Was ist NIS2?

!

Es ist die umfassendste europäische Cybersicherheitsrichtlinie.

Mit strengere Anforderungen für Risikomanagement und Incident Reporting, breitere Abdeckung von Sektoren,
und harte Strafen für Nichtkonformität → Hunderttausende Unternehmen und Einrichtungen müssen ihre Cybersicherheitsposition neu bewerten.

Frei verwendbar| © Siemens 2024 | NIS2 Cyber Security| Scherer | Januar 2024
SIEMENS

Die NIS-2-Richtlinie der EU[1]
Überblick

Zielsetzung	• **Hohes gemeinsames Cybersicherheitsniveau in der EU** und reibungsloses Funktionieren des Binnenmarkts • Neufassung der NIS1[1] – die erste und zugleich wichtigste Richtlinie der EU-weiten Cybersicherheitsgesetzgebung
Schwerpunkt	Regeln für die Sicherheit von **Netz- und Informationssystemen**
Zielgruppe	**Alle 27 EU-Länder**, Island, Liechtenstein, Norwegen und UK (=MS)
Inkrafttreten	Spätestens zum 18. Oktober 2024
Minimale Harmonisierung	**MS verabschiedet möglicherweise strengere Cybersicherheitsvorschriften bzw. hält solche Vorschriften aufrecht** – Vorausgesetzt, dass diese Vorschriften mit den Vorgaben von EU-Gesetzen konform sind

1 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union [**N**etzwerk- und **I**nformations**S**icherheitsrichtlinie (NIS)].

Unrestricted | © Siemens 2024 | NIS2 CRA Sondersession SEA DACH | Scheider | Januar 2024

Einrichtungen

Wesentliche Einrichtungen

Bußgelder:

Geldbußen von Behörden für die Nichteinhaltung von **Risikomanagementmaßnahmen** bzw. **Berichts-pflichten im Bereich der Cybersicherheit**

€10 M oder 2%
des globalen Jahresumsatzes

Vor-Ort-Kontrollen und externe Aufsichtsmaßnahmen, einschließlich Stichprobenkontrollen und regelmäßiger Audits

Weitere Informationen →

Wichtige Einrichtungen

Bußgelder:

Geldbußen von Behörden für die Nichteinhaltung von **Risikomanagementmaßnahmen** bzw. **Berichts-pflichten im Bereich der Cybersicherheit**

€7 M oder 1,4%
des globalen Jahresumsatzes

Vor-Ort-Kontrollen und externe nachträgliche Aufsichtsmaßnahmen

SIEMENS

Verantwortlichkeiten des Managements

Die **Mitglieder des Managements**
können für Schäden persönlich haftbar gemacht werden

Das **Top-Management** wesentlicher bzw. wichtiger Einrichtungen muss das **Cybersecurity-Risikomanagement genehmigen**, die **Einhaltung relevanter Vorgaben prüfen,** und **wird bei Nicht-einhaltung zur Rechenschaft gezogen**.

Die Mitglieder des Managements müssen routinemäßig spezielle Schulungen absolvieren und sich auf diese Weise ein ausreichendes Niveau an Fachwissen aneignen bzw. auf dem neuesten Stand bleiben, um Cybersicherheitsrisiken zu verstehen, ein angemessenes Sicherheitsmanagement umzusetzen und sich über Auswirkungen auf die Abläufe und Ergebnisse der Organisation bewusst zu sein.

Unrestricted | © Siemens 2024 | NIS2 CRA Sondersession SEA DACH | Scheider | Januar 2024
SIEMENS

Wesentliche Einrichtungen[1]

Große Einrichtungen

Energie (Strom, Fernwärme und Kühlung, Öl, Gas, Wasserstoff)

Transport (Luft, Schiene, Wasser, Straße)

Bankwesen

Finanzmarkt-Infrastrukturen

NEU

Gesundheit einschl. Herstellung **pharmazeutischer** Produkte wie z.B. Impfstoffe

Trinkwasser

Abwasser NEU

NEU

Digitale Infrastruktur

NEU

Luft- und Raumfahrt

1 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555&from=EN#d1e32-143-1

Frei verwendbar| © Siemens 2024 | NIS2 Cyber Security| Scherer | Januar 2024

SIEMENS

Wichtige Einrichtungen[1]

Mittelgroße Einrichtungen

Energie (Strom, Fernwärme und Kühlung, Öl, Gas, Wasserstoff)

Transport (Luft, Schiene, Wasser, Straße)

Bankwesen

Finanzmarkt-Infrastrukturen

NEU

Gesundheitswesen einschließlich Herstellung **pharmazeutischer** Produkte wie z.B. Impfstoffe

