Industrial Control Systems Security and Resilience https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer/portfolio-explorer-for-government.html?s=explore-the-use-cases&r=secure-government&u=industrial-control-systems-security-and-resiliency&o=technical-overview
- Abwasser
    - ⇒ Industrial Control Systems Security and Resilience https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer/portfolio-explorer-for-government.html?s=explore-the-use-cases&r=secure-government&u=industrial-control-systems-security-and-resiliency&o=technical-overview
- Digitale Infrastruktur

- ⇒ Network Security and Trust for Service Providers
  https://www.cisco.com/c/en/us/solutions/service-provider/service-provider-security-solutions/index.html
- ⇒ Secure Datacenter Architecture Design Guide
  https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/safe-secure-dc-architecture-guide.html
- ⇒ Zero Trust Network and Cloud Security Design Guide
  https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/zt-network-cloud-dg.html

- Verwaltung von IKT-Diensten B2B
  - ⇒ Connected Communities Infrastructure – General Solution Design Guide
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/General/cci-dg/cci-dg.html
  - ⇒ Connected Communities Infrastructure implementation guide
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/IG/cci-ig/cci-ig.html
  - ⇒ Connected Communities Infrastructure – Cities Solution Design Guide
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/Cities/cci-dg/cci-dg.html
- Öffentliche Verwaltung
  - ⇒ Connected Communities Infrastructure – General Solution Design Guide
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/General/cci-dg/cci-dg.html
  - ⇒ Connected Cities – General Solution Design Guide
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/Cities/cci-dg/cci-dg.html
  - ⇒ Public Safety
    https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer/portfolio-explorer-for-government.html?s=explore-the-use-cases&r=secure-government&u=public-safety&o=technical-overview
  - ⇒ Industrial control systems security and resiliency
    https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer/portfolio-explorer-for-government.html?s=explore-the-use-cases&r=secure-government&u=industrial-control-systems-security-and-resiliency&o=technical-overview
  - ⇒ Security Resilience for Government zero trust
    https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer/portfolio-explorer-for-government.html?s=explore-the-use-cases&r=secure-government&u=security-resilience-for-government-zero-trust
  - ⇒ Threat detection and incident response
    https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer/portfolio-explorer-for-government.html?s=explore-the-use-cases&r=secure-government&u=threat-detection-and-incident-response
  - ⇒ Trusted internet connections
    https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer/portfolio-explorer-for-government.html?s=explore-the-use-cases&r=secure-government&u=trusted-internet-connections&o=technical-overview
  - ⇒ Education cloud security
    https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer/portfolio-explorer-for-education-featuring-government.html?s=explore-the-use-cases&u=education-cloud-security&o=technical-overview
- Weltraum

Die Cisco Referenzarchitekturen für Betreiber wichtiger Dienste:

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Produktion, Herstellung und Handel mit chemischen Stoffen

- ⇒ Industrial Automation Security Design Guide
  https://www.cisco.com/c/en/us/td/docs/Technology/industrial-automation-security-design-guide.html
- ⇒ Industrial Security Implementation Guide
  https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/IA_Security/IA_Security_IG/IA_Security_IG.html
- ⇒ Industrial Security Portfolio Explorer
  https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer/portfolio-explorer-for-manufacturing-featuring-government.html?s=explore-the-use-cases&u=industrial-security-foundation&o=technical-overview
- ⇒ Industrial Security Solution Overview
  https://www.cisco.com/c/en/us/products/collateral/security/industrial-security-cvd-so.html
- ⇒ Industrial Security Design Guide
  https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/IA_Security/IA_Security_DG/IA_Security_DG.html

- Produktion, Verarbeitung und Vertrieb von Lebensmitteln
- Verarbeitendes Gewerbe / Herstellung von Waren
  - ⇒ Industrial Automation Security Design Guide
    https://www.cisco.com/c/en/us/td/docs/Technology/industrial-automation-security-design-guide.html
  - ⇒ Industrial Security Implementation Guide
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/IA_Security/IA_Security_IG/IA_Security_IG.html
  - ⇒ Industrial Security Portfolio Explorer
    https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer/portfolio-explorer-for-manufacturing-featuring-government.html?s=explore-the-use-cases&u=industrial-security-foundation&o=technical-overview
  - ⇒ Industrial Security Solution Overview
    https://www.cisco.com/c/en/us/products/collateral/security/industrial-security-cvd-so.html
  - ⇒ Industrial Security Design Guide
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/IA_Security/IA_Security_DG/IA_Security_DG.html
- Anbieter digitaler Dienste
  - ⇒ Network Security and Trust for Service Providers
    https://www.cisco.com/c/en/us/solutions/service-provider/service-provider-security-solutions/index.html
- Forschung

6. Die unternehmensbezogenen Pflichten der NIS 2-RL

6.1 Allgemeines

6.2 Vom spezifischen zum umfassenden Netzwerkschutz

6.3 Risikomanagementmaßnahmen

6.3.1 „Risk-based-Approach“ (Verhältnismäßigkeit)

Risikomanagement in der Cybersicherheit ist die Praxis der Identifizierung und Minimierung potenzieller Risiken oder Bedrohungen für vernetzte Systeme, Daten und Benutzer. Die Einhaltung eines Risikomanagementrahmens kann Unternehmen dabei helfen, ihre Vermögenswerte und ihr Geschäft besser zu schützen.

Was ist Enterprise Risk Management (ERM)?
ERM ist ein umfassender Ansatz zum Risikomanagement in einer großen Organisation. Ein ERM-Programm hilft Unternehmen dabei, ihre Risiken zu identifizieren und ihre Auswirkungen auf das Geschäft zu bewerten. Eine erfolgreiche ERM-Strategie kann dazu beitragen, betriebliche und finanzielle Risiken zu reduzieren und gleichzeitig Compliance und Sicherheit zu verbessern.

Warum ist Risikomanagement wichtig?
Risikomanagement ist wichtig, da der Prozess Unternehmen dabei hilft, sich auf potenzielle Bedrohungen für das Unternehmen vorzubereiten. Wenn Unternehmen über einen umfassenden Risikomanagementplan verfügen, sind sie besser in der Lage, Entscheidungen zu treffen, die ihre Daten und Systeme vor Angriffen schützen.

Welche Vorteile bietet das Risikomanagement?
Eine wirksame Risikomanagementstrategie kann folgende Vorteile ermöglichen:

- Reduziertes Risiko von Datenschutzverletzungen, Systemausfällen und anderen Sicherheitsvorfällen
- Erhöhte Sicherheit von Daten und Systemen
- Geschützter Ruf

Was ist Schwachstellenmanagement?
Beim Schwachstellenmanagement handelt es sich um den Prozess der proaktiven Identifizierung von Sicherheitsschwächen und Mängeln in IT-Systemen und Software, der Verfolgung der Schwachstellen und deren anschließender Priorisierung zur Behebung.

Was ist der Unterschied zwischen Risikomanagement und Schwachstellenmanagement?
Das Risikomanagement unterscheidet sich vom Schwachstellenmanagement. Das Risikomanagement hilft dabei, potenzielle Bedrohungen und Schwachstellen im gesamten Unternehmen zu identifizieren, zu bewerten und zu mindern, während das Schwachstellenmanagement auf Schwachstellen in Systemen, Prozessen oder Vermögenswerten abzielt, um die Wahrscheinlichkeit einer Ausnutzung zu minimieren.

Was ist risikobasiertes Schwachstellenmanagement?
Das risikobasierte Schwachstellenmanagement priorisiert die Behebung von Cybersicherheitsschwächen auf der Grundlage ihrer Ausnutzungswahrscheinlichkeit und ihrer Auswirkungen. Da nicht alle Schwachstellen behoben werden können, müssen Unternehmen die Schwachstellen mit dem höchsten Risiko priorisieren, um die Risikolage effizient zu verbessern.

Arten von Risiko Management Strategien

Auswahl einer Risikomanagementstrategie
Bei der Auswahl einer Risikomanagementstrategie müssen zunächst die Wahrscheinlichkeit von Risiken und ihre Auswirkungen beurteilt werden. Beispielsweise können von einem Angreifer ausgenutzte Schwachstellen zu System Kompromittierungen, Datendiebstahl und Dienstunterbrechungen führen. Organisationen können dann eine oder mehrere der vier Risikomanagementstrategien übernehmen: Vermeidung, Reduzierung, Übertragung oder Akzeptanz.

Risikovermeidung

Im Rahmen eines Risikovermeidungsansatzes implementieren Teams Richtlinien und Technologien, die zur Risikoeliminierung beitragen. Unter Risikovermeidung versteht man das Bemühen, Aktivitäten zu eliminieren oder besser zu steuern, die ein organisatorisches Risiko mit sich bringen.

Risikominderung
Das Ziel einer Risikominderungsstrategie besteht darin, die Wahrscheinlichkeit eines finanziellen oder betrieblichen Verlusts auf ein akzeptables Maß zu reduzieren.

Risikoübertragung
Bei der Risikoübertragung handelt es sich um die Abwälzung potenzieller Verluste auf einen beauftragten Dritten. Ein Beispiel für einen Risikotransfer ist der Abschluss einer Cyberversicherung.

Risikoakzeptanz
Nach der Vermeidung, Reduzierung oder Übertragung von Risiken können Organisationen ein gewisses Restrisiko akzeptieren, wenn dessen potenzielle Auswirkung gering oder unbedeutend ist. Wenn die richtigen Leitplanken vorhanden sind, kann es ein umsichtiger Weg sein, das Unternehmen mithilfe einer risikobasierten Priorisierung auf einem akzeptablen Risikoniveau zu steuern.

Risiko Management Prozess

Entwickeln Sie einen Plan
Das Ziel eines Cybersicherheits-Risikomanagementplans besteht darin, kritische Bedrohungen für Ihr Unternehmen zu identifizieren und abzuschwächen. Um das Risiko von Cyberangriffen effektiv zu reduzieren, planen Sie die Priorisierung der Schwachstellen, die die größte Bedrohung für Ihr Unternehmen darstellen. Befolgen Sie jeden Schritt im unten aufgeführten Risikomanagementprozess, um organisatorische Risiken proaktiv zu verwalten und zu reduzieren.

Identifizieren Sie Risiken
Der erste Schritt im Risikomanagementprozess ist die Durchführung einer Risikobewertung. Identifizieren Sie die Wahrscheinlichkeit potenzieller Schwachstellen und Angriffe und welche Vermögenswerte betroffen wären. Die Bestimmung der Wahrscheinlichkeit und Auswirkung potenzieller Angriffe kann dabei helfen, die Bemühungen zu priorisieren und sich auf die Risiken zu konzentrieren, die für das Unternehmen am relevantesten sind.

Identifizieren Sie Schwachstellen
Ein wichtiger Bestandteil des Risikomanagementprozesses ist die Identifizierung aller Schwachstellen in Ihrer IT-Umgebung. Schwachstellen sind Sicherheitslücken und Mängel in Systemen und Software, die Angreifer ausnutzen könnten. Teams verwenden Tools zum Scannen und Verwalten von Schwachstellen, um Sicherheitslücken aufzudecken und diese zu beheben.

Reduzieren Sie Risiken und Schwachstellen
Setzen Sie Sicherheitstools ein, um Ihre Schwachstellen zu beheben und Risiken effektiv zu reduzieren. Ein risikobasierter Ansatz hilft Teams dabei, herauszufinden, welche Schwachstellen zuerst behoben werden sollten. Eine Vielzahl von Lösungen erleichtert den Umgang mit kritischen Risiken, wie z. B. risikobasierte Schwachstellenmanagement-Tools, Intrusion-Detection-Systeme, Firewalls und Schulungen zum Sicherheitsbewusstsein.

Kontinuierlich überwachen
Überwachen Sie wichtige Leistungsindikatoren und wichtige Risikoindikatoren im gesamten Netzwerk, um den Erfolg von Risikominderungsmaßnahmen sicherzustellen und potenzielle Bedrohungen proaktiv anzugehen.

Bereiten Sie sich auf die Reaktion auf Vorfälle (IR) vor
Bevor eine Schwachstelle zu einem dringenden Sicherheitsereignis wird, bereiten Sie einen Plan zur Reaktion auf Vorfälle vor, den das IR-Team befolgen kann. Das Ziel eines IR-Plans besteht darin, Bedrohungen zu erkennen, ihre Auswirkungen zu minimieren und das erneute Auftreten von Vorfällen zu verhindern.

Planen Sie die Wiederherstellung
Entwickeln Sie einen Disaster-Recovery-Plan (DRP), um IT-Teams bei der Wiederherstellung des Betriebs zu unterstützen, falls ein Sicherheitsvorfall einen Tag oder länger andauert.

Arten von Risiko Management Lösungen - Wie kann Cisco Sie dabei beraten?

Beratung zum Sicherheitsrisikomanagement
Beratungsdienste für das Sicherheitsrisikomanagement nutzen menschliche und digitale Intelligenz, um Unternehmen dabei zu helfen, Risiken in ihrer Umgebung zu erkennen und datengestützte Entscheidungen zur Erreichung ihrer Geschäftsziele zu treffen. Entdecken Sie unsere Beratungsdienste

Sicherheitsrisikobewertungen
Sicherheitsrisikobewertungen sind eine Schlüsselkomponente, um die Risiken eines Unternehmens zu verstehen und die Widerstandsfähigkeit des Unternehmens zu stärken. Regelmäßige Tests können dabei helfen, Schwachstellen in der Sicherheitsinfrastruktur, den Abwehrmaßnahmen und den Reaktionen zu erkennen. Nutzen Sie unsere Bewertungsdienste – Assessment Services (PDF)

Lösungen für das Bedrohungsmanagement
Bedrohungsmanagement-Tools helfen, Risiken zu reduzieren, indem sie Bedrohungen erkennen, analysieren und Gegenmaßnahmen ergreifen. Beispiele für Bedrohungsmanagementlösungen sind:

- Endpunkt Erkennung und Reaktion (EDR)
- Netzwerk Erkennung und Reaktion (NDR)
- Managed Detection and Response (MDR)
- Erweiterte Erkennung und Reaktion (XDR)
- Incident-Response-Dienste (IR)

Vereinheitlichen Sie Ihre Tools für Bedrohungsmanagement

Lösungen für das Schwachstellenmanagement
Eine risikobasierte Schwachstellenmanagementlösung bietet Unternehmen die Möglichkeit, das relative Risiko zu ermitteln, das Software- und Geräteschwachstellen oder -schwächen für ihre Umgebung darstellen. Diese Erkenntnisse helfen Unternehmen dabei, die Schwachstellen zu beheben, die am wichtigsten sind. Ein wirksames Programm trägt dazu bei, das Risikoprofil einer Organisation zu senken. Gehen Sie risikobasiert vor – Vulnerability Management

Überwachungstools
Die kontinuierliche und proaktive Überwachung des Netzwerkverkehrs trägt dazu bei, organisatorische Risiken zu mindern. Stellen Sie Überwachungstools bereit, die einen vollständigen Überblick über die IT-Umgebung des Unternehmens ermöglichen, um Teams in die Lage zu versetzen, Bedrohungen und Anomalien in Echtzeit zu erkennen. Verbessern Sie Ihre Visibilität – Full Stack Observability

Incident-Response-Plan (IRP)
Ein Vorfallreaktionsplan legt ein Verfahren für das Sicherheitspersonal fest, um Bedrohungen zu erkennen und abzuschwächen und Maßnahmen zu ergreifen, die dazu beitragen, das erneute Auftreten von Bedrohungen zu verhindern. Da es unmöglich ist, jede Bedrohung zu verhindern, ist es wichtig, Schritte, Richtlinien und Verantwortlichkeiten für den Fall eines Sicherheitsvorfalls festzulegen. Erfahren Sie mehr über Incident Response Plans

Cisco Risk Management Solutions – Software Lösungen für Ihr Risiko Management

Risikobasiertes Schwachstellenmanagement
Cisco Vulnerability Management ermöglicht es Unternehmen, Schwachstellen proaktiv zu beheben, Exploits zu verhindern und Risiken in möglichst wenigen Schritten zu reduzieren – mit optimierten Arbeitsabläufen, umfassenden Bedrohungsinformationen und erweiterter Risikopriorisierung. Priorisieren Sie Ihr Risiko mit Cisco Vulnerability Management (vormals Kenna.VM)

Risikobasierte Endpunktsicherheit

Cisco Secure Endpoint erhöht die Sicherheit an Ihren Endpunkten durch scannerlose Transparenz, risikobasierten Schwachstellenkontext und umsetzbare Risikobewertungen, die Teams dabei helfen, die richtigen Schwachstellen für die Behebung zu priorisieren. Entdecken Sie Endpunktsicherheit mit Cisco Secure Endpoint

Erweiterte Erkennung und Reaktion (XDR)
Cisco XDR nutzt künstliche Intelligenz (KI) und Talos-Bedrohungsinformationen aus der realen Welt, um Bedrohungen nach dem größten Risiko zu priorisieren und schneller auf das Wesentliche zu reagieren. Entdecken Sie die Cisco XDR Funktionen

Umfangreiche Bedrohungsinformationen
Cisco Talos stattet Risikomanagementteams mit Zero-Day-Schwachstelleninformationen aus, um Sicherheitslücken mit hoher Priorität zu identifizieren und eine datengestützte Entscheidungsfindung zu ermöglichen. Erfahren Sie mehr über Cisco Talos

6.3.2 Verweis auf den „Stand der Technik“ und internationale Normen (Zertifizierung)

ISO/IEC 27000 Normenreihe zu Informationssicherheits-Managementsystemen (ISMS)

Nachfolgend finden Sie eine Auflistung sicherheitsrelevanter Normen der ISO/IEC 27000-Reihe:

ISO/ IEC 27000 – Überblick und Vokabular
Die ISO/ IEC 27000 ermöglicht eine schnelle Einführung in die umfangreiche ISO/ IEC 27000 Normenreihe.

ISO/ IEC 27001 – Anforderungen an Informationssicherheits-Managementsysteme (ISMS)
„Die ISO/IEC 27001 spezifiziert in den Kapiteln 4 bis 10 die Anforderungen an das Festlegen, Umsetzen, Betreiben, Überwachen, Überprüfen, Instandhalten und Verbessern eines dokumentierten Informationssicherheits-Managementsystems (ISMS) im Kontext zu den allgemeinen Geschäftsrisiken einer Organisation. Dazu zählen insbesondere folgende Punkte:

- **Managementverantwortung**
  Management Verantwortung, Informationssicherheits-Politik sowie organisatorische Rollen, Zuständigkeiten und Verantwortungen
- **Planung**
  Risikomanagement Kriterien
- **Unterstützung**
  Ressourcenverfügbarkeit, Qualifikationen, Awareness, Kommunikation und Dokumentation
- **Betrieb**
  Risikomanagement Prozesse
- **Überprüfung**
  Prüfungsmaßnahmen, Audits und Management-Review
- **Verbesserung**
  Abweichungen und Verbesserungsmaßnahmen sowie kontinuierliche Verbesserung

ISO/IEC 27001 – Annex A
Die ISO/IEC 27001 legt im Annex A (entspricht ISO/IEC 27002) darüber hinaus die Anforderungen für die Umsetzung der organisatorischen und technischen Sicherheitsmaßnahmen fest. Die festgelegten Anforderungen unterteilen sich in 14 Abschnitte (Sections), 35 Maßnahmenziele (Control Objectives) und 114 Maßnahmen (Controls).
Risikomanagement-Ansatz
Kernelement der ISO/IEC 27001 ist der Risikomanagement-Ansatz. Hierbei werden mittels Risikoanalyse die spezifischen Informationssicherheitsrisiken einer Organisation erhoben und bewertet. Ausgehend von den Analyseergebnissen wird das ISMS mit zielgerichteten Maßnahmen umgesetzt und direkt an den individuellen Anforderungen der Organisation ausgerichtet.“
(A-SIT, 2017) Mehr dazu lesen Sie hier:
https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Normen-und-Standards/ISO-IEC-27000/ISO-IEC-27001-Informationssicherheits-Managementsysteme-ISMS.html

ISO/ IEC 27002 – Leitfaden für das Management der Informationssicherheit

Die ISO/ IEC 27002 legt Richtlinien und allgemeine Grundsätze für die Einführung, Umsetzung, Aufrechterhaltung und Verbesserung des Informationssicherheits-Managements innerhalb einer Organisation fest.

ISO/ IEC 27003 – Leitfaden für die ISMS-Implementierung
Die ISO/ IEC 27003 dient als Leitfaden für die Implementierung eines ISMS gemäß den Anforderungen der ISO/ IEC 27001.

ISO/ IEC 27004 – Leitfaden für Informationssicherheits-Managementmessmethoden
Die ISO/ IEC 27004 stellt eine Anleitung für die Entwicklung und die Anwendung von Messmethoden in Bezug auf die Effektivität der Prozesse und Maßnahmen eines implementierten ISMS zur Verfügung.

ISO/ IEC 27005 – Leitfaden für das Informationssicherheits-Risikomanagement
Die ISO/ IEC 27005 dient als Leitfaden für das Informationssicherheits-Risikomanagement.

ISO/ IEC 27007 – Leitfaden für ISMS-Audits
Die ISO/ IEC 27007 dient als Leitfaden für die Anwendung eines ISMS-Auditprogramms.

ISO/ IEC 27010 -Inter-Sector Communication
Die ISO/ IEC 27010 dient als Leitfaden für das Informationssicherheits-Management für inter-sektorielle und inter-organisationaler Kommunikation.

ISO/ IEC 27011 – Leitfaden für das Informationssicherheits-Management im Telekom-Sektor
Die ISO/ IEC 27011 dient als Leitfaden für das Informationssicherheits-Management für Telekommunikationsunternehmen. Die Norm ist auch bekannt als ITU X.1051.

ISO/ IEC 27013 – Integrated Implementation of ISO/IEC 27001 and 20000-1
Die ISO/ IEC 27013 dient als Leitfaden für die integrierte Implementierung eines Informationssicherheits-Managementsystems (ISMS) nach ISO/IEC 27001 und eines IT-Servicemanagements (ITSM) nach ISO/IEC 20000-1.

ISO/ IEC 27014 -Governance of information security
Die ISO/ IEC 27014 beschreibt ein Governance-Rahmenwerk für Informationssicherheit.

ISO/IEC 27018 – Leitfaden für Datenschutz in Cloud-Diensten
Die ISO/IEC 27018 beschreibt Umsetzungsempfehlungen für die sichere Verarbeitung von personenbezogenen Daten durch Cloud-Dienste.

ISO/ IEC 27031 -Business Continuity Leitfaden
Die ISO/ IEC 27031 dient als Leitfaden für das Business Continuity Management.

ISO/ IEC 27032 -Cyber Security Leitfaden
Die ISO/ IEC 27032 behandelt die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen im Cyberspace.

ISO/ IEC 27033 -Network Security
Die ISO/ IEC 27033 Normenreihe enthält sechs Subnormen zum Thema Netzwerk-Sicherheit.

ISO/IEC 27034 – Application Security
Die ISO/IEC 27034 Normenreihe enthält sieben Subnormen zum Thema Applikations-Sicherheit.

ISO/IEC 27035 -Information security incident management
Die ISO/IEC 27035 dient als Leitfaden für die Umsetzung eines Managementsystems zur Erkennung und Behandlung von Sicherheitsvorfällen und Sicherheitsschwachstellen für große und mittlere Organisationen.

ISO/ IEC 27036 -Information Security for Supplier Relationships

Die ISO/ IEC 27036 enthält vier Subnormen zum Thema Sicherheitsaspekte beim Outsourcing und Cloud Computing.

ISO/ IEC 27037 -Digital Forensic Leitfaden
Die ISO/ IEC 27037 dient als Leitfaden für die Identifizierung, Sammlung, Sicherung und Erhaltung von digitalen Beweisinformationen in der IT-Forensik.

ISO/IEC 27799 - Informationssicherheits-Management im Gesundheitssektor
Die ISO/IEC 27799 spezifiziert die Anforderungen an ein Informationssicherheits-Managementsystem (ISMS) im Gesundheitswesen.

ISO/IEC TS 27008 - Leitfaden für die Überprüfung von Sicherheitsmaßnahmen
Die ISO/IEC TS 27008 dient als Leitfaden für die Überprüfung der Implementierung und des Betriebs von Sicherheitsmaßnahmen, einschließlich technischer Compliance-Tests.

Mehr dazu finden Sie hier:
https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Normen-und-Standards/ISO-IEC-27000.html

ISA/IEC-62443-3-3: Industrielle Sicherheit - Was ist das und wie kann man sie einhalten?

Der Schutz industrieller Automatisierungs- und Steuerungssysteme (IACS) vor Cyberbedrohungen hat für Industrieunternehmen oberste Priorität. Aber gute Absichten in Taten umzusetzen, kann eine gewaltige Aufgabe sein. Da IACS und die zugrunde liegenden Netzwerke oft sehr komplex sind und über veraltete Technologien und schlechte Sicherheitsverfahren verfügen, könnte man sich fragen, wo man anfangen soll.

Glücklicherweise hat die International Society of Automation (ISA) die ISA99-Reihe von Standards und technischen Berichten zusammengestellt. Die Internationale Elektrotechnische Kommission (IEC) arbeitete mit der ISA zusammen, um die meisten davon als IEC-Dokumente zu veröffentlichen und entwickelte zusätzliche Teile, die der gemeinsamen Reihe von ISA/IEC-62443 hinzugefügt werden.

Die Standards und technischen Berichte der ISA/IEC-62443-Serie sind in vier Gruppen unterteilt, die unterschiedlichen Schwerpunkten und Zielgruppen entsprechen. Teil 3-3 definiert Systemsicherheitsanforderungen und Sicherheitsfähigkeitsstufen, um ein IACS zu erstellen, das die angestrebte Sicherheitsstufe erfüllt, und um Ihre Praxis für jede Anforderung zu bewerten. Es bietet IT- und Betriebsteams eine gemeinsame Basis für die Zusammenarbeit beim Aufbau industrieller Infrastrukturen, die sowohl vor Cyberbedrohungen als auch vor gelegentlichen oder zufälligen Ereignissen wirksam geschützt sind und eine kontinuierliche Verbesserung vorantreiben.

Cisco ist vor allem für Unternehmensnetzwerke und Cybersicherheit bekannt. Weniger Menschen wissen, dass wir seit mehr als 15 Jahren auch Industrieunternehmen auf der ganzen Welt dabei unterstützen, ihre Abläufe zu digitalisieren. Wir haben mit Herstellern, Energie- und Wasserversorgern, Bergwerken, Häfen, Eisenbahnen, Straßen und mehr zusammengearbeitet. Tatsächlich ist Cisco in allen Segmenten des Marktes für industrielle Netzwerke führend.

Mit unserem umfassenden Verständnis der Anforderungen der Operational Technology (OT) und unserem führenden Cybersicherheitsportfolio ist Cisco ein idealer Partner, der Industrieunternehmen bei der Sicherung ihres IACS unterstützt, um die Einhaltung des ISA/IEC-62443-3-3-Standards zu erreichen. Dieses Dokument erläutert die im Standard aufgeführten Anforderungen und zeigt, wie Cisco helfen kann.

Die Sicherheitsprinzipien von ISA/IEC 62443-3-3
Teil 3-3 des Standards definiert wesentliche Sicherheitsanforderungen (Systemanforderungen – SR und Anforderungserweiterungen – RE), die aus den Grundanforderungen (FR) abgeleitet werden, um die in Teil 1-1 definierten Cybersicherheitsprinzipien einzuhalten, einschließlich:

Geringstes Privileg (Least privilege)

Durch dieses Prinzip erhalten Nutzer nur die Rechte, die sie für ihre Arbeit benötigen, um unerwünschte Zugriffe auf Daten oder Programme zu verhindern und einen Angriff im Falle einer Konto Kompromittierung zu blockieren oder zu verlangsamen.

Verteidigung in der Tiefe (Defense in depth)
Diese Technik ermöglicht mehrschichtige Verteidigungstechniken, um einen Cyberangriff auf das Industrienetzwerk zu verzögern oder zu verhindern. Der Standard verlangt außerdem, dass Systeme in Gruppen, sogenannte „Zonen“, unterteilt werden, die über Kommunikationskanäle, sogenannte „Leitungen“, miteinander kommunizieren können, unabhängig davon, ob diese physisch, elektronisch oder prozessbasiert sind.

Risikoanalyse (Risk analysis)
Das Konzept der Risikoanalyse, die auf Kritikalität, Wahrscheinlichkeit und Auswirkung basiert, ist nicht neu. Es wird bereits eingesetzt, um Risiken im Zusammenhang mit der Produktionsinfrastruktur, der Produktionskapazität (Produktionsausfall), den Auswirkungen auf Menschen (Verletzungen, Todesfälle) und der Umwelt (Verschmutzung) zu begegnen. Diese Technik muss jedoch auf die Cybersicherheit ausgeweitet werden, um den mit industriellen Informationssystemen verbundenen Risiken zu begegnen. ISA/IEC-62443-3-2 beschreibt eine Methodik zur Bewertung des Sicherheitsrisikos für ein IACS.

Kompensierende Sicherheitsmaßnahmen (Compensating security measures)
In vielen Fällen bieten die Komponenten eines IACS nicht die erforderlichen Funktionen, um eine bestimmte Sicherheitsstufe zu erfüllen. In solchen Szenarien kann der Einsatz kompensierender technischer oder verfahrenstechnischer Sicherheitsmaßnahmen dazu beitragen, die erforderliche Fähigkeit zu ermöglichen. Die Kombination mehrerer Techniken in einer Sicherheitslösung ist darauf ausgelegt, diese Rolle zu erfüllen.

Zonen und Leitungen (Zones and conduits)
Basierend auf diesen Prinzipien schlägt ISA/IEC-62443 eine industrielle Steuerungssystemarchitektur vor, die das in ISA95 verwendete Purdue-Referenzmodell nutzt (Abbildung 1) und diese Funktionsebenen in Zonen und Leitungen segmentiert (Abbildung 2). Die Segmentierung ist ein Ergebnis der Sicherheitsrisikobewertung gemäß ISA/IEC-62443-3-2.

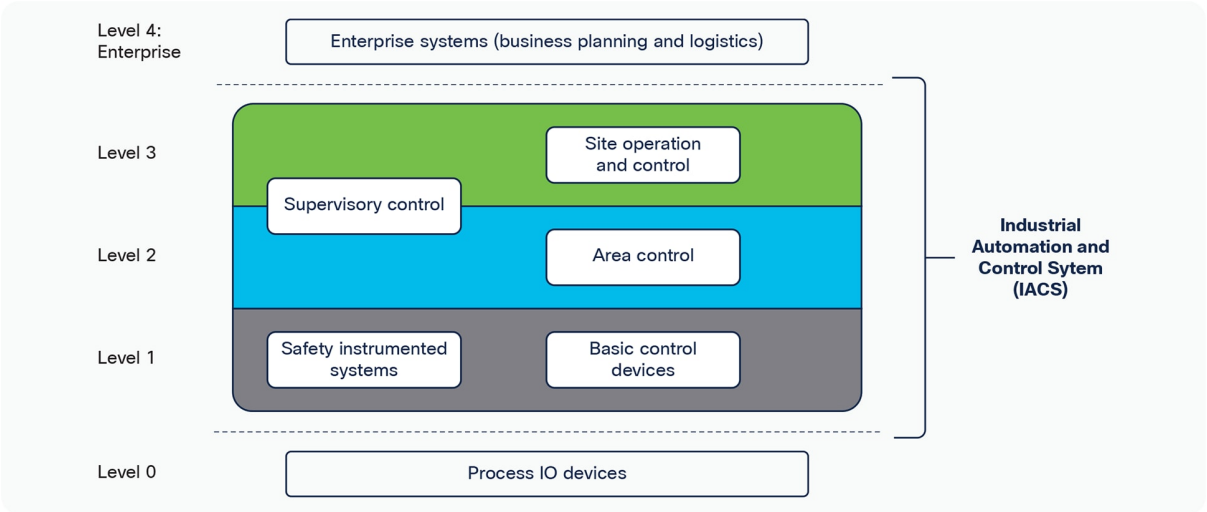

Abbildung 7 ISA/IEC 62443 funktionales Referenzmodell (Quelle: IEC-62443-3-3 Standard)

Gemäß dem Standard ist eine Zone eine Ansammlung von physisch und/oder funktionell verbundenen Vermögenswerten, die gemeinsame Sicherheitsanforderungen haben. Diese Zonen werden auf der Grundlage der physikalischen und funktionalen Modelle der industriellen Systemsteuerungsarchitektur definiert. Alle Vermögenswerte in einem IACS müssen in einer Zone positioniert sein.

Leitungen (engl. Conduits) unterstützen die Kommunikation zwischen Zonen. Ein Conduit ist eine logische Gruppierung von Kommunikationskanälen zwischen zwei oder mehr Zonen.

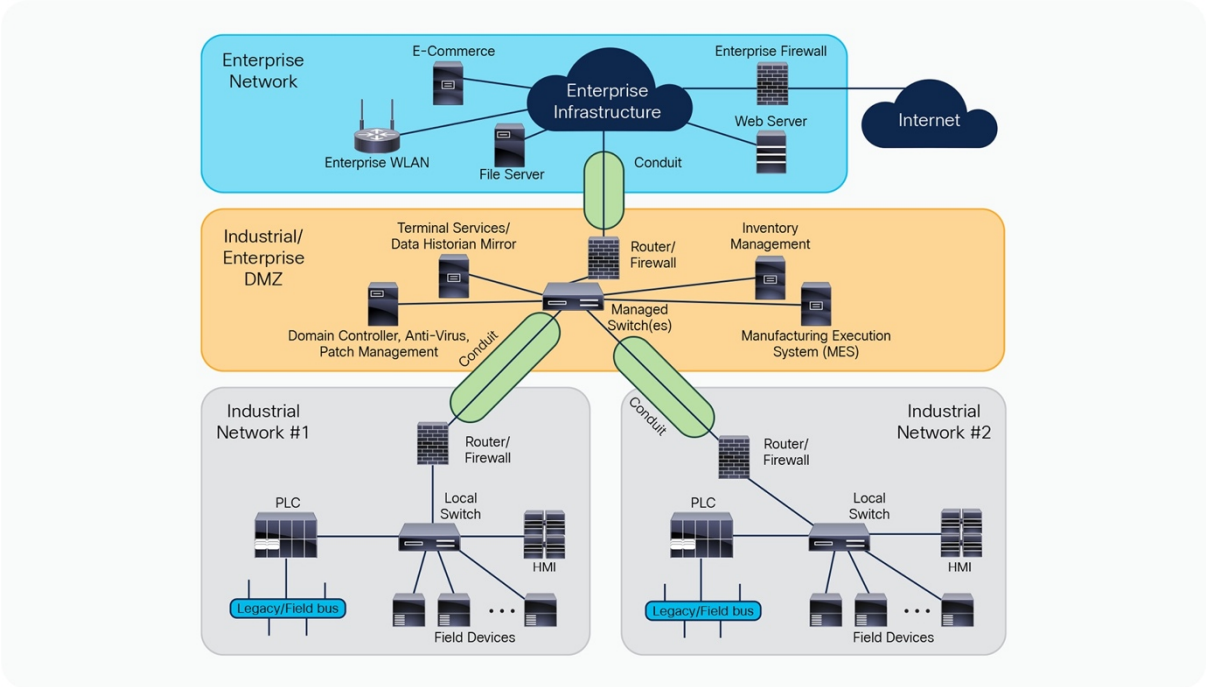

Abbildung 8 Beispiel für industrielle Netzwerkzonen und Leitungen (Quelle: IEC 62443-3-3 Standard)

Nutzung sicherer Komponenten
ISA/IEC-62443-3-3 konzentriert sich auf das Prinzip eines sicheren IACS, nutzt jedoch andere Teile der Standardreihe. Beispielsweise wird davon ausgegangen, dass ein Sicherheitsprogramm eingerichtet wurde und gemäß IEC 62443-2-1 betrieben wird: Anforderungen an Sicherheitsprogramme für IACS-Anlagenbesitzer.
ISA/IEC-62443-3-3 geht außerdem davon aus, dass sichere Komponenten eingesetzt oder zusätzliche Maßnahmen ergriffen werden, um die Anforderungen zu erfüllen und die aktuelle und zukünftige Schwachstellen- und Bedrohungslandschaft zu bewältigen. In den Teilen 4-2 und 4-1 werden Komponenten- und Entwicklungsanforderungen definiert, die für die Erreichung der Konformität unerlässlich sind.

ISA/IEC-62443-4-1: Anforderungen an den sicheren Produktentwicklungslebenszyklus
Dieser Teil der ISA/IEC-62443-Reihe umfasst Prozessanforderungen für die sichere Entwicklung von Produkten, die zum Aufbau eines IACS verwendet werden, sowie Reifegrade, um Maßstäbe für die Compliance festzulegen. Der Inhalt bezieht sich auf die folgenden Prozesse: Anforderung, Management, Design, Verwendung von Codierungsrichtlinien, Implementierung, Verifizierung und Validierung, Fehlermanagement, Patch-Management und Produktlebensende. Diese Anforderungen sind für die Sicherheitsfunktionen einer Komponente und den zugrunde liegenden Secure-by-Design-Ansatz der IACS-Lösung von wesentlicher Bedeutung. Der Gesamtschwerpunkt von Teil 4-1 liegt auf der kontinuierlichen Verbesserung, die für die Geschwindigkeit bei der Produktentwicklung und -veröffentlichung unerlässlich ist.
Software- und Hardwareprodukte von Cisco werden gemäß dem Cisco Secure Development Lifecycle (Cisco SDL) entwickelt, der von der Produktplanung bis zum Ende der Lebensdauer eine Secure-by-Design-Philosophie durchsetzt. Cisco hat die IEC-62443-4-1-Zertifizierung für Cisco SDL erhalten, die für die Entwicklung aller Industrieprodukte von Cisco gilt.

ISA/IEC 62443-4-2: Technische Sicherheitsanforderungen für IACS-Komponenten
Dieser Teil enthält Anforderungen an technische Steuerungssystemkomponenten im Zusammenhang mit den sieben Grundanforderungen (FRs). Es erweitert die in ISA/IEC-62443-3-3 definierten Systemanforderungen (SRs) und Anforderungserweiterungen (REs) zu einer Reihe von Komponentenanforderungen (Component Requirements CRs) und zugehörigen REs für die in einem IACS

enthaltenen Komponenten. Ziel ist es, die Auswahl und Beschaffung von Steuerungssystemkomponenten zum Aufbau und zur Integration einer IACS-Lösung zu unterstützen.

In diesem Zusammenhang spezifiziert der Standard, Sicherheitsfunktionen die die Integration einer Komponente in die Systemumgebung eines IACS auf einem bestimmten Sicherheitsniveau (SL) ermöglichen. Teil 4-2 enthält Anforderungen für vier Arten von Komponenten: Softwareanwendung, eingebettetes Gerät, Hostgerät und Netzwerkgerät, zugeschnitten auf die Besonderheiten dieser Assets. Im Wesentlichen muss eine sichere IACS-Lösung auf der Grundlage sicherer Komponenten und bei Bedarf durch die Anwendung kompensierender Sicherheitsmaßnahmen aufgebaut werden.

Mehrere Cisco-Produkte haben bereits die IEC-62443-4-2-Zertifizierung erhalten. In Kombination mit einem 62443-zertifizierten Entwicklungsprozess (Cisco SDL) bietet Cisco vertrauenswürdige Kommunikationsprodukte, die für den IACS-Einsatz in kritischen Infrastrukturen unerlässlich sind.

Grundlegende Anforderungen von ISA/IEC-62443-3-3
In diesem Kapitel werden die Systemanforderungen (System Requirements SRs) beschrieben, die in IEC-62443-3-3 für jede Grundanforderung (Foundational Requirements FRs) definiert sind, und wie Cisco dabei helfen kann, die Einhaltung zu erreichen. Die FRs selbst sind in ISA/IEC 62443-1-1 (Terminologie, Konzepte, Modelle) definiert.

Gemäß dem Geltungsbereich der Norm beziehen sich diese Anforderungen auf alle Komponenten, die zum Aufbau und Betrieb eines IACS verwendet werden. Cisco kann ein Industrieunternehmen dabei unterstützen, die Anforderungen und das gewünschte Sicherheitsniveau für Netzwerk- und Sicherheitskomponenten zu erfüllen.

Der Standard definiert fünf verschiedene Sicherheitsstufen (Security Levels SLs), die Unternehmen je nach Risikoanalyse für jede FR erreichen können:

- Stufe 0: Keine besonderen Anforderungen oder Sicherheitsmaßnahmen erforderlich.
- Stufe 1: Schutz vor zufälligen oder zufälligen Ereignissen.
- Stufe 2: Schutz vor absichtlichen Ereignissen durch böswillige Benutzer mit einfachen Mitteln, geringen Ressourcen, allgemeinen Fähigkeiten und geringer Motivation.
- Stufe 3: Schutz vor vorsätzlichen Ereignissen durch böswillige Benutzer mit ausgefeilten Mitteln, moderaten Ressourcen, spezifischen Fähigkeiten und moderater Motivation.
- Stufe 4: Schutz vor vorsätzlichen Ereignissen böswilliger Benutzer durch ausgefeilte Mittel, umfangreiche Ressourcen, spezifische Fähigkeiten und hohe Motivation.

Diese Sicherheitsstufen ermöglichen es einer Organisation, den erforderlichen Schutz auf der Grundlage von Sicherheitskontrollen für immer komplexere Arten von Bedrohungen zu definieren.

FR1: Identifikation, Authentifizierungskontrolle und Zugangskontrolle (Access Control AC)
Dieser Teil der Norm beschreibt Anforderungen zur Identifizierung und Authentifizierung von Benutzern (Menschen, Softwareprozesse und Geräte), bevor ihnen Zugriff auf das industrielle Steuerungssystem oder eine bestimmte Komponente gewährt wird. Es wird anerkannt, dass einige Komponenten möglicherweise stärkere Authentifizierungsmechanismen erfordern als andere, und es wird empfohlen, die Kontrollen innerhalb einer einzelnen Zone zu minimieren.

Wie kann Cisco helfen?
Die Cisco Identity Services Engine (ISE) arbeitet mit Netzwerkgeräten (sowohl kabelgebunden als auch drahtlos) zusammen, um eine umfassende kontextbezogene Identität mit Attributen wie Benutzer, Zeit, Standort, Bedrohung, Schwachstelle und Zugriffstyp zu erstellen. Diese Identität, ob menschlich oder nicht, kann verwendet werden, um eine hochsichere Zugriffsrichtlinie durchzusetzen, die der Geschäftsrolle der Identität entspricht. Administratoren können präzise steuern, wer, was, wann, wo und wie Endpunkte im Netzwerk zugelassen werden. ISE lässt sich in mehrere externe Identitätsanbieter wie Microsoft Active Directory integrieren.