Trinkwasser

NEU

Abwasser

NEU

Digitale Infrastruktur

NEU

Luft- und Raumfahrt

1 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555&from=EN#d1e32-143-1

Frei verwendbar| © Siemens 2024 | NIS2 Cyber Security| Scherer | Januar 2024

SIEMENS

Wichtige Einrichtungen[1]

Mittelgroße Einrichtungen

Große Einrichtungen

NEU Post- und Kurierdienste

Abfallmanagement NEU

NEU **Chemie**

NEU

Herstellung, Verarbeitung und Verteilung von **Nahrungsmitteln**

Herstellung von **medizinischen Geräten**, Rechnern, elektronischen Geräten, Maschinenausrüstung und **Kraftfahrzeugen** NEU

NEU Forschung

Digitalanbieter

1 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555&from=EN#d1e32-143-1

SIEMENS

NIS 2-Direktive - Sektoren

11 Sektoren mit hoher Kritikalität

- **Energie** (Strom, Öl, Gas, Wärme, Wasserstoff)
- **Gesundheit** (Versorger, Labore, F&E, Pharma)
- **Transport** (Luft, Schiene, Wasser, Straße)
- **Banken**
- **Finanzmärkte**
- **Wasser**
- **Abwasser**
- **Digital Infrastruktur**
- **ICT-Dienstleistungsverwaltung**
- **Raumfahrt**
- **Öffentliche Verwaltung**

7 sonstige kritische Sektoren

- **Post und Kurier**
- **Abfallwirtschaft**
- **Chemie**
- **Ernährung**
- **Forschung**
- **Digitale Dienste**
  - Online-Marktplätzen
  - Online-Suchmaschinen
  - Soziale Netzwerke
- **Verarbeitendes Gewerbe**
  - **Medizinprodukte**
  - **DV-Geräte, elektr./optische Erzeugnisse**
  - **Elektronische Ausrüstung**
  - **Maschinenbau**
  - **PKW/PKW-Teile**
  - **Sonstiger Fahrzeugbau**

Frei verwendbar | © Siemens 2024 | DI Horizontal Cybersecurity

SIEMENS

Art. 21 Abs. 2 NIS-2: Katalog der Mindestsicherheitsanforderungen

Wesentliche und **wichtige** Einrichtungen müssen **geeignete** und **verhältnismäßige technische, operative** und **organisatorische Maßnahmen** ergreifen:

- Konzepte für **Risikoanalyse**
- Konzepte für **Security von IT-Systemen**
- Bewältigung von Sicherheitsvorfällen **(Incident Handling)**
- **Business Continuity Management**
- Backup-management
- Disaster recovery
- Krisenmanage ment
- **Security in der Lieferkette**
- Security Maßnahmen bei Erwerb, Entwicklung und Wartung von Netz- IT-Systemen
- Inkl. Vulnerability Management / Disclosure
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von **Risikomanagement-maßnahmen** im Bereich der Cybersicherheit
- **Cyberhygiene** Verfahren und Cybersecurity **Schulungen**
- Konzepte und Verfahren für Einsatz von Kryptographie
- Sicherheit des Personals
- Konzepte für die Zugriffskontrolle und Management von Anlagen
- Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung
- Gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

SIEMENS

NIS-2 Umsetzung in Deutschland

NIS2UmsuCG: Entwurf

Frei verwendbar | © Siemens 2024 | DI Horizontal Cybersecurity

SIEMENS

Sind Sie vom NIS2UmsuCG* betroffen?

(*aktueller Entwurf zur NIS-2 Umsetzung: Stand Dez. 2023)

SIEMENS

NIS2UmsuCG – Betrifft es unser Unternehmen?

A

Ihr Unternehmen ist bereits durch das IT-Sig 2.0 als **KRITIS Betreiber** zu Cybersecurity Maßnahmen verpflichtet

o
d
e
r

B

In Ihrem Unternehmen sind **mindestens 50 Mitarbeitende** angestellt.

In Ihrem Unternehmen erwirtschaftet einen **Jahresumsatz** von **über 10 Mio. Euro.**

Ihr Unternehmen ist in einem kritischen Sektor tätig.