Cisco ISE bietet außerdem eine einfach bereitzustellende interne Zertifizierungsstelle. ISE unterstützt sowohl eigenständige Bereitstellungen als auch solche, bei denen die Zertifizierungsstelle in die bestehende öffentliche Schlüsselinfrastruktur Ihres Unternehmens integriert ist, und erleichtert die manuelle Erstellung von Massen- oder Einzelzertifikaten und Schlüsselpaaren, um Geräte mit einem hohen Maß an Sicherheit mit dem Netzwerk zu verbinden.
Für menschliche Benutzer, die auf Windows-Workstations im Fertigungsbereich zugreifen oder aus der Ferne auf das Netzwerk zugreifen, bietet Cisco Secure Access by Duo die Multifaktor-Authentifizierung (MFA), um die Benutzeridentität zu überprüfen, bevor Zugriff gewährt wird. Durch die Installation der Duo-Authentifizierung für Windows-Anmeldungen wird MFA zu allen interaktiven Windows-Anmeldeversuchen von Benutzern hinzugefügt, sei es an einer lokalen Konsole oder über Remote Desktop Protocol (RDP), es sei denn, Sie wählen im Installationsprogramm die Option „Nur zur Duo-Authentifizierung auffordern, wenn Sie sich über RDP anmelden“. .
Cisco Cyber Vision bietet in erster Linie Asset-Inventarisierung und Einblick in Flussdaten. Es kann auch das Vorhandensein von Anmeldeinformationen erkennen, die mithilfe von Klartextprotokollen gesendet werden, sodass Administratoren die Möglichkeit haben, Abhilfe zu schaffen, bevor es zu einem Man-in-the-Middle-Angriff kommt.

FR2: Kontrolle des Zugriffs der Benutzung (Use Control UC)
Bei dieser grundlegenden Anforderung geht es darum, die richtigen Berechtigungen für einen Benutzer (Mensch, Softwareprozess oder Gerät) nach der Identifizierung und Authentifizierung durchzusetzen, um eine Komponente vor unbefugten Aktionen (Lesen/Schreiben von Daten, Herunterladen von Programmen, Festlegen von Konfigurationen usw.) zu schützen. Es kümmert sich auch um die Überwachung von Benutzeraktionen und empfiehlt die Anpassung von Benutzerrechten basierend auf Tageszeit, Datum, Ort und Art und Weise, mit der der Zugriff erfolgt.

Wie kann Cisco helfen?
Die Cisco Identity Services Engine (ISE) ist ein AAA-Server (Authentifizierung, Autorisierung und Accounting), der für die Zugriffskontrolle in kabelgebundenen und kabellosen Industrienetzwerken verwendet wird. Die Authentifizierung bietet eine Möglichkeit, einen Benutzer zu identifizieren, typischerweise indem der Benutzer einen gültigen Benutzernamen und ein gültiges Kennwort eingibt, bevor der Zugriff gewährt wird. Allerdings sind die meisten Geräte im Netzwerk keine Menschen und verfügen daher nicht über die Möglichkeit, einen Benutzernamen oder ein Passwort bereitzustellen.
ISE bietet die Möglichkeit, MAC Authentication Bypass (MAB) durchzuführen, bei dem die MAC-Adresse eines Geräts verwendet wird, um die Ebene des bereitzustellenden Netzwerkzugriffs zu bestimmen. Vor der MAB-Authentifizierung ist die Identität des Endpunkts unbekannt und der gesamte Datenverkehr wird blockiert. Der Switch untersucht ein einzelnes Paket, um die Quell-MAC-Adresse zu erfahren und zu authentifizieren. Nachdem MAB erfolgreich war, ist die Identität des Endpunkts bekannt und der Datenverkehr von diesem Endpunkt ist zulässig. Der Switch führt eine Quell-MAC-Adressfilterung durch, um sicherzustellen, dass nur der MAB-authentifizierte Endpunkt Datenverkehr senden darf.
Bei der Autorisierung handelt es sich um den Prozess der Durchsetzung von Richtlinien und der Bestimmung, auf welche Art von Aktivitäten, Ressourcen oder Diensten ein Benutzer oder ein Gerät zugreifen darf. Cisco ISE wird von einem zentralen Standort aus gesteuert und verteilt die Durchsetzung auf die gesamte Netzwerkinfrastruktur. Administratoren können zentral eine Richtlinie definieren, die Anbieter von registrierten Benutzern unterscheidet und den Zugriff auf der Grundlage der geringsten Rechte gewährt. ISE bietet eine Reihe von Zugriffskontrolloptionen, wie herunterladbare Zugriffskontrolllisten (dACLs), VLAN-Zuweisungen und Security Group Tags (SGT) oder Cisco TrustSec. Diese Technologien werden in FR5 näher erläutert, wo die Netzwerksegmentierung behandelt wird. Cisco Secure Firewall bietet detailliertere Richtlinien über Netzwerkgrenzen hinweg für Funktionen wie die Durchsetzung von Lese-/Schreibzugriffen.
Das Accounting überwacht die Ressourcen, die ein Benutzer während des Zugriffs macht. Dazu kann die Systemzeit oder die Datenmenge gehören, die ein Benutzer während einer Sitzung gesendet oder empfangen hat. Das Accounting macht die Protokollierung von Sitzungsstatistiken und Nutzungsinformationen, die zur Berechtigungskontrolle, Ressourcennutzung und Kapazitätsplanung verwendet werden.

Audit-Protokolle werden durch Cisco Cyber Vision ergänzt, da alle Pakete, die durch die Netzwerkinfrastruktur fließen, einer umfassenden Paketprüfung unterzogen werden und bei der Überprüfung von Ereignissen im Netzwerk OT-spezifische Daten bereitgestellt werden.

FR3: Systemintegrität (SI)
Das Ziel dieser grundlegenden Anforderung besteht darin, die Integrität jeder Komponente des IACS sicherzustellen, indem unbefugte Manipulationen während des gesamten Lebenszyklus der Komponente, d. h. während der Test-, Betriebs- und Nichtbetriebsphase, verhindert werden. Auch die Integrität der Datenübertragung ist eine zentrale Voraussetzung, um beispielsweise Manipulationen an Messwerten oder Befehlsparametern zu verhindern.

Wie kann Cisco helfen?
Zusätzlich zu den Sicherheitskontrollen ist gehärtete und robuste Ausrüstung erforderlich, um bestimmte physische und umweltbedingte Auswirkungen zu bewältigen und Auswirkungen durch elektromagnetische Interferenzen (EMI) und andere raue Bedingungen auszuschließen. Dazu gehören Verkabelung, Schnittstellen und die Gestaltung der Kommunikationsgeräte. Ein perfektes Beispiel hierfür ist die Norm IEC-61850-3 für Geräte, die in Umspannwerken installiert sind. Die robusten Industrie-Switches von Cisco, die in Netzwerken zur Umspannwerkautomatisierung eingesetzt werden, sind alle nach Teil 3 von IEC-61850 zertifiziert.
Darüber hinaus ist eine robuste, zuverlässige und in einigen Fällen redundante Netzwerkarchitektur von entscheidender Bedeutung, um eine hohe Datenverfügbarkeit sicherzustellen und Auswirkungen durch Umgebungsbedingungen zu minimieren.
Um Einblicke in die Integrität der Datenübertragung zu erhalten, empfiehlt Cisco die Verwendung von Endpunktsoftware und einem Intrusion Detection System (IDS), um die Auswirkungen von Schadcode oder nicht autorisierter Software zu verhindern, zu erkennen, zu melden und abzuschwächen. Cisco Snort ist ein Open-Source-IPS/IDS, das sowohl in Cisco Secure Firewall als auch Cyber Vision integriert ist. Cisco Secure Endpoint ist ein Endpoint-Schutztool, das Malware auf Workstations, Windows-basierten Mensch-Maschine-Schnittstellen (HMIs) und Tablets, die in industriellen Netzwerken verwendet werden, erkennen und verhindern kann.

FR4: Datenvertraulichkeit (DC)
Das Ziel dieser grundlegenden Anforderung besteht darin, Daten vor unbefugter Offenlegung zu schützen, sei es bei der Übermittlung oder bei der Speicherung. Dies bedeutet nicht nur den Schutz von Kommunikationskanälen und Speicher, sondern erfordert auch, dass Organisationen definieren, welche Daten geschützt werden müssen und wer Zugriff darauf haben soll.

Wie kann Cisco helfen?
MACsec ist der IEEE 802.1AE-Standard zur Authentifizierung und Verschlüsselung von Paketen zwischen zwei MACsec-fähigen Geräten. Die Switches der Cisco Catalyst IE3400 Rugged-Serie unterstützen beispielsweise die 802.1AE-Verschlüsselung mit MACsec Key Agreement (MKA) auf Switch-zu-Host-Verbindungen für die Verschlüsselung zwischen dem Switch und fähigen Hostgeräten. Der Switch unterstützt außerdem MACsec-Verschlüsselung für Switch-to-Switch-Sicherheit mithilfe von Cisco TrustSec Network Device Admission Control (NDAC), Security Association Protocol (SAP) und MKA-basiertem Schlüsselaustauschprotokoll.
Der Schutz von Daten während der Speicherung liegt außerhalb des Verantwortungsbereichs von Cisco und es sollten hierzu weitere Überlegungen angestellt werden.

FR5: Eingeschränkter Datenfluss (RDF)
Das Ziel dieser grundlegenden Anforderung besteht darin, die nahtlose Kommunikation zwischen Komponenten einzuschränken, um das vom Standard empfohlene Prinzip der geringsten Rechte durchzusetzen. Die Einschränkung der Kommunikation wird durch die Segmentierung des IACS-Netzwerks erreicht, um die Zonen und Leitungen zu unterstützen, die von jeder Organisation basierend auf ihrer Risikobewertung und dem Sicherheitsniveau, das sie erreichen möchte, definiert werden. Die Netzwerksegmentierung gilt als effiziente Möglichkeit, die Gefährdung des Kontrollsystems durch Cyberbedrohungen zu verringern und die Ausbreitung von Angriffen einzudämmen. Es wird auch genutzt,

um auf einen Vorfall zu reagieren, indem Verbindungen zwischen verschiedenen Netzwerksegmenten unterbrochen werden.

Wie kann Cisco helfen?
Die Industrial Demilitarized Zone (IDMZ) ist der Puffer zwischen kritischen Umgebungen oder Produktionssystemen und dem Unternehmensnetzwerk. Alle gemeinsamen Dienste zwischen der Industriezone und der Unternehmenszone werden im IDMZ angesiedelt sein. Cisco bietet Grenz- oder „Edge"-Sicherheitsgeräte wie die Cisco Secure Firewall, die den Datenverkehr beim Betreten und Verlassen jeder Sicherheitszone überprüfen kann, sowie Replikationsdienste wie den Cisco Telemetry Broker, um die Lücke zwischen dem kritischen und dem unkritischen Netzwerk zu schließen Netzwerk unter Beibehaltung eines segmentierten Netzwerks.
Innerhalb der Anlage selbst und zur Unterstützung des in IEC 62443 vorgeschlagenen Zonen- und Leitungsmodells nutzt Cisco ISE die TrustSec-Technologie zur logischen Segmentierung von Steuerungssystemnetzwerken. Cisco TrustSec-Klassifizierungs- und Richtliniendurchsetzungsfunktionen sind in Cisco Switching-, Routing-, Wireless LAN- und Firewall-Produkte integriert. Am Punkt des Netzwerkzugriffs wird einem Endpunkt eine Cisco TrustSec-Richtliniengruppe namens Security Group Tag (SGT) zugewiesen, normalerweise basierend auf den Benutzer-, Geräte- und Standortattributen dieses Endpunkts. Der SGT bezeichnet die Zugriffsberechtigungen des Endpunkts und der gesamte Datenverkehr vom Endpunkt überträgt die SGT-Informationen. Das SGT wird von Switches, Routern und Firewalls verwendet, um Weiterleitungsentscheidungen zu treffen. Da SGT-Zuweisungen Geschäftsrollen und -funktionen bezeichnen können, können Cisco TrustSec-Kontrollen im Hinblick auf Geschäftsanforderungen und nicht auf zugrunde liegende Netzwerkdetails definiert werden.
Cisco Cyber Vision hilft bei der Definition dieser Geschäftsrollen. Cyber Vision nutzt eine einzigartige Kombination aus passiver und aktiver Erkennung, um alle Ihre Vermögenswerte ohne Risiko für Geräte und Prozesse zu identifizieren. Da die Erkennung durch Ihre industriellen Netzwerkelemente erfolgt, werden Anfragen nicht durch Firewalls oder NAT-Grenzen (Network Address Translation) blockiert, was zu 100 % Transparenz führt. Cyber Vision zeigt Anlagen und ihre Kommunikation in Karten, die Betriebsteams leicht mit ihren industriellen Prozessen in Verbindung bringen können. Dies gibt ihnen die Möglichkeit, Assets in Zonen (z. B. Produktionszellen) zu gruppieren und die Netzwerksegmentierungslogik zu definieren. Cyber Vision teilt diese Informationen automatisch mit ISE, um entsprechende Sicherheitsrichtlinien zu erstellen. Um Compliance-Anforderungen zu erfüllen, verwaltet Cyber Vision den Verlauf aller Ereignisse und Anwendungsflüsse, einschließlich variabler Zugriffe, sodass Sie problemlos forensische Suchen durchführen und Berichte erstellen können.

FR6: Rechtzeitige Reaktion auf Ereignisse (TRE)
Das Ziel dieser grundlegenden Anforderung besteht darin, sicherzustellen, dass IACS-Komponenten ordnungsgemäß überwacht werden, um sicherzustellen, dass sie sicher bleiben. Diese Anforderungen sind so konzipiert, dass Organisationen die Tools und Verfahren implementieren, um forensische Beweise zu sammeln und auf Sicherheitsverstöße zu reagieren. Die fünf Sicherheitsstufen legen unterschiedliche Erwartungen daran fest, wie schnell die zuständigen Behörden benachrichtigt werden, wenn ein Ereignis Auswirkungen auf die Sicherheit der Systeme hat.

Wie kann Cisco helfen?
Cisco Cyber Vision verwaltet den Verlauf aller Ereignisse und Anwendungsflüsse. Es ermöglicht Ihnen, schnell Ihren aktuellen Sicherheitsstatus zu verstehen, Anomalien und Schwachstellen zu identifizieren und auf Bedrohungen zu reagieren. Cyber Vision bietet verschiedene Dashboards, Berichte und Ereignisverläufe, um Sicherheitsbedenken leicht zu erkennen. Darüber hinaus integriert Cyber Vision die Snort IDS-Engine, die die Bedrohungsinformationen von Cisco Talos nutzt, um bekannte und neu auftretende Bedrohungen wie Malware oder böswilligen Datenverkehr zu erkennen.
Cyber Vision ist mit führenden SIEM- und SOAR-Plattformen (Security, Orchestration, Automation, and Response) wie IBM QRadar und Splunk vorintegriert und kann OT-Ereignisse und -Warnungen mithilfe von Syslog an jedes andere Tool weiterleiten. Um Ereignismüdigkeit zu vermeiden, können Sie sogar auswählen, welche Ereignistypen geteilt werden sollen.
Cisco XDR bündelt Informationen aus Cisco-Sicherheitsprodukten und Quellen von Drittanbietern, um zu ermitteln, ob beobachtbare Daten wie Datei-Hashes, IP-Adressen, Domänen und E-Mail-Adressen verdächtig sind. Wenn Sie eine Untersuchung starten, wird automatisch Kontext von integrierten Cisco-

Sicherheitsprodukten hinzugefügt, sodass Sie sofort wissen, welches Ihrer Systeme angegriffen wurde und wie. Es bringt dieses Wissen aus Geheimdienstquellen und Sicherheitsprodukten zurück und zeigt Ergebnisse in Sekundenschnelle an. Cisco XDR bietet Sicherheitsteams außerdem die Möglichkeit, sofort zu handeln, indem sie benutzerdefinierte Workflows auslösen oder ihre Untersuchung mit den bereitgestellten Tools fortführen.

FR7: Ressourcenverfügbarkeit (RA)
Das Ziel dieser grundlegenden Anforderung besteht darin, sicherzustellen, dass IACS-Komponenten weiterhin wesentliche Funktionen bereitstellen, um einen weiterhin sicheren Betrieb zu gewährleisten, wenn sie in einer beeinträchtigten Umgebung ausgeführt werden, beispielsweise wenn ein Denial-of-Service-Angriff (DoS) auftritt. Dies bedeutet, dass Sie in der Lage sind, den Netzwerkverkehr zu priorisieren, Abweichungen von den Baselines zu erkennen, Systeme aus Backups wiederherzustellen und vieles mehr. Damit all dies möglich ist, müssen Unternehmen eine detaillierte Bestandsaufnahme aller ihrer IACS-Komponenten führen.

Wie kann Cisco helfen?
Das gesamte Ziel der industriellen Sicherheitsarchitektur von Cisco besteht darin, die Integrität und Verfügbarkeit von IACS-Ressourcen sicherzustellen. Dies wird durch verschiedene Techniken erreicht, wie in der folgenden Tabelle beschrieben.
Darüber hinaus bietet die Cisco-Netzwerkinfrastruktur die Möglichkeit, Quality of Service (QoS) zum Schutz vor DoS-Angriffen zu konfigurieren. Benutzer können bestimmten Netzwerkverkehr auswählen und ihn entsprechend seiner relativen Bedeutung priorisieren. Durch die Implementierung von QoS im Netzwerk wird die Netzwerkleistung vorhersehbarer und die Bandbreitennutzung effektiver. Wenn ein Netzwerksegment gefährdet ist, trägt QoS dazu bei, sicherzustellen, dass die Ressourcennutzung anderer Netzwerksegmente in derselben physischen Infrastruktur nicht beeinträchtigt wird.

Systemanforderungen für die Ressourcenverfügbarkeit

SR	Beschreibung	Worauf sollten Sie achten?
7.1	DoS-Schutz	● Obwohl Cisco DoS-Schutz bietet, gilt diese Anforderung, während eines DoS-Angriffs in einem herabgesetzten Modus ausgeführt zu werden, für IACS-Entwickler.
7.2	Resourcenmanagement	● Cisco empfiehlt die Verwendung von QoS-Richtlinien in der Netzwerkinfrastruktur, um sicherzustellen, dass kritische Systeme im Netzwerk immer Vorrang haben und nicht von DoS-Angriffen auf die Netzwerkinfrastruktur betroffen sind.
7.3	Sicherung des Steuerungssystems	● Cisco bietet die Möglichkeit, Netzwerkkonfigurationen zu sichern, wenn ein zentralisiertes Verwaltungstool wie Cisco Catalyst Center (vormals DNA-Center) verwendet wird.
7.4	Wiederherstellung und Wiederherstellung des Kontrollsystems	● Cyber Vision kann verwendet werden, um zu erkennen, welches System kompromittiert wurde, um die für die Rekonstruktion des IACS-Netzwerks erforderliche Zeit zu verkürzen. ● Cyber Vision hilft zu beweisen, dass das System nach der Wiederherstellung einen bekannten sicheren Zustand erreichen konnte.
7.5	Notstrom	● Die Cisco Industrial Ethernet (IE)-Switches bieten die Möglichkeit, zu und von einer Notstromversorgung umzuschalten, um sicherzustellen, dass das Netzwerk auch bei einem primären Stromausfall betriebsbereit bleibt.
7.6	Netzwerk- und Sicherheitskonfigurationseinstellungen	● Die Netzwerkkonfiguration kann vom Cisco Catalyst Center live auf dem Steuerungssystem überprüft und mit

		empfohlenen Netzwerk- und Sicherheitskonfigurationen verglichen werden.
7.7	Geringste Funktionalität	● Cisco Secure Firewall kann verwendet werden, um die Verwendung unnötiger Funktionen, Ports, Protokolle und/oder Dienste über Netzwerkgrenzen hinweg zu verhindern. ● Cisco ISE kann verwendet werden, um dieselben Dienste seitlich/vertikal zu verbieten, wenn sie die Netzwerkinfrastruktur über ACLs und/oder SGTs durchqueren. ● Cyber Vision hilft bei der Erkennung verbotener oder unerwarteter Netzwerkkommunikation (Flows, Ports, Shadow- Kommunikation, Network Pollution usw.).
7.8	Bestandsaufnahme der Komponenten des Steuerungssystems	● Cyber Vision erkennt installierte Komponenten und deren Eigenschaften passiv, wenn sie im Netzwerk kommunizieren. ● Cyber Vision ist in der Lage, Komponenten im Netzwerk mithilfe der Semantik der verwendeten Protokolle aktiv abzufragen, um zusätzliche Details zu deren Eigenschaften und Konfigurationen zu sammeln.

Abbildung 9 Tabelle der Systemanforderungen für die Ressourcenverfügbarkeit

Beginnen Sie jetzt Ihre ISA/IEC-62443-3-Reise

Seit über 15 Jahren unterstützt Cisco Industrieunternehmen auf der ganzen Welt bei der Digitalisierung ihrer Abläufe durch die Entwicklung eines marktführenden Netzwerkportfolios, das speziell für industrielle Anwendungsfälle entwickelt wurde. Unser tiefes Verständnis der OT-Anforderungen und ein umfassendes Cybersicherheitsportfolio sind eine seltene Kombination.

Cisco ist davon überzeugt, dass eine solide und flexible Netzwerkarchitektur ein wichtiges Erfolgskriterium für robuste Sicherheit ist. Schlechtes Netzwerkdesign kann eine große Schwachstelle schaffen und die Konzepte der Segmentierung und Erweiterbarkeit sowie die Integration von Cybersicherheitskontrollen und physischen Sicherheitsmaßnahmen behindern.

Unsere Erfahrung zeigt jedoch, dass der Aufbau eines sicheren industriellen Netzwerks nicht über Nacht gelingt. Um den Erfolg sicherzustellen, fördert Cisco einen stufenweisen Ansatz, bei dem jede Phase die Grundlage für die nächste bildet, sodass Sie Ihre Sicherheitslage in Ihrem eigenen Tempo verbessern und allen Beteiligten auf diesem Weg einen Mehrwert bieten können.

Aufbauend auf dem Zonen- und Leitungskonzept ISA/IEC-62443-3 hat Cisco eine Referenzarchitektur entwickelt, die die verschiedenen Schritte beschreibt, die Unternehmen befolgen sollten, um ihre industriellen Steuerungssysteme zu sichern und gleichzeitig die Einhaltung des Standards sicherzustellen. Das Cisco Industrial Security Validated Design (CVD) erfüllt die Betriebsanforderungen gemäß ISA/IEC-62443-3 und nutzt außerdem das NIST-Cybersicherheits-Framework, mit dem IT- und Sicherheitsteams besser vertraut sind.

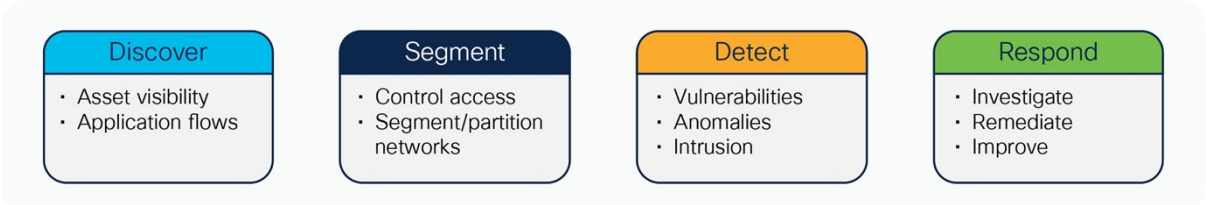

Abbildung 10 Die Elemente des NIST Cybersecurity Frameworks

Entdecken - Discover

Cisco Cyber Vision bietet Einblick in alle Industrieanlagen und deren Anwendungsabläufe. Es erstellt dynamische Inventare mit detaillierten Informationen zu allen angeschlossenen Geräten, verfolgt Kommunikationsaktivitäten zur Überwachung von Zonen und Leitungen und hilft bei der Risikobewertung,

indem es die IACS-Gefährdung durch Cyberbedrohungen identifiziert. Cyber Vision-Sensoren sind in die Zellen-/Bereichsnetzwerkausrüstung eingebettet, um eine maßstabsgetreue Sichtbarkeit zu gewährleisten.

Segmentieren - Segment
Das Industrienetzwerk ist vom Unternehmensnetzwerk durch eine Industrial Demilitarized Zone (IDMZ) getrennt, die von Cisco Secure Firewalls implementiert wird. Es kann auch verwendet werden, um die verschiedenen Teile des Industrienetzwerks zu segmentieren, sodass jedes Segment eine halbautonome Zone bildet, um Sicherheitsvorfälle innerhalb einer Zone zu begrenzen und einzudämmen.
Für eine detailliertere Segmentierung und dynamische Zugriffskontrolle setzt die Cisco Identity Services Engine (ISE) automatisch Sicherheitsrichtlinien auf Geräteebene durch. Es nutzt Zonen, die von Kontrollingenieuren in Cyber Vision konfiguriert wurden, um das Netzwerk anzuweisen, den Kommunikationsfluss entsprechend einzuschränken.
Cisco ISE kann auch Aktivitäten von Remote-Benutzern einschränken, die über Cisco Secure Client (einschließlich AnyConnect) VPN-Zugriff auf das Industrienetzwerk erhalten. Cisco Secure Equipment Access ist eine weitere Fernzugriffslösung, die nur einzelnen Geräten Zugriff gewährt. Beide Lösungen können MFA mit Cisco Duo nutzen.

Erkennen - Detect
Cisco Cyber Vision warnt Sie vor Hardware- und Software-Schwachstellen, die für jedes OT-Gerät behoben werden müssen, und integriert außerdem eine Snort IDS-Engine zur Erkennung von Eindringlingen und bösartigem Datenverkehr. Dank dieser umfassenden Transparenz der OT-Netzwerkaktivitäten können Sie Baselines erstellen, um Abweichungen vom normalen Verhalten zu erkennen.
Cisco Secure Network Analytics (ehemals Cisco Stealthwatch) hilft auch bei der Erkennung von Anomalien, indem es Telemetriedaten von Netzwerkgeräten sammelt und Netzwerkflüsse überwacht.
Cisco Secure Firewall integriert Cisco Secure IPS, Secure Firewall Malware Defense, erweiterte Distributed DoS (DDoS)-Abwehr und URL-Filterung, um eine umfassende Erkennung und Schutz vor Eindringlingen zu bieten. Es kann auch Talos-Signaturdateien nutzen, um Schwachstellen-Exploits zu blockieren.
Cisco Secure Endpoint bietet erweiterten Malware-Schutz für Ihre verschiedenen Endpunkte (Workstations, Server, Laptops, Tablets usw.) und kann identifizieren, welche Prozesse auf dem geschützten Endpunkt im Netzwerk kommunizieren.

Reagieren - Respond
Cisco XDR beschleunigt Untersuchungen, indem es Bedrohungsinformationen und Daten aus mehreren Sicherheitstechnologien – Cisco und anderen – in einer einheitlichen Ansicht zusammenfasst. Es optimiert Abhilfemaßnahmen, indem es ein umfassendes Fallmanagement bietet und benutzerdefinierte Playbooks für Ihre spezifische Umgebung ermöglicht.
Cyber Vision und andere Sicherheitstools können Protokollereignisse zur weiteren Untersuchung und Korrelation auf SIEM-Plattformen exportieren.

Das Cisco Validated Design (CVD)
Das OT-Sicherheitsreferenzdesign von Cisco ist ein Entwurf für ein sicheres, robustes und zuverlässiges Industrienetzwerk. Es nutzt die umfassenden Netzwerk- und Sicherheitstechnologien von Cisco, um Industrieanlagentransparenz, Makro-/Zonensegmentierung, Zonenzugriffskontrolle, Bedrohungserkennung und Reaktion bereitzustellen. Es ermöglicht die Koordination mit der Informationssicherheit für ein konsistentes Zugriffsrichtlinienmanagement und die Aggregation industrieller Sicherheitsereignisse im Security Operations Center (SOC).

Wie in der Abbildung unten dargestellt, folgt dieses Design dem Purdue/ISA95-Modell und bietet detaillierte Design- und Implementierungsrichtlinien, um die Einhaltung von ISA/IEC-62443-3 zu erreichen.

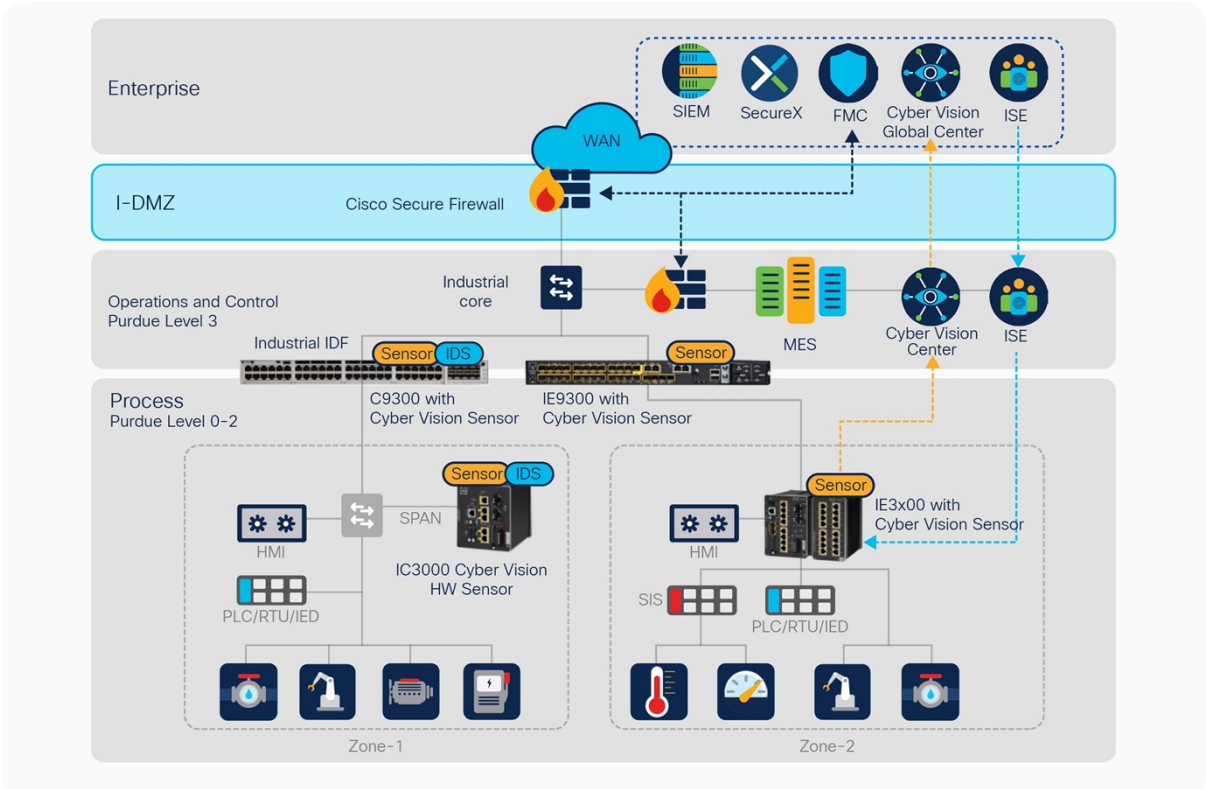

Abbildung 11 Cisco OT Security Validated Design

Zusammenfassung

Wie bei jeder anderen Sicherheitsmaßnahme ist der Schutz industrieller Automatisierungs- und Steuerungssysteme kein Produkt, sondern ein kontinuierlicher Prozess. Dies gilt für die Komponentenentwicklung bestehend aus Hardware und Software, den Betrieb, die Wartung und alle anderen damit verbundenen Tätigkeiten. Cisco geht dieses wesentliche Paradigma nicht nur bei der Produktentwicklung auf Basis von Cisco SDL an, sondern auch bei der Verbesserung von Architektur- und Bereitstellungsreferenzen wie den Cisco Validated Designs.

Links und Referenzen

- ISA99 standard committee
- IEC62443-3-3 standard download
- Cisco Validated Design for industrial security
- Cisco Industrial Threat Defense solution for securing industrial networks
- Cisco Secure Development Lifecycle (Cisco SDL)
- Contact Cisco to discuss your industrial security needs

Cisco Zero Trust Framework

Diese Übersicht bietet Anleitungen zu den verschiedenen Zero Trust Frameworks und ihrer Beziehung zum Cisco Zero Trust Framework. Für jedes der Zero Trust Frameworks wird eine Zuordnung zum Cisco-Produkt bereitgestellt.

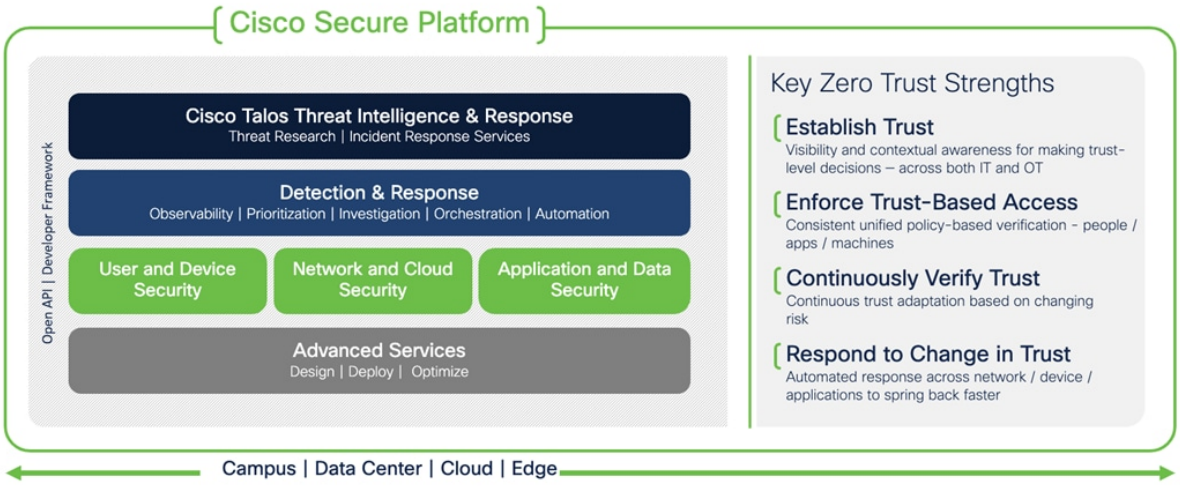

Abbildung 12: Zero Trust Architecture Framework

Sicherheit ist kein Patentrezept und Zero Trust ist mehr als nur Netzwerksegmentierung. Um die Architektur besser zu verstehen, hat Cisco sie in drei Säulen unterteilt:

1. **Benutzer- und Gerätesicherheit**: Stellen Sie sicher, dass Benutzer und Geräte unabhängig vom Standort vertrauenswürdig sind, wenn sie auf Systeme zugreifen
2. **Netzwerk- und Cloud-Sicherheit**: Schützen Sie alle Netzwerkressourcen vor Ort und in der Cloud und gewährleisten Sie einen sicheren Zugriff für alle verbindenden Benutzer
3. **Anwendungs- und Datensicherheit**: Verhindern Sie unbefugten Zugriff in Anwendungsumgebungen, unabhängig davon, wo diese gehostet werden

Zero Trust kann nicht durch ein einzelnes Produkt gelöst werden. Zero Trust kann nur durch die ordnungsgemäße Integration von Sicherheitstools verwirklicht werden, um eine adaptive, skalierbare und integrierte Sicherheitslösung bereitzustellen, die alle Zero Trust-Prinzipien anwendet.

Im Allgemeinen führt der übermäßige Einsatz der „besten“ Einzelprodukte nicht zu der zusammenhängenden Sicherheitsstrategie, die Zero Trust bieten kann.

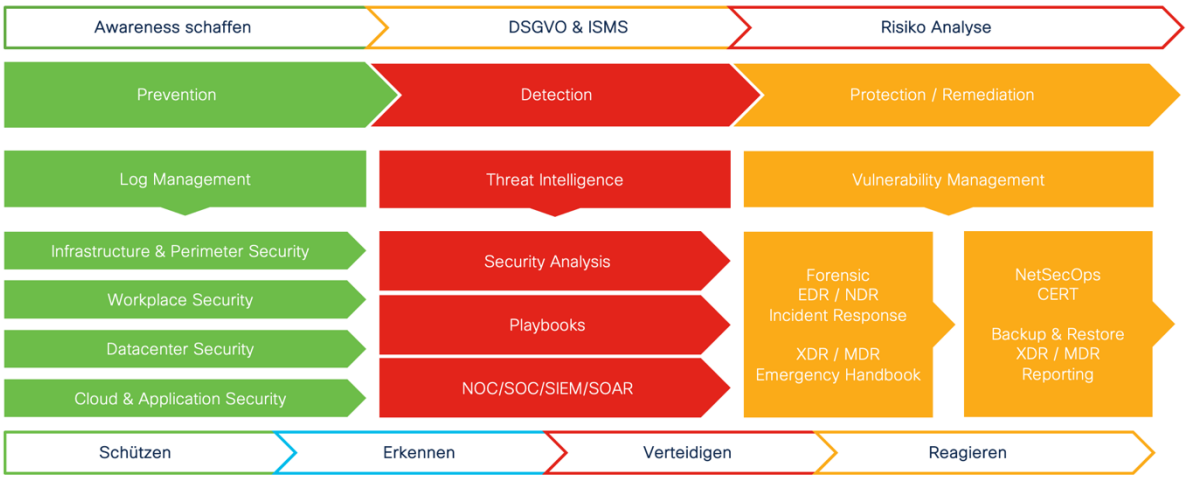

Abbildung 13 Cybersecurity Verteidigungskonzept

Nachfolgende Abbildung zeigt eine Übersicht der Netzwerk Segmentierungsstrategien, aufgeteilt in Makro- Mikro- sowie Nanosegmentierung als auch die Remediation Werkzeuge von Cisco.

Netzwerk	Makro- Segmentierung	Mikro- Segmentierung	Nano- Segmentierung	Remediation
Cloud	Multicloud Defense cdFW	Multicloud Defense Secure Workload	Secure Workload	XDR cdFMC CDO
DMZ	Secure Firewall Meraki MX			XDR FMC CDO
Campus	Secure Firewall SD-Access	Identity Services Engine TrustSec Catalyst Center	Secure Network Analytics	XDR FMC ISE
Datacenter/Apps	Secure Firewall ACI	ACI Secure Workload cdFW	Secure Workload	XDR FMC
WAN	Secure Firewall Meraki MX	Catalyst SD-WAN Meraki SD-WAN	Secure Access	XDR FMC CDO
Industrie DMZ	Secure Firewall			XDR FMC
OT	Secure Firewall	Cyber Vision Identity Services Engine TrustSec	Cyber Vision Identity Services Engine Secure Network Analytics	XDR FMC ISE
Endpunkt/Client	Secure Firewall Meraki MX	Secure Endpoint Secure Client ISE Posture		XDR FMC CDO ISE Secure Endpoint

Abbildung 14 Netzwerk Segmentierungsstrategien sowie Remediation mit Cisco

Zero-Trust-Sicherheits-Frameworks

Die folgende Tabelle zeigt, wie Zero Trust Frameworks dem Cisco Zero Trust Framework zugeordnet werden.

Cisco	NIST 800-207 Zero Trust Architecture	CISA Zero Trust Maturity Model	DISA Zero Trust Framework	Common
User and Device Security	Users and/or Devices	Identity	Users	Visibility & Analytics Automation & Orchestration Governancec
		Devices	Devices	
Network and Cloud Security	Policy Decision and Enforcement Points	Networks	Network/Environment	
Application and Data Security	Enterprise Resources	Applications and Workloads	Workloads	
		Data	Data	

Abbildung 15 Zero Trust Frameworks Mapping

NIST-Sonderpublikation 800-207 – Zero-Trust-Architektur

Das National Institute of Standards and Technology (NIST) entwickelt Cybersicherheitsstandards, Richtlinien, Best Practices und andere Ressourcen, um den Anforderungen der US-amerikanischen Industrie, Bundesbehörden und der breiten Öffentlichkeit gerecht zu werden.

NIST definiert sowohl Zero Trust als auch eine Zero Trust-Architektur wie folgt: „Zero Trust (ZT) bietet eine Sammlung von Konzepten und Ideen, die darauf abzielen, die Unsicherheit bei der Durchsetzung präziser Zugriffsentscheidungen mit den geringsten Berechtigungen pro Anfrage in Informationssystemen und -diensten angesichts eines zu minimieren Netzwerk als gefährdet angesehen. Zero Trust Architecture (ZTA) ist der Cybersicherheitsplan eines Unternehmens, der Zero-Trust-Konzepte verwendet und

Komponentenbeziehungen, Workflow-Planung und Zugriffsrichtlinien umfasst. Daher ist ein Zero-Trust-Unternehmen die Netzwerkinfrastruktur (physisch und virtuell) und betriebsbereit Richtlinien, die für ein Unternehmen als Produkt eines ZTA-Plans gelten." (NIST 800-207 – 2.0 – Zero Trust-Grundlagen)

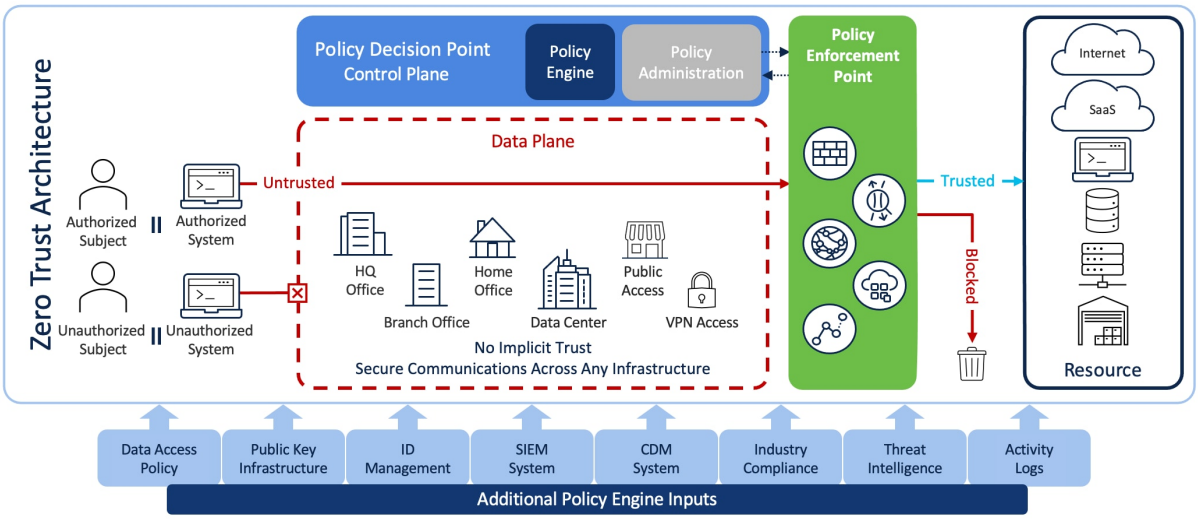

Abbildung 16: NIST Zero Trust Architecture

NIST SP800-207 – Zuordnung der Zero-Trust-Architektur zum Cisco-Produkt

NIST 800-207 Logical Component	Cisco Product
Policy Engine (PE)	Cisco Secure Access Cisco Duo Cisco Umbrella Cisco Identity Services Engine
Policy Administrator (PA)	Cisco Secure Access Cisco Duo Cisco Umbrella Cisco Identity Services Engine Cisco Defense Orchestrator Cisco Secure Firewall Management Center Cisco Secure Workload
Data Access Policies	Cisco Secure Access Cisco Duo Cisco Umbrella Cisco Identity Services Engine Cisco Defense Orchestrator Cisco Secure Firewall Management Center Cisco Secure Workload Cisco Secure Network Analytics Cisco Network Devices

NIST 800-207 Logical Component	Cisco Product
	Cisco Wireless Devices
Continuous Diagnostics and Mitigation System	Cisco Secure Access Cisco Duo Cisco Identity Services Engine Cisco Defense Orchestrator Cisco Secure Firewall Management Center Cisco Secure Workload Cisco Secure Network Analytics Cisco Secure Application Cisco Secure Application Cloud Native Cisco Network Devices Cisco Wireless Devices
Industry Compliance System	Cisco Secure Access Cisco Duo Cisco Identity Services Engine Cisco Secure Network Analytics
Public Key Infrastructure	
Policy Enforcement Point	Cisco Secure Access Cisco Duo Cisco Umbrella Cisco Identity Services Engine Cisco Secure Firewall Cisco Secure Workload Cisco Cyber Vision Cisco Network Devices Cisco Wireless Devices
Threat Intelligence Feed(s)	Cisco Secure Firewall Cisco Identity Services Engine Cisco XDR Cisco Talos Cisco Secure Insights Cisco Network Devices Cisco Wireless Devices Cisco Security Analytics and Logging (SAL) Cisco Vulnerability Management (Kenna.VM)

NIST 800-207 Logical Component	Cisco Product
Network and System Activity Logs	Cisco Secure Access Cisco Duo Cisco Secure Application Cisco Secure Application Cloud Native Cisco Network Devices Cisco Wireless Devices
ID Management System	
Security Information and Event Management (SIEM)	Cisco XDR

Abbildung 17 Zuordnung NIST Framework zum Cisco Produkt

CISA Zero Trust Maturity Model V2.0
Die Cybersecurity and Infrastructure Security Agency (CISA) leitet die nationalen Bemühungen der Vereinigten Staaten, Risiken für unsere Cyber- und physische Infrastruktur zu verstehen, zu verwalten und zu reduzieren. Ihre Mission erstreckt sich auf drei Hauptbereiche: Cybersicherheit, Infrastruktursicherheit und Notfallkommunikation.