- **11 Sektoren von hoher Kritikalität**

- **Energie** (Strom, Öl, Gas, Wärme, Wasserstoff)
- **Gesundheit** (Versorger, Labore, F&E, Pharma)
- **Transport** (Luft, Schiene, Wasser, Straße)
- **Banken**
- **Finanzmärkte**
- **Wasser**
- **Abwasser**
- **Digital Infrastruktur**
- **ICT-Dienstleistungsverwaltung**
- **Raumfahrt**
- **Öffentliche Verwaltung**

- **7 sonstige kritische Sektoren**

- **Post und Kurier**
- **Abfallwirtschaft**
- **Chemie**
- **Ernährung**
- **Verarbeitendes Gewerbe**
  - Medizinprodukte
  - DV-Geräte, elektr./optische Erzeugnisse
  - Elektronische Ausrüstung
  - Maschinenbau
  - PKW/PKW-Teile
  - Sonstiger Fahrzeugbau
- **Digitale Dienste** (Online-Marktplätzen, Online-Suchmaschinen, sozialer Netzwerke)
- **Forschung**

NIS2UmsuCG adressiert ihr Unternehmen

C

Sonderfälle

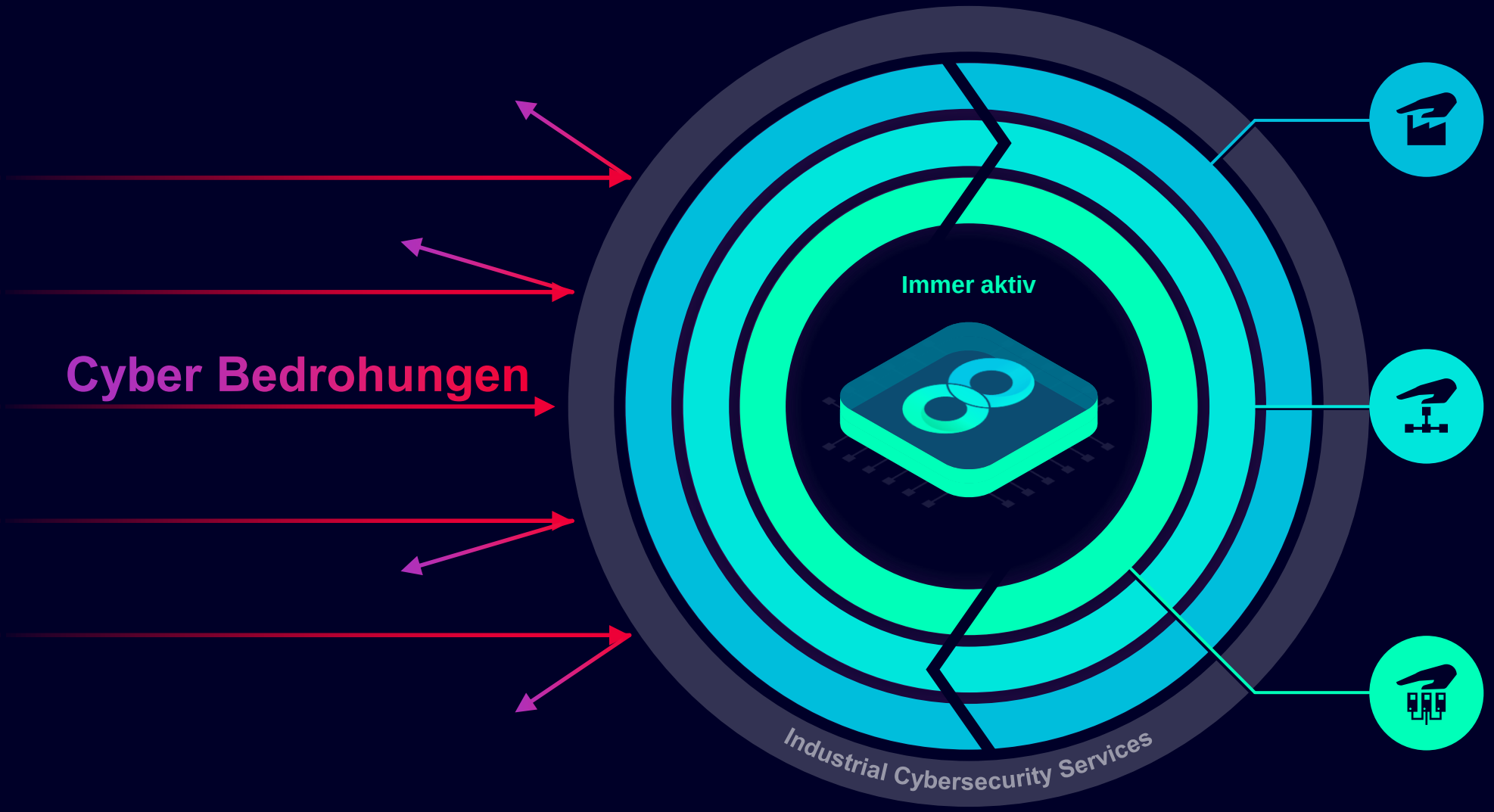
Frei verwendbar | © Siemens 2024 | DI Horizontal Cybersecurity