Das CISA Zero Trust Maturity Model v2.0 ist eine von vielen Roadmaps, auf die Behörden beim Übergang zu einer Zero-Trust-Architektur zurückgreifen können. Das Reifegradmodell zielt darauf ab, Behörden bei der Entwicklung von Zero-Trust-Strategien und Implementierungsplänen zu unterstützen und Wege aufzuzeigen, wie verschiedene CISA-Dienste Zero-Trust-Lösungen behördenübergreifend unterstützen können.

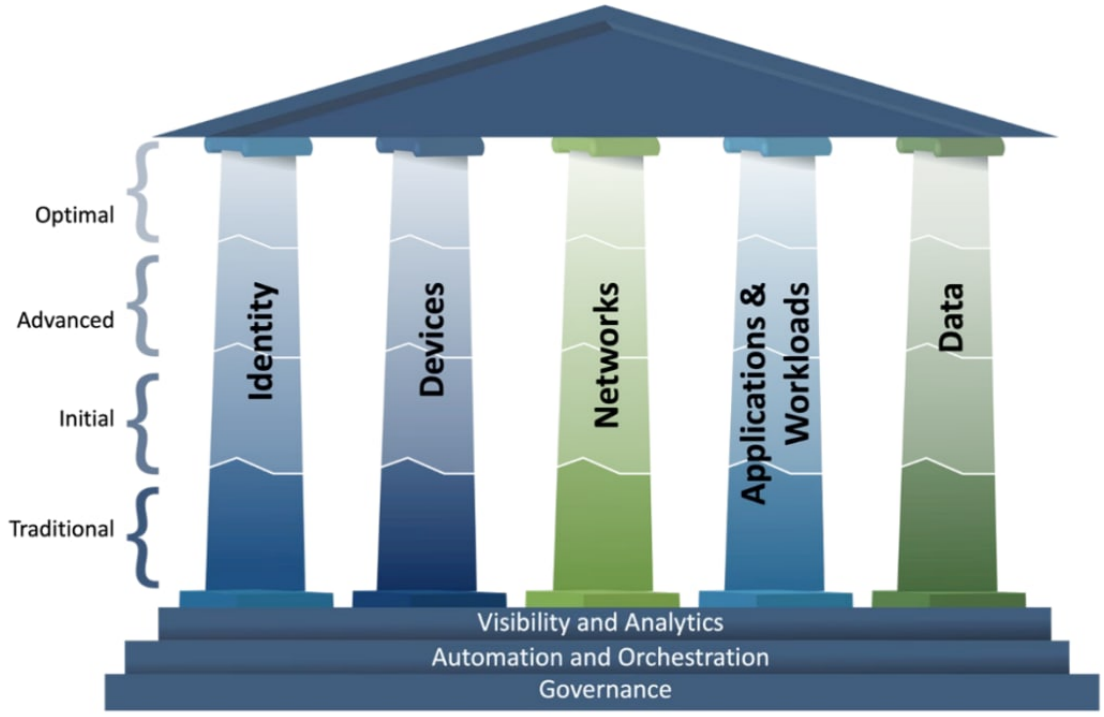

Abbildung 18 CIST Zero Trust Reifegrad Modell

Quelle: CISA Zero Trust Maturity Model V2.0

Behörden sollten die folgenden Leitkriterien jeder Phase verwenden, um den Reifegrad für jede Zero-Trust-Technologiesäule zu ermitteln und für Konsistenz im gesamten Reifegradmodell zu sorgen:

- **Traditionell** – manuell konfigurierte Lebenszyklen (d. h. von der Einrichtung bis zur Stilllegung) und Zuweisungen von Attributen (Sicherheit und Protokollierung); statische Sicherheitsrichtlinien und -lösungen, die jeweils eine Säule mit diskreten Abhängigkeiten von externen Systemen adressieren; geringste Berechtigung wird nur bei der Bereitstellung festgelegt; isolierte Säulen der Richtliniendurchsetzung; manuelle Reaktions- und Schadensbegrenzungsbereitstellung; und begrenzte Korrelation von Abhängigkeiten, Protokollen und Telemetrie
- **Anfänglich** – beginnende Automatisierung der Attributzuweisung und Konfiguration von Lebenszyklen, Richtlinienentscheidungen und -durchsetzung sowie erste säulenübergreifende Lösungen mit Integration externer Systeme; einige reaktionsfähige Änderungen an der geringsten Berechtigung nach der Bereitstellung; und aggregierte Sichtbarkeit für interne Systeme
- **Erweitert** – wo anwendbar, automatisierte Kontrollen für den Lebenszyklus und die Zuweisung von Konfigurationen und Richtlinien mit säulenübergreifender Koordination; zentralisierte Sichtbarkeit und Identitätskontrolle; Durchsetzung der Politik über alle Säulen hinweg integriert; Reaktion auf vordefinierte Abhilfemaßnahmen; Änderungen der geringsten Privilegien basierend auf Risiko- und Haltungsbewertungen; und Aufbau einer unternehmensweiten Sensibilisierung (einschließlich extern gehosteter Ressourcen)

- **Optimal** – vollständig automatisierte Just-in-Time-Lebenszyklen und Zuweisungen von Attributen zu Assets und Ressourcen, die sich selbst mit dynamischen Richtlinien auf der Grundlage automatisierter/beobachteter Auslöser melden; dynamischer Zugriff mit geringsten Privilegien (gerade ausreichend und innerhalb von Schwellenwerten) für Assets und ihre jeweiligen Abhängigkeiten unternehmensweit; säulenübergreifende Interoperabilität mit kontinuierlicher Überwachung; und zentralisierte Sichtbarkeit mit umfassendem Situationsbewusstsein

Eine Zuordnung des CIST Zero Trust Reifegrad Modells zu Cisco Produkten finden Sie hier: https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/zt-frameworks.html

DISA Zero Trust Framework
Das DISA Zero Trust Framework ist eine Reihe von Sicherheitsprinzipien und Best Practices, die von der U.S. Defense Information Systems Agency (DISA) entwickelt wurden, um die Cybersicherheit in Regierungsbehörden und anderen Organisationen zu verbessern. Das Framework soll das Risiko von Cyberangriffen und Datenschutzverletzungen minimieren, indem es davon ausgeht, dass kein Benutzer, Gerät oder Netzwerk grundsätzlich vertrauenswürdig ist, und stattdessen jede Anfrage überprüft, bevor Zugriff auf sensible Ressourcen gewährt wird.

Zero-Trust-Säulen sind identifiziert und stimmen mit der branchenüblichen Identifizierung von Zero-Trust-Säulen überein. Eine Säule ist ein zentraler Schwerpunktbereich für die Implementierung von Zero-Trust-Kontrollen. Zero Trust wird unten als ineinandergreifende Puzzleteile dargestellt, die eine Datensäule symbolisieren, die von Schutzsäulen umgeben ist. Alle Schutzsäulen arbeiten zusammen, um die Datensäule effektiv zu schützen.

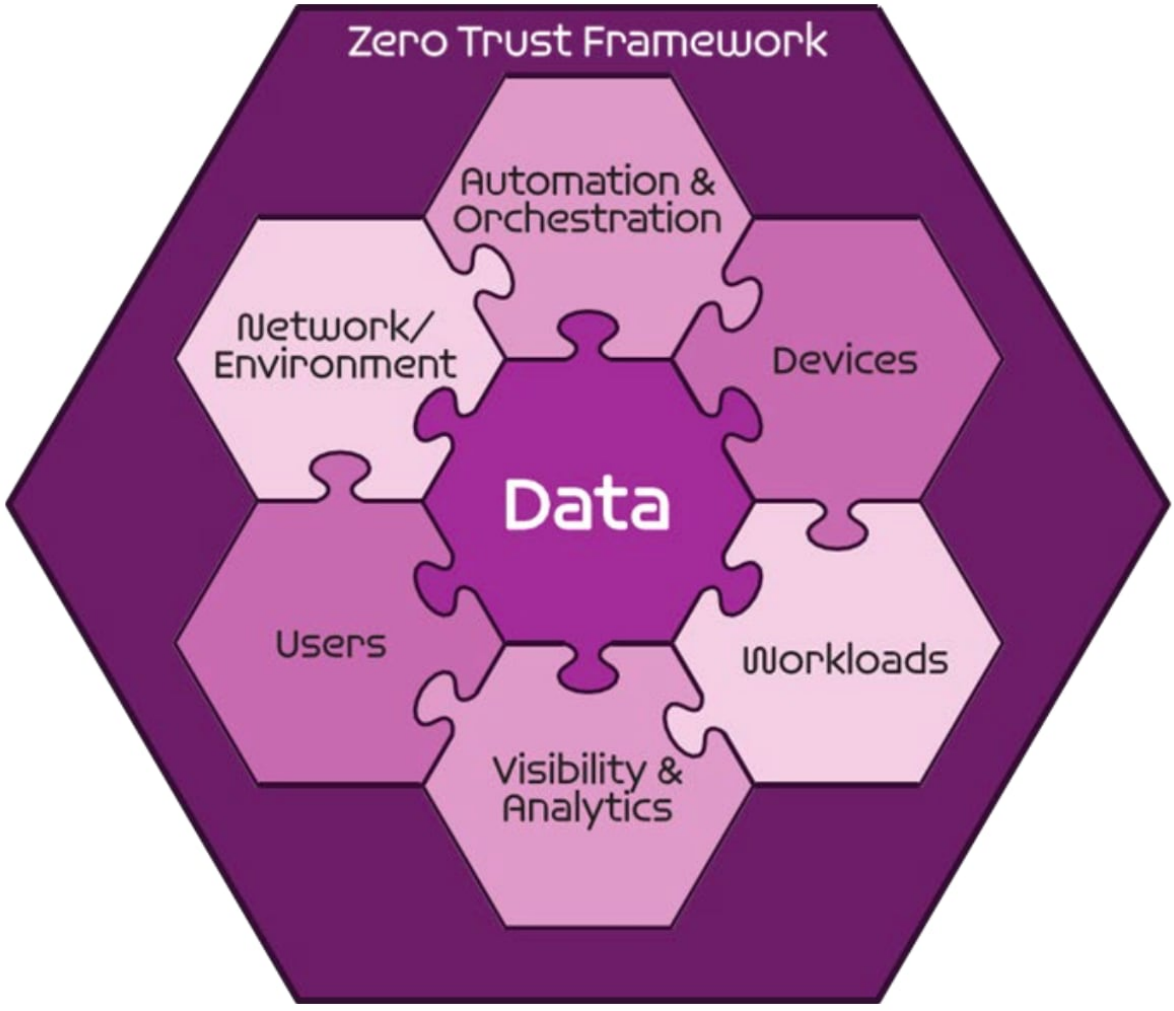

Abbildung 19 DISA Zero Trust Framework

Um das DISA Zero Trust Framework zu implementieren, verfolgen Unternehmen in der Regel einen mehrschichtigen Ansatz, der Technologien wie Netzwerksegmentierung, Identitäts- und Zugriffsverwaltung (IAM), Privileged Access Management (PAM) sowie kontinuierliche Überwachungs- und Bedrohungserkennungstools umfasst. Dieser Ansatz hilft Unternehmen, ein hohes Maß an Sicherheit aufrechtzuerhalten und das Risiko von Datenschutzverletzungen und Cyberangriffen zu verringern.

Links und Referenzen

- Cisco Zero Trust Security
- Zero Trust: Going Beyond the Perimeter
- Cisco Secure Workload
- Cisco Software-Defined Access
- Cisco SAFE
- Cisco Zero Trust Architecture Guide
- Cisco Zero Trust: User and Device Design Guide (CVD)
- Cisco Zero Trust: Network and Cloud Security Design Guide (CVD)
- CISA Zero Trust Maturity Model V2.0
- NIST Special Publication 800-207 – Zero Trust Architecture
- DISA Zero Trust Framework

Cisco Validated Design

Unser Plan für erfolgreiches Systemdesign

Cisco Validated Designs sind getestete und dokumentierte Ansätze, die Sie beim erfolgreichen Entwerfen, Bereitstellen und Erweitern neuer Technologien unterstützen. Diese Leitfäden dokumentieren den Aufbau möglicher Netzwerkkonfigurationen, wie sichergestellt wird, dass neue Lösungen in bestehende Systeme passen, und bieten Best Practices für erfolgreiche Bereitstellungen.

Schnellere Bereitstellungen

Von Systementwürfen bis hin zu Konfigurationsanweisungen – CVDs erleichtern Ihnen die schnelle Implementierung Ihrer Lösungen.

Weniger Risiko

Seien Sie zuversichtlich, dass Produkte für den Erfolg zusammenarbeiten – CVDs basieren auf gemeinsamen Anwendungsfällen und technischen Systemprioritäten.

Vorhersagbarkeit

Aufgrund umfangreicher Tests helfen Ihnen CVDs dabei, Leistungserwartungen festzulegen und schnellere, zuverlässigere Bereitstellungen sicherzustellen.

Mehr darüber erfahren Sie in der Cisco Validated Design Zone für Ihre Branche und Anforderungen:
https://www.cisco.com/c/en/us/solutions/design-zone.html
Sowie in der Cisco Validated Design Guides for Industries:
https://www.cisco.com/c/en/us/solutions/design-zone/industries.html

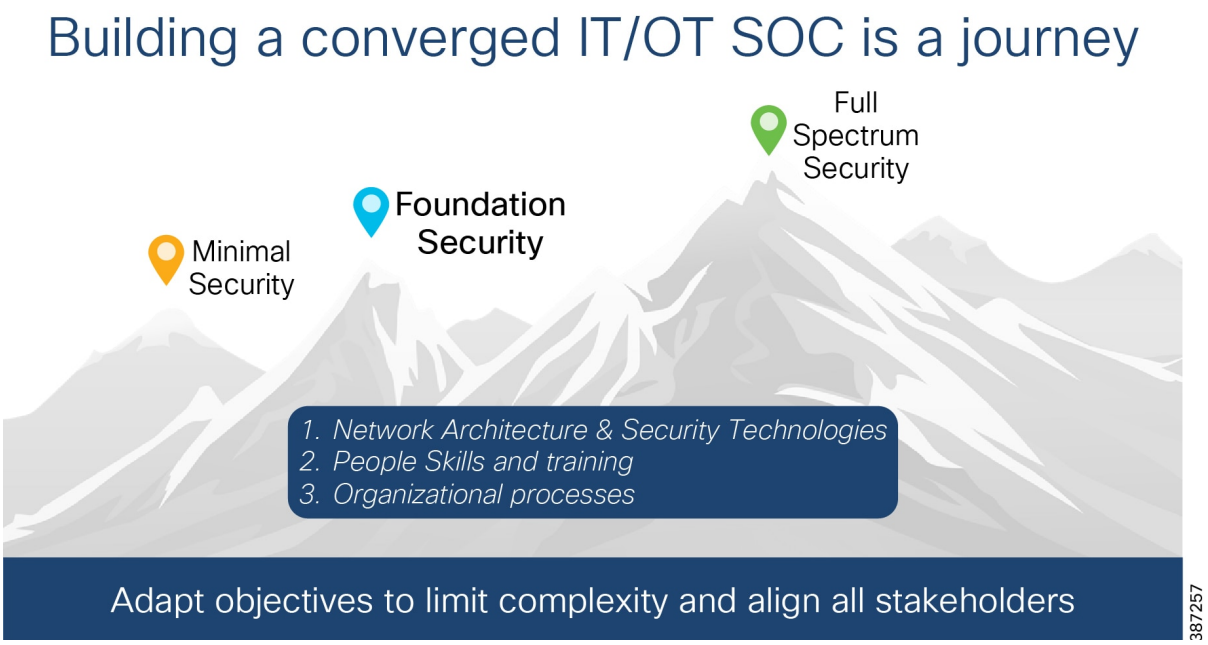

Abbildung 20: Security Reise

Die Reise zur umfassenden IT/OT Sicherheitsstrategie beginnt bei der Netzwerkarchitektur sowie der Einsatz von geeigneten Sicherheitstechnologien, setzt sich bei Menschen und ihren Fähigkeiten fort und mündet in organisatorischen Prozessen.

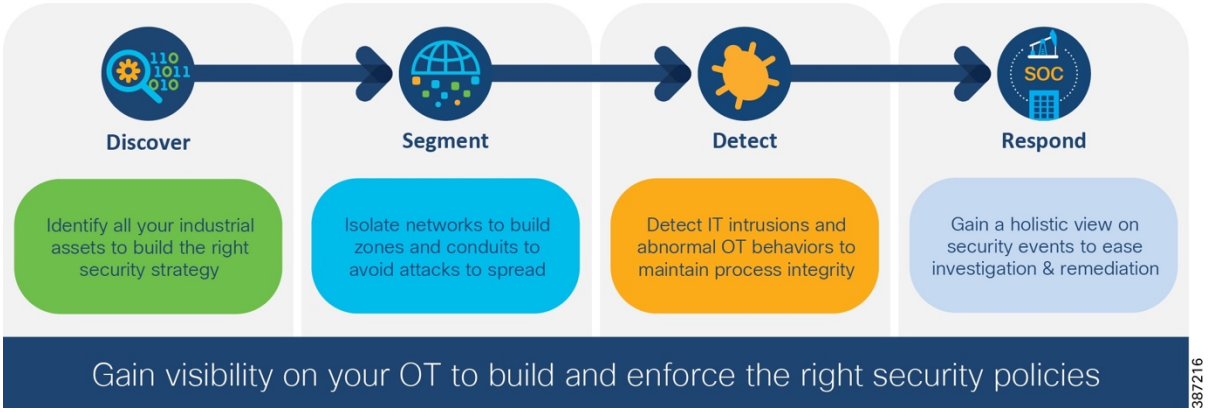

Abbildung 21: Schlüsselelemente und Phasen basierter Ansatz zur Sicherheit im Industriellen Netzwerk.

In Anlehnung an das NIST Framework ergeben sich die Phasen der IT/OT Sicherheit:

1. **Identifizieren der Assets** im Unternehmen, Sichtbarkeit in IT- und OT-Bereiche bekommen, Kommunikation im Netzwerk, am Endpunkt und von Applikationen überwachen
2. **Schützen durch** Zugangskontrolle, **Netzwerk Segmentierung**, Mikro- und Makrosegmentierung, Erstellen von Zonen, um Angriffe lokal zu halten
3. **Erkennen von Schwachstellen und Anomalien**, sowie Attacken erkennen
4. **Reagieren**, Untersuchen, Kontrollieren, Abhilfe schaffen sowie Verbessern
5. **Wiederherstellen**, Prozesse und Abläufe planen sowie effektiv nach intern und extern Kommunizieren

Von ICS/OT-Sichtbarkeit über Zero Trust bis hin zu einer konvergenten IT/OT-Sicherheitsstrategie – finden Sie bei Cisco Lösungen und dies analog zum NIST Cybersecurity Framework:

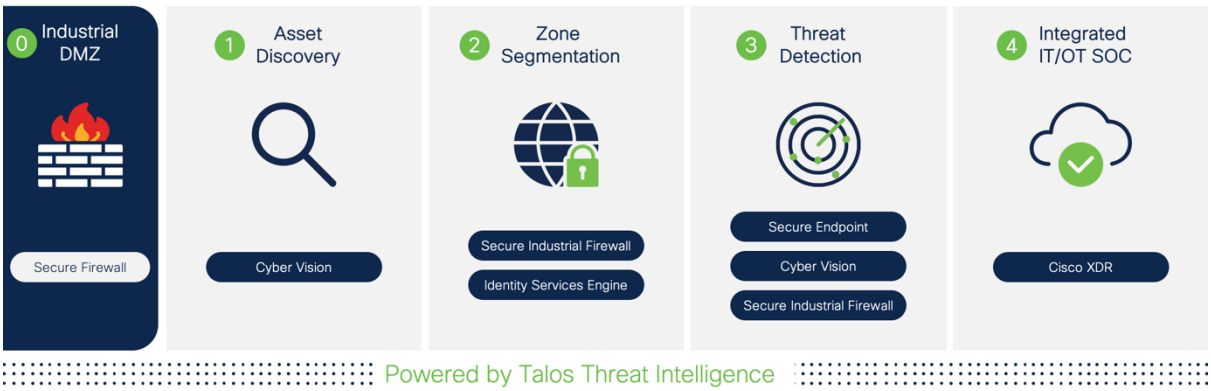

Abbildung 22: Phasenmodell der IT/OT Sicherheit

Industrial DMZ - Industrielle DMZ
Das Industrienetzwerk ist vom Unternehmensnetzwerk durch eine Industrial Demilitarized Zone (IDMZ) getrennt, die von Cisco Secure Firewalls implementiert wird. Es kann auch verwendet werden, um die verschiedenen Teile des Industrienetzwerks zu segmentieren, sodass jedes Segment eine halbautonome Zone bildet, um Sicherheitsvorfälle innerhalb einer Zone zu begrenzen und einzudämmen.

Discover - Asset Discovery - Bewerten Sie Ihre industrielle Cybersicherheitslage
Inventarisieren Sie Ihre OT-Ressourcen und deren Verhalten mit Lösungen, die Ihr Netzwerk als Sensor nutzen, um vollständige Transparenz im großen Maßstab zu bieten und die Erkenntnisse, die Sie zur Reduzierung der Angriffsfläche benötigen. Cisco Cyber Vision bietet eine Knowledge Base mit einem großen Katalog an Industrie Kontrollsystemen und Industrieprotokollen, überwacht deren Kommunikationsverhalten und erkennt Anomalien im OT-Netzwerk.

Segment - Zone Segmentation - Schützen Sie den Betrieb
Setzen Sie ISA/IEC62443-Zonen durch und verhindern Sie die Ausbreitung von Bedrohungen. Entwickeln Sie eine Zero-Trust-Mikrosegmentierungsstrategie mit Cyber Vision, Identity Services Engine und TrustSec bzw. Security Group Tags. Setzen Sie Ihre Secure Firewall und Identity Services Engine für eine gezielte Isolierung und Remediation ein. Mehr zu TrustSec, Software Defined Segmentation erfahren sie hier:

Für eine detailliertere Segmentierung und dynamische Zugriffskontrolle setzt die Cisco Identity Services Engine (ISE) automatisch Sicherheitsrichtlinien auf Geräteebene durch. Es nutzt Zonen, die von OT-MitarbeiterInnen in Cyber Vision konfiguriert wurden, um das Netzwerk anzuweisen, den Kommunikationsfluss entsprechend einzuschränken. Cisco ISE kann auch Aktivitäten von Remote-Benutzern einschränken, die über Cisco Secure Client (einschließlich AnyConnect) VPN-Zugriff auf das Industrienetzwerk erhalten. Cisco Secure Equipment Access ist eine weitere Fernzugriffslösung, die nur einzelnen Geräten Zugriff gewährt. Beide Lösungen können MFA mit Cisco Duo nutzen.

Detect - Threat Detection – Erkennen Sie die Bedrohung
Cisco Cyber Vision warnt Sie vor Hardware- und Software-Schwachstellen, die für jedes OT-Gerät behoben werden müssen, und integriert außerdem eine Snort IDS-Engine zur Erkennung von Eindringlingen und bösartigem Datenverkehr. Dank dieser umfassenden Transparenz der OT-Netzwerkaktivitäten können Sie Baselines erstellen, um Abweichungen vom normalen Verhalten zu erkennen.
Cisco Secure Network Analytics (ehemals Cisco Stealthwatch) hilft auch bei der Erkennung von Anomalien, indem es Telemetriedaten von Netzwerkgeräten sammelt und Netzwerkflüsse überwacht.
Cisco Secure Firewall integriert Cisco Secure IPS, Secure Firewall Malware Defense, erweiterte Distributed DoS (DDoS)-Abwehr und URL-Filterung, um eine umfassende Erkennung und Schutz vor Eindringlingen zu bieten. Es kann auch Talos-Signaturdateien nutzen, um Schwachstellen-Exploits zu blockieren.

Cisco Secure Endpoint bietet erweiterten Malware-Schutz für Ihre verschiedenen Endpunkte (Workstations, Server, Laptops, Tablets usw.) und kann identifizieren, welche Prozesse auf dem geschützten Endpunkt im Netzwerk kommunizieren.
Über die Implementierung von Cisco Identity Services Engine und den Aufbau einer TrustSec Policy Matrix können Sie eine Mikrosegmentierung von Benutzern und Geräten in der IT über 802.1x und in der OT über Security Group Tags bereitstellen.

Alternativ dazu gibt es Cisco Secure Equipment Access, wird über die Cloud bereitgestellt und ermöglicht sicheren Fernzugriff, der in Cisco Netzwerkgeräte integriert ist. Dadurch vermeiden Sie Schatten-IT – und Ihre OT-Teams können Industrieanlagen von überall aus sicher verwalten.

Respond – Integrated IT/OT SOC - Finden und blockieren Sie Bedrohungen in der gesamten IT und OT
Cisco XDR beschleunigt Untersuchungen, indem es Bedrohungsinformationen und Daten aus mehreren Sicherheitstechnologien – Cisco und anderen – in einer einheitlichen Ansicht zusammenfasst. Es optimiert Abhilfemaßnahmen, indem es ein umfassendes Fallmanagement bietet und benutzerdefinierte Playbooks für Ihre spezifische Umgebung ermöglicht.
Cyber Vision und andere Sicherheitstools können Protokollereignisse zur weiteren Untersuchung und Korrelation auf SIEM-Plattformen exportieren.
Mit OT-Einblicken in Ihre IT-Sicherheitstools können Sie Bedrohungen in der gesamten IT und OT erkennen, untersuchen und beheben – alles über eine einzige Konsole, mit Cisco XDR.

Weiterführende Informationen
Cisco Industrial IoT Security
https://www.cisco.com/site/us/en/products/security/industrial-security/index.html
Cisco Industrial Security Validated Design Guide:
https://www.cisco.com/c/en/us/products/collateral/security/industrial-security-cvd-so.html
Security Design Guide für die Industrielle Automatisierung:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/IA_Security/IA_Security_DG/IA_Security_DG.html
NIST Framework und Whitepaper
https://www.cisco.com/c/dam/en/us/products/collateral/security/nist-cybersecurity.pdf

Cisco Cloud Controls Framework

Das Cisco Cloud Controls Framework (CCF) ist das Ergebnis einer Forschung, die darauf abzielt, festzustellen, was erforderlich ist, um SaaS-Produkte für mehrere branchenweit anerkannte Sicherheits-Compliance-Standards zu zertifizieren und Konformität zu erreichen. Das CCF ist eine reine Orientierungshilfe, und jede Organisation muss den Kontrollrahmen überprüfen, bewerten und entsprechend Ihren Anforderungen anpassen und in Ihr eigenes Compliance-System integrieren.

Beschleunigung der SaaS-Produktsicherheitszertifizierungen zur Maximierung des Marktzugangs.
Das (CCF) ist ein umfassender Satz internationaler und nationaler Sicherheits-Compliance- und Zertifizierungsanforderungen, zusammengefasst in einem einzigen Framework. Zusätzlich zur Kontrollzuordnung enthält das CCF auch Anleitungen zur Implementierung und zu Prüfartefakten.
Das Cisco CCF wird aktualisiert, wenn sich die Sicherheits-Compliance-Frameworks und -Vorschriften weiterentwickeln. Um von diesem Rahmenwerk zu profitieren, überprüfen, bewerten und passen Sie es bitte an, um Ihre Compliance-Ziele zu erreichen.

Warum das Cisco Cloud Controls Framework (CCF) anwenden?

Dieses Framework ermöglicht es Ihrem Unternehmen, mit der zunehmenden Komplexität der Markt- und Kundenanforderungen Schritt zu halten. Es bietet einen strukturierten „Build-Once-Use-Many"-Ansatz, der zur Rationalisierung und Operationalisierung der Cloud-Compliance und -Zertifizierung beitragen soll. Das CCF stellt die jahrelange Forschung der Cloud-Compliance-Experten von Cisco dar und kann Ihren Unternehmen dabei helfen, die herausfordernde Compliance-Landschaft besser zu bewältigen und Ihre Marktzugangsziele zu erreichen.

Was bekomme ich mit dem CCF?

Zusätzlich zur Kontrollzuordnung zu jedem der unten genannten Standards stellt das CCF-Kontrollberichte und unterstützende Prüfartefakte für jede Kontrolle im CCF bereit. Diese Ausführungen helfen Ihnen dabei, Hinweise zu Aktivitäten und Maßnahmen zur Implementierung und Durchführung einer Kontrolle zu geben. Die Prüfungsartefakte bieten ein umfassendes Verständnis dessen, was Prüfer normalerweise benötigen, wenn sie die betriebliche Wirksamkeit einer Kontrolle testen. Diese Ausführungen und Artefakte dienen Ihnen als Orientierungshilfe zum Überprüfen, Bewerten und Aktualisieren entsprechend Ihren Geschäftsanforderungen und Ihrer Umgebung.

Warum macht Cisco das CCF öffentlich zugänglich?

Eine starke Cybersicherheit ist für alle gut. Effiziente Wege zur Compliance und Zertifizierung helfen Unternehmen, Risiken schneller zu verstehen und anzugehen. Hoffentlich trägt diese Arbeit dazu bei, sicherere Clouds für alle voranzutreiben.

In CCF abgebildete Standards:

- SOC 2® - SOC for Service Organizations: Trust Services Criteria
- ISO/IEC 27001:2013
  Information technology – Security techniques – Information security management systems – Requirements
- ISO/IEC 27017:2015
  Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2019
  Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27701:2019
  Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines
- ISO 22301:2019
  Security and resilience – Business continuity management systems – Requirements
- Esquema Nacional de Seguridad (ENS)
- Infosec Registered Assessors Program (IRAP December 2021)

- Payment Card Industry Data Security Standard (PCI-DSS v3.2.1)
- Information System Security Management and Assessment Program (ISMAP)
- Cloud Computing Compliance Controls Catalogue (C5)
- EU Cloud Code of Conduct (CoC)
- Third Party Cybersecurity Compliance Certificate (CCC)
- The Federal Risk and Authorization Management Program (FedRAMP LI-SAAS/Tailored)
- National Institute of Standards and Technology (NIST) 800-171
- European Union Cybersecurity Certification Scheme on Cloud Services (EUCS)
- SecNumCloud

Download der CCF Excel-Datei und weiterführende Informationen finden Sie hier:
https://www.cisco.com/c/en/us/about/trust-center/compliance/ccf.html

Cisco Multicloud Defense

Cisco Multicloud Defense schützt die gesamte Datenebene Ihrer Cloud-Umgebungen mithilfe einer einzigen Software-as-a-Service (SaaS)-Steuerungsebene und eliminiert so ineffiziente, komplexe und kostspielige Punktlösungen wie veraltete virtuelle Firewalls in der Cloud oder komplexe Serviceverkettungen (Cloud). native Tools + WAF, DLP usw. von Drittanbietern usw.).
Multicloud-Verteidigung in 4 Ebenen:

1. **Vereinfachen Sie die Multicloud-Sicherheit**: Verwalten Sie die Sicherheit in öffentlichen und privaten Clouds von einem Ort aus. Erstellen, erzwingen und aktualisieren Sie Richtlinien in allen Ihren Clouds in Echtzeit.
2. **Erhalten Sie multidirektionalen Schutz**: Schutz vor Ein- und Austritt sowie Ost-West-Schutz stoppt eingehende Bedrohungen, blockiert Befehls- und Kontrollfunktionen sowie Datenexfiltration und verhindert seitliche Bewegungen.
3. **Erhöhen Sie die betriebliche Effizienz**: Automatisieren Sie zugrunde liegende Cloud-Netzwerkkonstruktionen und integrieren Sie sie in Infrastructure as Code (IaC), um mehr Agilität, Flexibilität und Skalierbarkeit zu erzielen.
4. **Risiken reduzieren, Compliance wahren**: Schließen Sie Sicherheitslücken in Ihrer Cloud-Umgebung proaktiv durch Echtzeit-Asset-Discovery.

Mehr über Cisco Multicloud Defense erfahren Sie hier:
https://www.cisco.com/site/us/en/products/security/multicloud-defense/index.html

6.3.3 Das „Pflichtprogramm“ des Artikel 21 Absatz 2 NIS-2-RL

Welche Vorbereitung zur Erfüllung der NIS- Richtlinie ist notwendig?

Organisatorische Maßnahmen

- Regelmäßige Security Audits
- Sicherheitsüberprüfung durch QuaSte
- Cybersecurity Konzepte
- Verpflichtung zur Übermittlung von Informationen
- Zugriffkontrolle
- Backup-, Notfall-, Krisenmanagement
- Awareness Schulungen

Technische Maßnahmen

- Advanced Threat Protection
- Risikomanagement
- Atack Surface & Vulnerability Management
- Zero Trust Prinzip
- Netzwerk Segmentierung
- Identitäts- und Zugriffsmanagement
- Multifaktor Authentifizierung
- Gesicherte interne Kommunikation

Abbildung 23 Notwendige Organisatorische- und Technische Maßnahmen

Im folgenden Abschnitt sind die in der NIS-2-RL festgelegten 10 Risikomanagement- Maßnahmen aufgezählt und wie Cisco Sie dabei unterstützen kann:

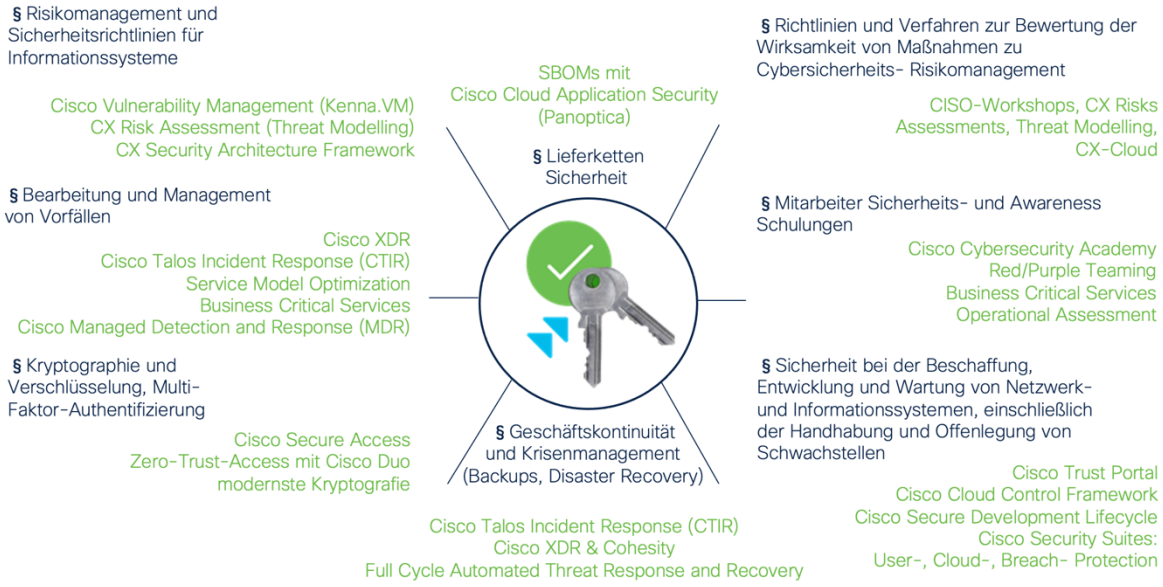

Abbildung 24 Risiko- und Informationssicherheits- Management Maßnahmen

a) „Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme“ (Artikel 21 Absatz 2 littera a NIS-2-RL);

- Risikoanalyse, Risiko Priorisierung mit risikobasierten Vulnerability Management Plattform
  Cisco Vulnerability Management
  https://www.cisco.com/site/us/en/products/security/vulnerability-management/index.html
- Sicherheitsstrategie-, Risiko- und Compliance-Services
  Cisco CX
  https://www.cisco.com/site/de/de/services/index.html

- Beratungsworkshop für CISO – CISO Advisory Workshops
  Cisco CX
  https://www.cisco.com/site/de/de/services/index.html
- Software-Lebenszyklusentwicklung mit Security & Trust Office Abteilung
  Cisco Secure Development Lifecycle
  https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-secure-development-lifecycle.pdf
- Netzwerksicherheit, Implementierung von 802.1x sowie Software Definierte Segmentierung für Benutzer und Geräte
  Cisco TrustSec verwendet Tags, um logische Gruppenprivilegien darzustellen. Dieses Tag, Security Group Tag (SGT) genannt, wird in Zugriffsrichtlinien verwendet. Das SGT ist bekannt und wird zur Durchsetzung des Datenverkehrs durch Cisco-Switches, Router und Firewalls verwendet. Cisco TrustSec ist in drei Phasen definiert: Klassifizierung, Verbreitung und Durchsetzung.
  Cisco Identity Services Engine (ISE)
  https://www.cisco.com/site/us/en/products/security/identity-services-engine/index.html
- Netzwerksegmentierung, Makro-, Mikro-, Nano- Segmentierung
  Cisco Secure Firewall
  https://www.cisco.com/site/us/en/products/security/firewalls/index.html
  Cisco Identity Services Engine (ISE)
  https://www.cisco.com/site/us/en/products/security/identity-services-engine/index.html
  Cisco Platform Exchange Grid (pxGrid)
  https://www.cisco.com/c/en/us/products/security/pxgrid.html
  Cisco Secure Workload
  https://www.cisco.com/site/us/en/products/security/secure-workload/index.html
  SD-Access Segmentation Design Guide
  https://community.cisco.com/t5/networking-knowledge-base/sd-access-segmentation-design-guide/ta-p/4935734
- Identitäts- und Zugriffsmanagement, Zero Trust Framework
  Die Sicherung des Netzwerks durch Sicherstellung der richtigen Benutzer, des richtigen Zugriffs und der richtigen Ressourcen ist die Kernfunktion der Cisco Identity Services Engine (ISE). ISE erstellt Kontext zu Benutzern (Wer), Gerätetyp (Was), Zugriffszeit (Wann), Zugriffsort (Wo), Zugriffstyp (kabelgebunden/kabellos/VPN) (Wie) und den wichtigsten Bedrohungen und Schwachstellen. Alle diese Kontextdaten werden in die Definition logischer Richtliniengruppen, sogenannte Security Group Tags für jeden verbundenen Endpunkt eingespeist. Diese kontextsensitiven Tags werden dann verwendet, um die Grundlage für Sicherheitsrichtlinien zu bilden, zentral auf der ISE verwaltet und in verschiedenen Teilen des Netzwerks auf herkömmliche Weise oder über die Netzwerkstruktur als Teil von Software Defined Access (SD-Access) durchgesetzt zu werden.
  Cisco Duo Security ist stark auf unsere Vision und Strategie für absichtsbasierte Netzwerke abgestimmt und stärkt gleichzeitig unsere bestehenden ISE- und Catalyst Center Funktionen. Wir kombinieren die Zero-Trust-Funktionen für Anwendungen von Duo mit den Zero-Trust-Funktionen für Netzwerke von SD-Access, um die branchenweit einzige umfassende Netzwerk- und Cloud-Zugriffskontrolllösung zu schaffen.
- Netzwerk und Security Design Guides
  https://www.cisco.com/c/en/us/solutions/design-zone/networking-design-guides.html
- Referenz Architekturen für wesentliche und wichtige Infrastruktur
  https://www.cisco.com/c/en/us/solutions/design-zone/industries.html
- Schulungsmaßnahmen u.a. Security Awareness
  https://www.cisco.com/c/en/us/products/collateral/security/email-security/at-a-glance-c45-744492.html
- Cisco Cloud Application Security (Panoptica)
  https://www.panoptica.app
- Cisco Trust Center
  https://www.cisco.com/c/en/us/about/trust-center.html

- Cisco Value Chain Security
  https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-value-chain-security-faqs.pdf
- Cisco Validated Designs
  https://www.cisco.com/c/en/us/solutions/design-zone.html
- Cisco Security Design Guides
  https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/index.html

b) „Bewältigung von Sicherheitsvorfällen“ (Artikel 21 Absatz 2 littera b NIS-2-RL);

- Vorbereitung auf eine Krise und Unterstützung während einer Krise
  Cisco Talos Incident Response – Emergency Response
  https://talosintelligence.com/incident_response/emergency
- Threat modelling, Threat hunting Workshops
  In Zusammenarbeit mit Cisco CX bietet Cisco Talos Threat Modelling und Threat Hunting Workshops an
  https://talosintelligence.com/incident_response/hunting
- Security Operations Center (SOC), Extended Detection and Response (XDR) Software and Services
  Mehr über Cisco XDR erfahren Sie hier:
  https://www.cisco.com/site/de/de/solutions/security/extended-detection-response-xdr/index.html
  Basierend auf Cisco XDR bietet Cisco CX Managed Detection and Response (MDR) Services an, mehr dazu erfahren Sie hier:
  https://www.cisco.com/c/en/us/products/security/service-listing/managed-detection-and-response.html
  Cisco Security Advisories
  https://sec.cloudapps.cisco.com/security/center/home.x
  Respond to a Security Incident
  https://sec.cloudapps.cisco.com/security/center/tacticalresources.x#~RespondingtoaSecurityIncident
  Cisco Talos Incident Response Plans
  https://talosintelligence.com/incident_response/plans

Abbildung 25: Talos Incident Response Retainer Services

c) „Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement“ (Artikel 21 Absatz 2 littera c NIS-2-RL);

- Vorbereitung auf eine Krise und Unterstützung während einer Krise

Cisco Talos Incident Response Playbooks
https://talosintelligence.com/incident_response/playbooks