SIEMENS

Erfüllung liegt beim KRITIS Betreiber.
ABER
Unterstützung von Siemens

SIEMENS

Der Defense-in-Depth Ansatz der IEC 62443 ist die Basis unseres mehrschichtigen Cybersecurity Ansatzes



Plant Security

- Physischer Schutz
- Security Policies
- Security Monitoring

Netzwerk Security

- Netzwerksegmentierung
- Firewalls und Industrial DMZ
- Fernwartungslösungen
- Zero Trust

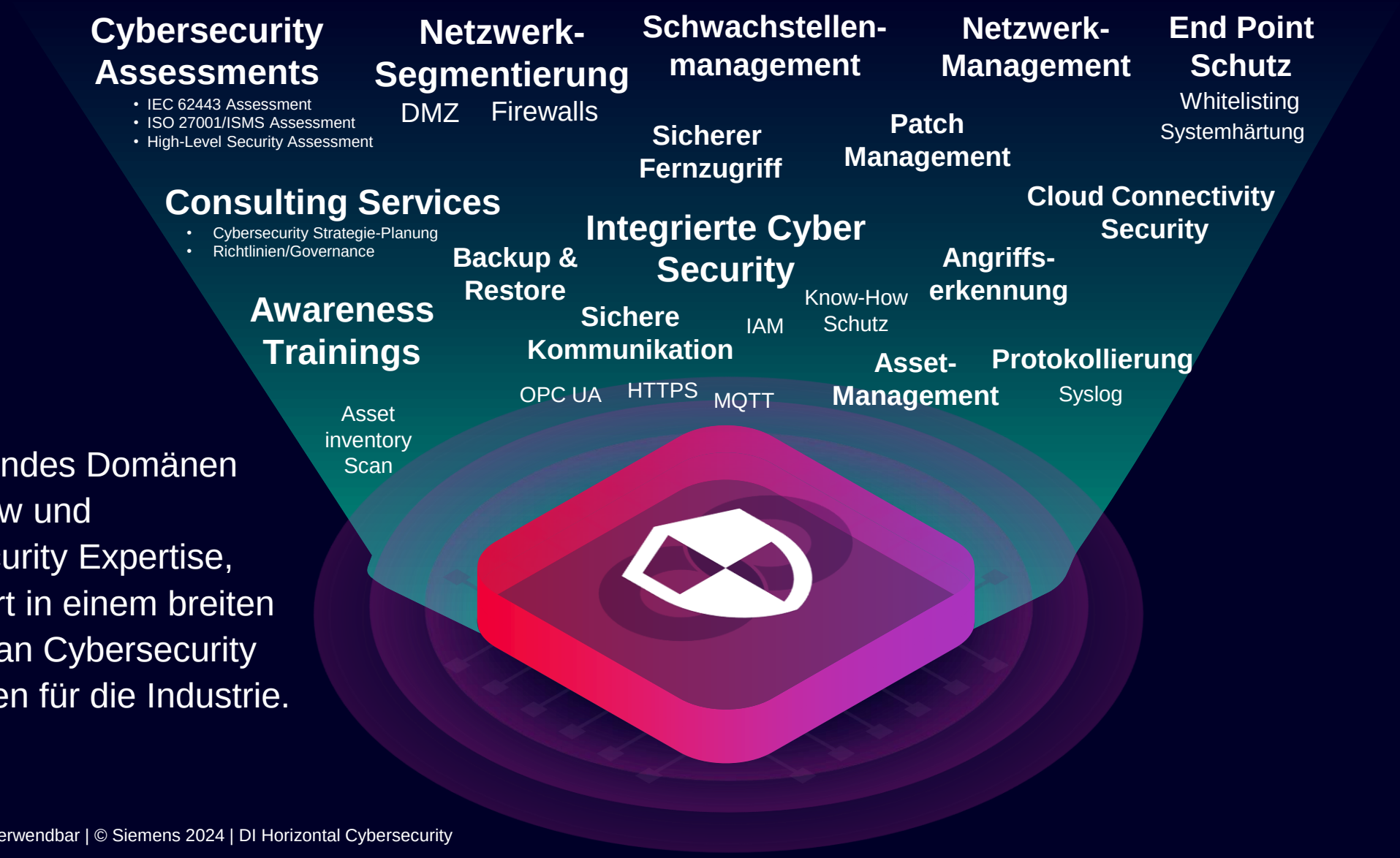
System Integrität

- Systemhärtung
- Patch Management
- Authentifizierung und Zugriffsschutz

Frei verwendbar | © Siemens 2024 | DI Horizontal Cybersecurity

SIEMENS

Cybersecurity Bausteine zur Unterstützung bei der NIS-2 Umsetzung



Tiefgreifendes Domänen Know-How und Cybersecurity Expertise, kombiniert in einem breiten Angebot an Cybersecurity Bausteinen für die Industrie.