- Wiederherstellung der Infrastruktur nach einem Notfall
  Cisco Talos Incident Response – Emergency Response
  https://talosintelligence.com/incident_response/emergency
  Mit Cisco XDR und Cohesity können Sie Ihre Infrastruktur- und Unternehmensdatensicherung durchführen, sowie eine aktuelle Wiederherstellung und schnelle automatisierte Reaktionen gewährleisten.
  Mehr über die Zusammenarbeit mit Cohesity lesen Sie hier:
  https://blogs.cisco.com/security/from-risk-to-resilience-ransomware-recovery-with-cisco-xdr-and-cohesity

d) „Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern“ (Artikel 21 Absatz 2 littera d NIS-2-RL);

- Software-Inventarliste, Software Bill of Material (SBOM) erstellen
  Wie Sie mit Cisco Cloud Application Security (Panoptica) eine SBOM erstellen können erfahren Sie hier: https://www.panoptica.app/blog/what-is-an-sbom-software-bill-of-materials
- Partnerschaft mit Ihrer Security & Trust Office Abteilung

e) „Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen“ (Artikel 21 Absatz 2 littera e NIS-2-RL);

- Bereitstellung von Dokumenten zu Sicherheit, Vertrauen, Datenschutz und Privatsphäre, einschließlich ISO-, SOC-Zertifizierungen und Compliance-Dokumente.
  Im Cisco Trust Portal finden Sie dazu alle Informationen zu unseren Lösungen:
  https://trustportal.cisco.com/c/r/ctp/home.html
- Schwachstellenforschung, Malware Erkennungs- und Präventionssysteme
  Die Cisco Talos Intelligence Group ist eines der größten kommerziellen Threat-Intelligence-Teams der Welt und besteht aus erstklassigen Forschern, Analysten und Ingenieuren. Diese Teams werden durch konkurrenzlose Telemetrie und hochentwickelte Systeme unterstützt, um genaue, schnelle und umsetzbare Bedrohungsinformationen für Cisco-Kunden, -Produkte und -Dienste zu erstellen. Talos verteidigt Cisco-Kunden vor bekannten und neu auftretenden Bedrohungen, entdeckt neue Schwachstellen in gängiger Software und fängt Bedrohungen im Umlauf ab, bevor sie dem Internet insgesamt weiteren Schaden zufügen können. Talos unterhält die offiziellen Regelsätze von Snort.org, ClamAV und SpamCop und veröffentlicht darüber hinaus zahlreiche Open-Source-Recherche- und Analysetools.
  Mehr zu Cisco Talos erfahren Sie hier:
  https://www.talosintelligence.com/
  Cisco Cloud Application Security (Panoptica) ist eine Cloud Native Sicherheitsplattform, die zum Schutz der Kubernetes-Orchestrierungsumgebung und Container, Microservices, APIs, serverlosen Funktionen und der Software-Lieferkette entwickelt wurde. Es vereinfacht die Aufgabe, den Entwicklungslebenszyklus Ihrer Cloud-nativen Anwendung umfassend zu sichern – von Build-Pipelines bis hin zu Workload-Laufzeiten, die in einer oder mehreren Clouds ausgeführt werden.
  Mehr über Cisco Cloud Application Security (Panoptica) erfahren Sie hier:
  https://www.panoptica.app
  Mehr über Cisco Full-Stack Observability (FSO) erfahren Sie hier:
  https://www.cisco.com/site/us/en/solutions/full-stack-observability/index.html
  Cisco Secure Malware Analytics (ehemals Threat Grid) kombiniert fortschrittliches Sandboxing mit Bedrohungsinformationen in einer einheitlichen Lösung, um Unternehmen vor Malware zu schützen. Mit einer robusten, kontextreichen Malware-Wissensdatenbank verstehen Sie, was Malware tut oder zu tun versucht, wie groß die Bedrohung ist und wie Sie sich dagegen wehren können.
  Mehr über Cisco Secure Malware Analytics erfahren Sie hier:
  https://www.cisco.com/c/en/us/products/security/threat-grid/index.html
  Cisco Policies and Processes
  https://sec.cloudapps.cisco.com/security/center/securityResources.x

Network Design Considerations for Security
https://sec.cloudapps.cisco.com/security/center/tacticalresources.x#~NetworkDesignConsiderationsforSecurity
Running a secure network
https://sec.cloudapps.cisco.com/security/center/tacticalresources.x#~RunningaSecureNetwork
Cisco Security Tools

- Cisco Software Checker
- Cisco Vulnerability Repository
- Bug Search
- Cisco PSIRT openVuln API
- CVRF Repository
- OVAL Repository

f) „Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit“ (Artikel 21 Absatz 2 littera f NIS-2-RL);

- Risikoanalyse, Risiko Priorisierung mit risikobasierten Vulnerability Management
  Cisco Vulnerability Management bietet Ihnen die Kontextinformationen und die Threat-Intelligence, die Sie benötigen, um drohende Exploits frühzeitig zu stoppen und präzise zu reagieren.
  Mehr über Cisco Vulnerability Management (ehemals Kenna.VM) erfahren Sie hier:
  https://www.cisco.com/site/de/de/products/security/vulnerability-management/index.html
- Sicherheitsstrategie-, Risiko- und Compliance-Services
  Stärken Sie Ihren Sicherheitsstatus: Erweitern und optimieren Sie Ihre IT-Sicherheit unter Wahrung der Compliance. Schützen und verteidigen Sie Ihr Netzwerk mit einem proaktiven Ansatz, um Sicherheitsrisiken mindern zu können, bevor sie zum Problem werden.
  Vereinfachen Sie Ihre IT-Sicherheitsverfahren: Durch integrierte führende Automatisierungslösungen können Sie Bedrohungen transparent erkennen und sich entsprechend besser schützen. Kombinieren Sie automatisierte Prozesse mit dem Know-how unserer SicherheitsexpertInnen, um die Bedrohungstransparenz zu verbessern und rund um die Uhr auf Bedrohungen reagieren zu können.
  Mehr über Cisco Security Services (CX) erfahren Sie hier:
  https://www.cisco.com/site/de/de/products/security/services/index.html

g) „Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit“ (Artikel 21 Absatz 2 littera g NIS-2-RL);

- Vorbereitung auf eine Krise und Unterstützung während einer Krise
  Cisco Talos Incident-Response als führende Cyber Security Organisation hilft Ihnen, Security Resilience zu erlangen und Sie bei Bedarf zu unterstützen.
  Mehr über Cisco Talos erfahren Sie hier:
  https://www.cisco.com/site/us/en/products/security/talos/index.html
- Threat modelling workshops
  Cisco CX bietet Ihnen maßgeschneiderte Threat modelling Workshops für Ihr Unternehmen an.
  Mehr über die Services von Cisco CX erfahren Sie hier:
  https://www.cisco.com/site/de/de/products/security/services/index.html
- Schulungsmaßnahmen u.a. Security Awareness
  Cybersicherheits-Einsatzteams stehen an vorderster Front beim Schutz und bei der Abwehr von Cyberangriffen. Aber Cybersicherheitsbedrohungen scheinen sich von Tag zu Tag schneller zu entwickeln. Das Cisco Certified CyberOps Schulungs- und Zertifizierungsprogramm vermittelt Ihnen das Wissen, die Fähigkeiten und die praktische Praxis, die Sie zum Schutz der digitalen Vermögenswerte Ihres Unternehmens benötigen. Cisco Cybersecurity Awareness Trainings helfen die Resilienz des Unternehmens gegen Cyberattacken zu stärken.
  Mehr über das Cisco Certified CyberOps Certifications und Trainings Programm erfahren Sie hier:
  https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/cyberops.html
  Mehr über die Cisco Cybersecurity Awareness erfahren Sie hier:
  https://www.cisco.com/c/de_de/products/security/national-cybersecurity-awareness-month.html

h) „Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung“ (Artikel 21 Absatz 2 littera h NIS-2-RL);

- Verschlüsselung auf allen Ebenen des ISO/OSI Referenzmodells
  Mit Cisco Secure Firewall ist es einfach und kostengünstig, Zero Trust in Ihrer IT-Umgebung zu implementieren. Damit schaffen Sie ein System, in dem nichts als vertrauenswürdig eingestuft wird, bis es verifiziert ist. Automatisieren Sie den Zugriff, und antizipieren Sie potenzielle Sicherheitsbedrohungen. Ein sicherer Zugriff über VPN ist nur der Anfang. Ihre Teams brauchen einen problemlosen Zugang zu Unternehmensressourcen und privaten Apps. Die Sicherheit Ihres Unternehmens sollte dabei oberste Priorität haben. Cisco Secure Access macht genau dies möglich. Schützen Sie Ihre hybride Belegschaft mit agiler Cloud-Security. Security Service Edge (SSE) ist eine Cloud-basierte Lösung, die auf Zero Trust aufbaut, benutzerfreundlich ist und sicheren standortunabhängigen Zugriff ermöglicht. Cisco Secure Client nutzt das leistungsstarke, branchenführende AnyConnect-VPN/ZTNA und unterstützt IT- und SicherheitsexpertInnen beim Management dynamischer und skalierbarer Agents für die Sicherheit von Endpunkten – und all das in einer einheitlichen Ansicht.
  Mehr über Cisco Secure Firewall erfahren Sie hier:
  https://www.cisco.com/site/de/de/products/security/firewalls/index.html
  Mehr über Cisco Secure Access erfahren Sie hier:
  https://www.cisco.com/site/de/de/products/security/secure-access/index.html
  Mehr über Cisco Secure Client erfahren Sie hier:
  https://www.cisco.com/site/de/de/products/security/secure-client/index.html
- Verschlüsselung in Lösungen zur gesicherten Sprach-, Video- und Textkommunikation
  Cisco Unified Communications Manager (CUCM) unterstützt die neuesten Protokolle für Authentifizierung, Verschlüsselung und Kommunikation. Es erfüllt wichtige Branchenzertifizierungen und sichert Daten sowie die Kommunikation für Kunden in den Bereichen Finanzwesen, Fertigung, Einzelhandel und für Behörden auf der ganzen Welt.
  Mehr über CUCM erfahren Sie hier:
  https://www.cisco.com/c/de_de/products/unified-communications/unified-communications-manager-callmanager/index.html

i) „Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen“ (Artikel 21 Absatz 2 littera i NIS-2-RL);

- Lösungen zu Video- Aufzeichnungen (CCTV) und deren Analyse
  Revolutionäre Überwachung dank intelligenter Cloud-Managed Kameras für erhöhte Sicherheit und mehr Einblicke. Durch die Speicherung und Verarbeitung in der jeweiligen intelligenten Kamera entfällt die Komplexität, die separate Speicher, Server und Management mit sich bringen.
  Sichere Anzeige von Videos überall und auf beliebigen Geräten – ohne Konfiguration und ohne zu installierende Software oder Plug-ins. Integrierter Datenschutz und Sicherheit, mit eindeutigen Benutzerkonten und standardmäßig verschlüsselten Daten auf jedem Schritt des Weges.
  Mehr über Cisco Meraki Überwachungskameras erfahren Sie hier:
  https://meraki.cisco.com/de-de/products/smart-cameras/
- Lösungen zur Unterstützung des AAA-Frameworks (Authentifizierung, Autorisierung und Accounting)
  Mit Cisco Identity Services Engine (ISE) erfassen und kontrollieren Sie Geräte und BenutzerInnen in Ihrem Netzwerk. Nutzen Sie Informationen aus Ihrem gesamten Stack, um Richtlinien durchzusetzen, Endpunkte zu managen und vertrauenswürdigen Zugriff zu ermöglichen. Multicloud-NAC mit Zero Trust macht es möglich.
  Mehr über Cisco ISE erfahren Sie hier:
  https://www.cisco.com/site/de/de/products/security/identity-services-engine/index.html
- Lösungen zu gesicherten Remote Zugriff auf OT-Equipment
  Sichern Sie den Fernzugriff auf Ihre ICS- und OT-Ressourcen und setzen Sie mit unserer Zero Trust Network Access (ZTNA)-Lösung, die für industrielle Netzwerke und raue Umgebungen entwickelt wurde.
  Mehr über Cisco Secure Equipment Access erfahren Sie hier:
  https://www.cisco.com/site/us/en/products/security/industrial-security/secure-equipment-access/index.html

j) „Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung“ (Artikel 21 Absatz 2 littera j NIS-2-RL).

- Multifaktor Lösungen für Authentifizierung nach dem Zero Trust Prinzip
  Cisco Duo ist die benutzerfreundliche „Zero Trust“ Sicherheitsplattform von Cisco, die Unternehmen jeder Größe umfassenden, skalierbaren Schutz vertraulicher und sensibler Daten für alle Benutzer, Geräte und Anwendungen bietet.
  Mehr dazu erfahren Sie hier: https://duo.com/de/duo-overview

- Lösungen zur Zusammenarbeit für eine gesicherte Sprach- Video- und Textkommunikation
  Cisco Unified Communication und Collaboration (CUCM) ist ein führender und innovativer Anbieter von Technologien und Lösungen für Kommunikationssysteme verschiedener Ausprägungen. Um unseren Partnern und Kunden einen Leitfaden zum Design und die dazu empfohlenen Einstellungen von verschiedenen Kollaborationslösungen zu bieten, hat Cisco so genannte „Preferred Architectures“ (PAs) für die folgenden Szenarien entwickelt und getestet:
  - On-premise – Alle Kollaborationsdienste werden im Rechenzentrum des Kunden bereitgestellt und verwaltet.
  - Hybrid – Einige Kollaborationsdienste werden lokal betrieben, während andere in der Cloud gehostet werden.
  - Cloud-Bereitstellung – Alle Kollaborationsdienste werden in der Cloud bereitgestellt und verwaltet.

  Cisco Preferred Architectures (PAs) wurden für bestimmte Marktsegmente basierend auf gängigen Anwendungsfällen entwickelt. Sie umfassen einen Teil der Produktpalette des Cisco Collaboration-Portfolios. Die Auswahl dieser Produkte erfolgte auf Grund des vorgegebenen Marktsegments und der der definierten Anwendungsfälle. Hierbei wurde auch auf größtmögliche Skalierbarkeit und Flexibilität geachtet, damit die Architektur schnell an neue Geschäftsanforderungen angepasst werden kann.

  Ein wichtiger Teil der Preferred Architecturs (PAs) ist auch die Absicherung der Lösung nach verschiedenen Gesichtspunkten. Dazu gehören unter anderem:
  - Eine Absicherung der Kollaborationslösung in Schichten – beginnend von der physischen Zugangskontrolle zu den Rechenzentren, über die Netzwerksegmentierung bis hin zu rollen-basierten Administratoren bei den einzelnen Systemkomponenten.
  - Eine spezielle Absicherung von Kommunikationslösungen wie Telefonie erfordert auch das Verhindern der Erreichbarkeit von unerwünschten Mehrwertnummern, die einerseits zu hohen Kosten, andererseits auch zur Belegung von Ressourcen wie SIP Trunks führen können.
  - Sobald mit der Außenwelt kommuniziert werden soll, sollten auch hier die eingesetzten Komponenten nach den Cisco Vorgaben konfiguriert und abgesichert werden.

  Weitere Informationen zu diesem Thema befinden sich im „Security“ Kapitel des „Cisco Collaboration 14 Enterprise for On-Premises Deployments“ Dokuments unter https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/enterprise/14/collbcvd/security.html#pgfId-1080263.

  Neben der Verschlüsselung und Absicherung gegen Angreifer von außen ist für Kommunikationssysteme die Verfügbarkeit der Lösung auch im Fall von (technischen) Ausfällen eine wichtige Komponente. Hierfür bietet Cisco mehrere Möglichkeiten – beispielsweise Clustering von mehreren Servern, was speziell für große Standorte eine empfohlene Lösung ist. Für kleinere Standorte sorgt SRST (survivable remote site telephony) dafür, dass selbst im Fall von Kommunikationsausfällen des Firmennetzes noch ohne großen Verlust von Features über das lokale Gateway telefoniert werden kann. Für hochsichere Anforderungen wie Notfallleitungen im Krisenfall können mit Hilfe von analogen Gateways Verbindungen ins Festnetz hergestellt werden, die selbst bei einem Totalausfall der lokalen Stromversorgung noch zur Verfügung stehen.

Da viele Kunden auf Grund von Kosten die Auslagerung von Video- und Webkonferenzlösungen in die Cloud forcieren, stellt sich auch hier die Frage der Sicherheit. Cisco Webex bietet eine geeignete Plattform, um sowohl Standardmeetings als auch Meetings mit einer höheren Sicherheitsstufe entsprechend absichern zu können. Die Verschlüsselung erfolgt dabei mit 256 Bit – im Fall von so genannten „Zero Trust Meetings" findet der Austausch dieser Schlüssel direkt zwischen den Teilnehmern statt, sodass es Cisco technisch nicht möglich ist, Zugriff auf die Inhalte (Audio, Video, Bildschirmfreigabe) eines Meetings zu erlangen. Weitere Informationen zur Sicherheit von Webex Meetings finden sich unter https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html.

Collaboration Preferred Architectures
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/design/guides/PAdocs.html
Cisco Webex Trust Center
https://www.cisco.com/c/en/us/about/trust-center/webex.html
Webex Meetings Security Whitepaper
https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html
Securing Internet Telephony Media with SRTP and SDP
https://sec.cloudapps.cisco.com/security/center/resources/securing_voip.html

- Lösungen für die Sicherheit in der E-Mail-Kommunikation, Domain Protection, Antimalware-, Antiphishing Lösungen
  Cisco Secure Email umfasst erweiterte Funktionen zum Schutz vor Bedrohungen, um Bedrohungen schneller zu erkennen, zu blockieren und zu beheben, Datenverluste zu verhindern und wichtige Informationen während der Übertragung mit End-to-End-Verschlüsselung zu sichern.
  Mit Cisco Secure Email können Kunden:
  - Erkennen und blockieren Sie mehr Bedrohungen mit erstklassigen Bedrohungsinformationen von Cisco Talos, unserem Bedrohungsforschungsteam.
  - Bekämpfen Sie Ransomware, die in Anhängen versteckt ist und sich der Ersterkennung entzieht, mit Cisco Secure Email Threat Defense.
  - Löschen Sie E-Mails mit riskanten Links automatisch oder blockieren Sie den Zugriff auf neu infizierte Websites mit Echtzeit-URL-Analyse zum Schutz vor Phishing und BEC.
  - Verhindern Sie Markenmissbrauch und raffinierte identitätsbasierte E-Mail-Angriffe mit den Diensten Cisco Secure Email Domain Protection und Cisco Secure Email Threat Defense.
  - Schützen Sie sensible Inhalte in ausgehenden E-Mails mit Data Loss Prevention (DLP) und benutzerfreundlicher E-Mail-Verschlüsselung – alles in einer Lösung.
  - Bieten Sie Benutzerverhaltensschulungen mit Cisco Secure Awareness Training an, damit Benutzer intelligenter und sicherer arbeiten können.
  - Maximieren Sie die Bereitstellungsflexibilität mit einer Cloud-, virtuellen, lokalen oder hybriden Bereitstellung oder wechseln Sie phasenweise in die Cloud.
  - Integrieren Sie eine wachsende Anzahl von Cisco-Sicherheitsprodukten und beschleunigen Sie wichtige Sicherheitsbetriebsfunktionen wie Sichtbarkeit, Erkennung, Automatisierung, Untersuchung und Behebung mit Cisco XDR.