Frei verwendbar | © Siemens 2024 | DI Horizontal Cybersecurity

SIEMENS

Wie unterstützt Sie Siemens bei Ihren Anforderungen an die Cybersecurity?

frei verwendbar | © Siemens 2023 | DI Horizontal Cybersecurity

SIEMENS

Siemens ist Ihr verlässlicher Partner für Cybersecurity bei der Digitalisierung Ihrer OT.

Tiefgreifende OT-Cybersecurity Wissen
Durch viele Jahre Erfahrung in eigenen Werken

Breites Portfolio
Hardware, Software und integrierte Security-Elemente

Proaktives Handeln
Mit unserem Cyber Emergency Response Team (CERT)

Umfassende Services
für Anlagen- und Netzwerksicherheit und Systemintegrität

SIEMENS

Zusammen mit starken Partnern hat Siemens eine „Charter of Trust“ unterzeichnet

Mit folgenden drei Zielen

01 Daten von Einzelpersonen und Unternehmen schützen

02 Schäden von Menschen, Unternehmen und Infrastrukturen abwenden

03 Verlässliches Fundament schaffen, auf dem in einer vernetzten, digitalen Welt aufgebaut werden

Eine gemeinsame Initiative für eine sichere digitale Welt

Charter of Trust

charteroftrust.com

SIEMENS

Siemens Webinar Reihe zum Thema Cybersecurity

- Webinar-Reihe zum Thema Cybersecurity im Automatisierungsumfeld
- Fokus auf ganzheitlichen Cybersecurity Ansatz
- Zielgruppe: technisch interessierte Kunden mit Fokus OT/IT

Warum? Wieso? Weshalb? Rechtliches und Normen

- Regulatorische und rechtliche Vorgaben (IT-SiG 2.0, NIS-2)
- Ganzheitlicher Ansatz nach Defense in Depth
- OT-Cybersecurity Normen (IEC 62443)

Datum:
28.02.2024

Die 3 Bausteine einer sicheren Netzwerkstruktur

- Aufbau einer sicheren Anlage nach der IEC 62443
- Sichere Trennung von IT und OT
- Sicheres Ausschleusen von Daten aus dem OT-Umfeld

Datum:
10.04.2024

Härtungsmaßnahmen u. Benutzerverwaltung meistern

- Härtungsmaßnahmen innerhalb der System- und Netzwerkumgebung im Automatisierungsumfeld
- Einsatz einer durchgängigen Benutzerverwaltung

Datum:
15.05.2024

Schwachstellen-management u. Erkennen v. Angreiferaktivitäten

- Ganzheitliches und vollständiges Logging innerhalb einer OT-Anlage
- Schwachstellenmonitoring
- Angriffserkennung innerhalb einer Automatisierungsanlage

Datum:
12.06.2024

Registrierung | Webinarreihe Erfolgreich mit Industrial Cybersecurity (invitario.com)

Wissen kompakt – Make it secure mit TIA Portal V19 - Siemens Deutschland

SIEMENS

DIE UHR TICKT ...

SIEMENS

Disclaimer

© Siemens 2024

Änderungen und Irrtümer vorbehalten. Die Informationen in diesem Dokument enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, welche im konkreten Anwendungsfall nicht immer in der beschriebenen Form zutreffen bzw. welche sich durch Weiterentwicklung der Produkte ändern können. Die gewünschten Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart werden.

Alle Produktbezeichnungen können Marken oder sonstige Rechte der Siemens AG, ihrer verbundenen Unternehmen oder dritter Gesellschaften sein, deren Benutzung durch Dritte für ihre eigenen Zwecke die Rechte der jeweiligen Inhaber verletzen kann.

SIEMENS

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Herausgeber: Siemens AG

Gernot Scherer
Planerbetreuer W/WW
Siemens Deutschland
Digital Industries
Promotion 2 for FA 2
RC-DE DI FA 2 PROM2
Gateway Gardens
De-Saint-Exupéry-Str. 5
60549 Frankfurt am Main, Deutschland
Mobil: +49 (173) 6760973
mailto:gernot.scherer@siemens.com

SIEMENS