  Mehr zu Cisco Secure Email erfahren Sie hier:
  https://www.cisco.com/site/us/en/products/security/secure-email/index.html

Zusammenfassend zu den „Big 10“ Maßnahmen in der NIS-2 Richtlinie nachfolgend eine Übersicht zur technischen Umsetzung mit Cisco:

NIS-2 Richtlinie “Big 10” Maßnahmen	Technische Umsetzung mit Cisco					
a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme	ISMS, InfoSec Pentest (CX) ISO 27001	GAP-A (CX)	EDR (Secure Endpoint) XDR/MDR Awareness (CX)	NAC (ISE) MFA (DUO)	Secure FW VPN (Secure Client)	Web Sec (Umbrella) (Secure Email)
b) Bewältigung von Sicherheitsvorfällen	IR (Talos)	SOC (XDR/MDR)	EDR (Secure Endpoint) XDR/MDR	BMS (Cyber Vision)		
c) Aufrechterhaltung des Betriebs, Wiederherstellung nach einem Notfall und Krisenmanagement	IR (Talos)	SOC (XDR/MDR)	Backup / Restore (Cohesity)	BMS (Cyber Vision)	Notfall-HB (CX)	
d) Sicherheit der Lieferkette, sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen. ihren unmittelbaren Anbietern oder Diensteanbietern	Zertifikate ISO 27000	SBOM (Cloud Application Security)	Jumphost (Secure Equipment Access)	VPN (Secure Client)	MFA (DUO)	
e) Sicherheitsmaßnahmen von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen	ISMS, InfoSec IR (Talos)	XDR/MDR	EDR (Secure Endpoint) XDR/MDR	NAC (ISE) MFA (DUO)	Secure FW VPN (Secure Client)	Web Sec (Umbrella) (Secure Email)
f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit	ISMS, InfoSec Pentest (CX) ISO 27000	GAP-A (CX)	(Vulnerability Management)			
g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit	Pentest (CX)	GAP-A (CX)	Awareness (CX)			
h) Konzepte und Verfahren fur den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung	FW (Secure Firewall) VPN (Secure Client)	ZTNA (Secure Access)	Web Sec (Umbrella)	Data Encryption (Webex)	Data Loss Prevention (CloudLock)	
i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen	GAP-A (CX)	Awareness (CX)	MFA (DUO)	NAC (ISE)	Asset Visibility (Cyber Vision)	ZTNA (Secure Equipment Access)
j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.	MFA (DUO)	NAC (ISE)	ZTNA (Secure Access)	Email (Secure Email)	Voice, Video (CUCM, SRST)	Messaging, Calling (Webex)

Abbildung 26 Big 10 Maßnahmen und technische Umsetzung

NIS-2-RL Umsetzung anhand der Cisco Security Referenz Architektur

Im folgenden Abschnitt werden die Referenzarchitekturen zu den Einrichtungen im Sinne der Anhänge I und II der NIS-2-RL zugeordnet:

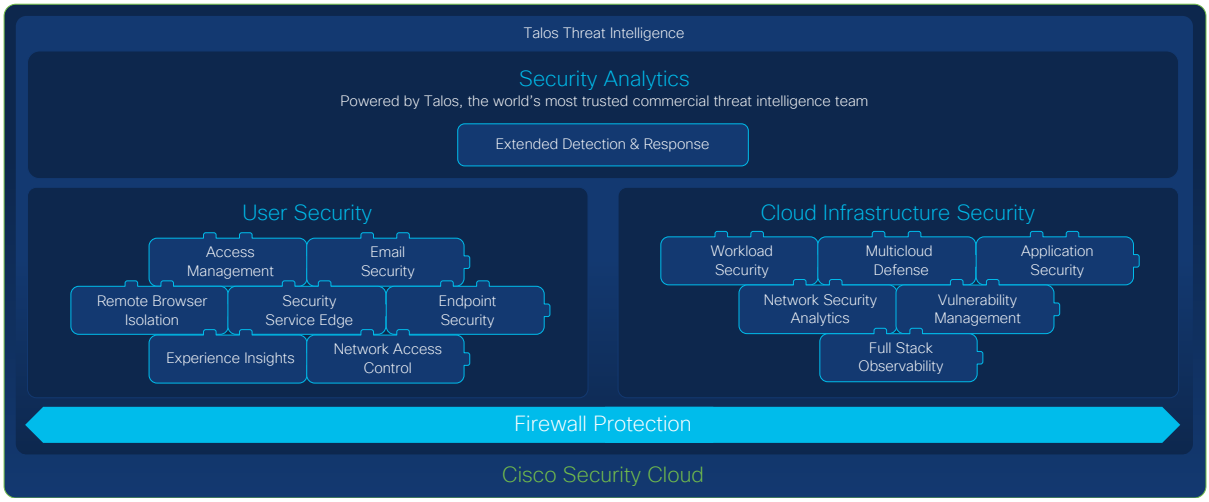

Abbildung 27: Cisco Security Portfolio

Die Cisco Security Reference Architecture bietet einen Überblick über das Cisco Secure-Portfolio, häufig eingesetzte Anwendungsfälle und die empfohlenen Funktionen innerhalb einer integrierten Architektur. Die Referenzarchitektur ist auf Domänen ausgerichtet, die eng an Branchensicherheits-Frameworks wie NIST, CISA und DISA ausgerichtet sind.

Nachfolgend sind die fünf Hauptkomponenten der Referenzarchitektur aufgeführt:

1. Bedrohungsinformationen
2. Toolset für Security Operations
3. Benutzer-/Gerätesicherheit
4. Netzwerksicherheit: Cloud-Edge und On-Premises
5. Workload-, Anwendungs- und Datensicherheit

Jede Organisation verfügt über eine einzigartige Umgebung, die auf den Geschäftsanforderungen basiert. Nur weil die Referenzarchitektur bestimmte Funktionen umfasst, heißt das nicht, dass Ihre Umgebung dies auch tun muss. Darüber hinaus werden in den meisten Fällen mehrere aufgeführte Funktionen in einem einzigen Produkt instanziiert, um den Betrieb zu vereinfachen.

Wir empfehlen Ihnen, sich mit Ihrem Cisco Account-Team in Verbindung zu setzen und Ihre Sicherheitsreise zu planen.

Abbildung 28: Cisco Security Reference Architecture

Die obige Übersicht umfasst mehrere häufig eingesetzte Anwendungsfälle wie Zero Trust, SASE und XDR. Auf hoher Ebene ist Talos die wichtigste Grundkomponente, die Bedrohungsinformationen und Malware-Analysen für die gesamte Architektur bereitstellt. Talos bietet umsetzbare Bedrohungsinformationen sowie Malware-Forschung und -Analysen, die eine durchgängige Bedrohungsprävention in Echtzeit im gesamten Netzwerk ermöglichen. Talos liefert dynamische Bedrohungsinformationen über IP- und Domänenreputation, SNORT-Signaturen, Analyse und Kontrolle bösartiger Dateien sowie URL-Kategorisierung an die Cisco-Sicherheitsplattform und sorgt so für umsetzbare Informationsdurchsetzung im Endpunkt, in der Firewall, in E-Mails und Web-Gateways.

Zero Trust umfasst die SASE-Schicht und alles darin, da Zero Trust eine Methodik ist, die die gesamte Architektur umfasst und nicht ein einzelnes Produkt oder mehrere einzelne Produkte. Zero Trust besteht aus mehreren Anforderungen, die für Benutzer und Geräte durchgesetzt werden können, die den Cloud-Edge oder lokale Netzwerke nutzen, wenn sie auf Arbeitslasten mit Anwendungen und Daten zugreifen. Die Schicht unterhalb von Zero Trust ist SASE. SASE beschreibt eine Architektur zur Sicherung von Remote-Mitarbeitern und Cloud-Edge-Netzwerken wie Remote-Büros oder Zweigstellen. Die Benutzer-/Gerätesicherheitskomponente bietet die notwendigen Funktionen, um über den neuen einheitlichen Secure Client einen sicheren und einfachen Benutzerzugriff zu ermöglichen. Wenn Benutzer/Geräte auf Workloads, Anwendungen und Daten zugreifen (unten im Diagramm), können zwei mögliche Pfade (Cloud- oder lokaler Zugriff) gewählt werden. Jeder Zugriff auf öffentliche SaaS-Anwendungen oder das Internet würde über das Cloud-Edge-Netzwerk erfolgen, in dem Cloud-Sicherheitsdienste durchgeführt würden. Der andere Zugriffspfad auf Workloads/Anwendungen/Daten wäre der lokale Zugriff, bei dem herkömmliche lokale Sicherheitsdienste zum Einsatz kommen würden.

Die jeweils aktuellste Cisco Security Reference Architecture finden Sie hier:
https://www.cisco.com/c/en/us/products/security/cisco-security-reference-architecture.html

Weitere Einzelheiten finden Sie in den folgenden Anwendungsfällen:

Anwendungsfall: gemeinsame Identität

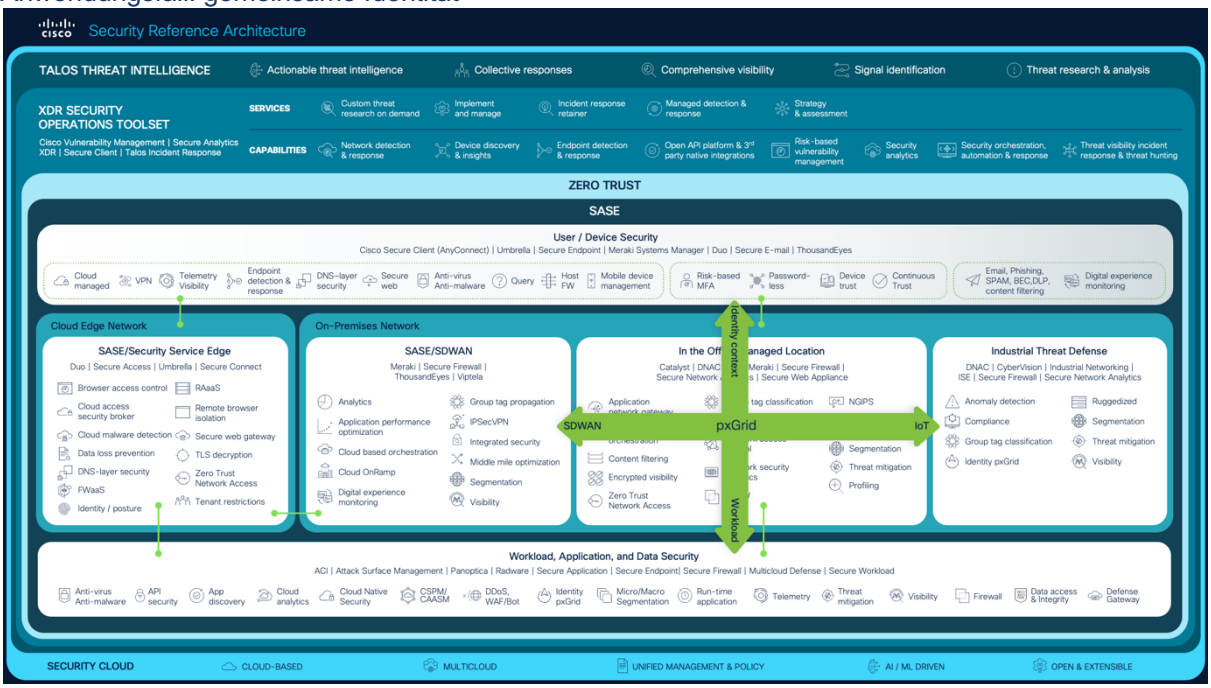

Abbildung 29: Common Identity

Cisco pxGrid erleichtert die gemeinsame Nutzung von Benutzer-/Gerätekontexten im gesamten Netzwerk und in der Anwendungssicherheitskomponente von Zero Trust für Workloads für hybride private/öffentliche Clouds wie AWS, Azure und GCP. Die Identitätsfreigabe mit Cisco Umbrella unter Cloud Edge ist ab sofort über AD/LDAP-Konnektoren verfügbar, um die Identität vor Ort im Rahmen der Richtlinienkontrolle von Umbrella auf die Umbrella-Cloud auszudehnen. Die Ausweitung der Identität auf Umbrella mithilfe von pxGrid wird in Zukunft eine Option sein und es Umbrella-Kunden ermöglichen, ihre Cloud-Zugriffsrichtlinien mit mehr Kontextdetails zu erweitern. Viele Fortune-1000-Kunden nutzen pxGrid und nutzen es, um pxGrid-Ökosystemlösungen von Drittanbietern in ihre Identitäts- und Zugriffsbereitstellungen zu integrieren.

Anwendungsfall: konvergente Multicloud-Richtlinie

Abbildung 30: Unified Access Policy

Eine konvergente Multicloud-Richtlinie kann stufenweise erstellt und verwaltet werden, angefangen bei Anwendungs-Workloads bis hin zu den Endpunkten. Viele Kunden fordern eine Synchronisierung der Workload- und Rechenzentrums-Perimeterrichtlinien, um die Firewall-Richtlinienverwaltung im Allgemeinen zu verbessern. Beispielsweise kann eine umfassende sichere Workload-Richtlinie mit den Richtlinien der AWS VPC Network Security Group synchronisiert werden, auf denen EC2-Agenten und serverlose Apps ausgeführt werden. Über die Grenzen des Rechenzentrums hinaus kann die Workload-Richtlinien-Engine mit Netzwerk-Firewalls synchronisiert werden, um die betriebliche Effizienz zu verbessern. Dies erfordert eine weitere Prüfung und Planung der Netzwerkrichtlinien, da die Zusammenführung mehrerer Firewall-Ebenen komplex ist. Dieses Konzept einer konvergenten Multicloud-Richtlinien-Engine ist heute verfügbar und wird auf der Grundlage häufig eingesetzter Kundenanwendungsfälle weiterentwickelt und verbessert.

Anwendungsfall: SASE-Integrationen

Abbildung 31: SASE Integration

Die Cisco SASE-Lösung über Cisco Umbrella bietet Bedrohungsschutz und sicheren Zugriff überall dort, wo sich der Benutzer befindet – zu Hause, im örtlichen Café, in der Zentrale oder im Regionalbüro. Durch die Kombination mit SD-WAN wird sichergestellt, dass die entsprechende Zugriffsrichtlinie angewendet wird, ohne dass der Benutzer entscheiden muss, wie er eine sichere Verbindung herstellt. Mit der Auto-Tunnel-Funktion der Cisco SASE-Lösung – beispielsweise unter Verwendung von Viptela vManage, Meraki oder Firepower – können Kunden problemlos Tausende sicherer IP-Tunnel mit wenigen Klicks und API-Schlüsseleingaben erstellen. Mithilfe der Secure Internet Gateway (SIG)-Funktionen von Umbrella können Kunden Sicherheitsfunktionen wie DNS-Sicherheit, Snort IPS, cloudbasierte Firewall, Remote-Browser-Isolation, CASB, Malware-Inspektion und mehr nutzen. Diese erweiterten Sicherheits- und Bereitstellungsfunktionen reduzieren menschliches Versagen bei groß angelegten Bereitstellungen und tragen dazu bei, kontextreiche Richtlinien zu ermöglichen, die unbefugten Zugriff eindämmen.

Anwendungsfall: Zero-Trust-Netzwerkzugriff (ZTNA)

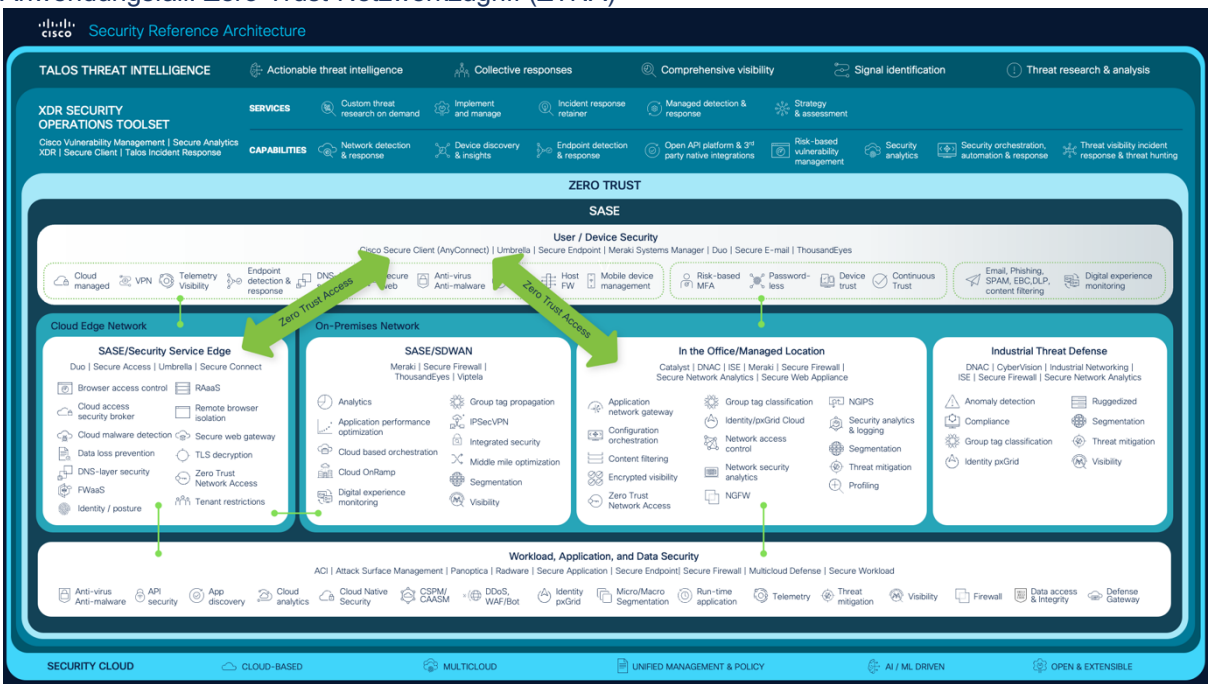

Abbildung 32: Zero Trust Access

Die Cisco Zero Trust-Lösung bietet Benutzer- und Anwendungssicherheit in der gesamten Architektur. Sowohl persönliche Bring-Your-Own-Device (BYOD) als auch vom Unternehmen ausgegebene Geräte werden einem adaptiven Multi-Faktor-Authentifizierungsprozess (risikobasierte Authentifizierung) unterzogen und erhalten den am wenigsten privilegierten Zugriff mit kontinuierlicher Vertrauensüberwachung. Der Anwendungszugriff wird dynamisch widerrufen oder autorisiert, wenn sich der Status des Benutzers/Geräts ändert. Mit dem Managed Zero Trust Network Access (ZTNA) von Umbrella können Kunden die Fernzugriffsverwaltung auf Cisco Managed Services verlagern und schnell Zero Trust Services für den Schutz öffentlicher und privater Anwendungen bereitstellen. Selbstverwaltete ZTNA-Kunden können weiterhin AnyConnect VPN-Dienste bereitstellen oder Duos Cloud Single Sign-On (SSO) und Duo Network Gateway für nicht VPN-basierten Anwendungszugriff nutzen. Das passwortlose SSO von Duo verbessert und vereinfacht die Anmeldeerfahrung der Benutzer.

Anwendungsfall: XDR-Telemetrie und Orchestrierung

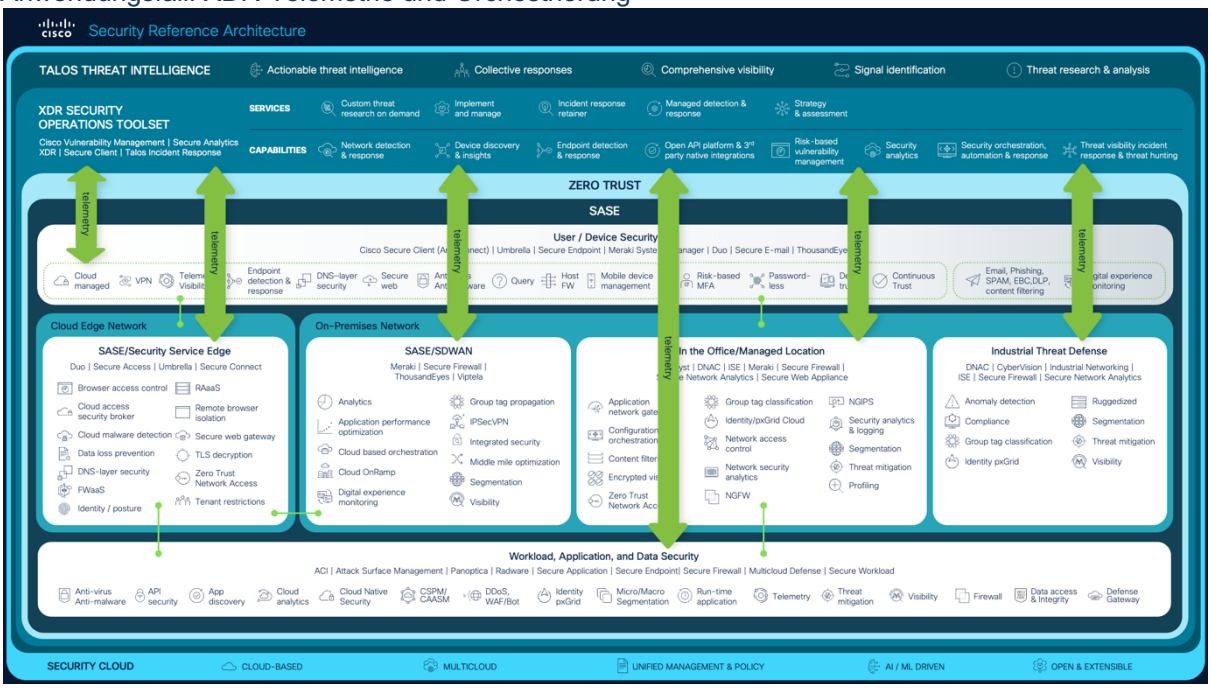

Abbildung 33: Extended Detection and Response XDR

Die Cisco XDR-Plattform bietet Transparenz, priorisierte Untersuchung/Reaktion von Vorfällen auf Basis von KI/ML und Orchestrierung mit Kontext- und Bedrohungsdatenaustausch zur Unterstützung von SecOps. Endpunktgeräteinformationen (von der Mobilgeräteverwaltung über Endpunktsicherheitssoftware wie Duo Device Health, Cisco Secure Clients und EDR-Lösungen auch von Drittanbietern) können für eine vollständige Bestandsaufnahme und Compliance-Validierung an Cisco XDR Insights gesendet werden. Cisco Die offenen und flexiblen API-Funktionen von Cisco XDR verbessern die Bedrohungswirksamkeit durch Integrationen von Drittanbietern weiter. Somit verbessert Cisco XDR wirklich die Art und Weise, wie Sicherheitsabläufe die Erkennung und Reaktion im Alltag unterstützen.

7. Das Sanktionsregime der NIS-2-RL

Siehe White Paper „Die NIS-2-RL und ihre Anforderungen an Unternehmen“ Schiefer Rechtsanwälte GmbH

8. Ausblick auf die innerstaatliche Umsetzung (NISG-Novelle und Vollzugspraxis)

Siehe White Paper „Die NIS-2-RL und ihre Anforderungen an Unternehmen“ Schiefer Rechtsanwälte GmbH

9. NIS-2-Implementierung: DSGVO-Erfahrungen nutzen

Siehe White Paper „Die NIS-2-RL und ihre Anforderungen an Unternehmen“ Schiefer Rechtsanwälte GmbH

ABBILDUNGSVERZEICHNIS

QUELLENVERZEICHNIS

ISO. (2016). *ISO 27799:2016*. Retrieved from https://www.iso.org/standard/62777.html

ISO. (2022). Retrieved from https://www.iso.org/standard/75652.html

WKO. (2023, 7 10). *Cybersicherheits-Richtlinie NIS2*. Retrieved from https://www.wko.at/service/innovation-technologie-digitalisierung/nis2-uebersicht.html

A-SIT. (24. März 2017). *onlinesicherheit.gv.at*. Von ISO/ IEC 27001 – Anforderungen an Informationssicherheits-Managementsysteme: https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Normen-und-

Standards/ISO-IEC-27000/ISO-IEC-27001-Informationssicherheits-Managementsysteme-ISMS.html abgerufen