3. Zukunftsforum Burgenland

Cybersecurity – Voraussetzung für den Einsatz von AI

09.04.2026

SIEMENS

Diese Veranstaltung ist KEINE Rechtsberatung

Überprüfen Sie unbedingt die konkreten Auswirkungen auf Ihr Unternehmen gemeinsam mit Ihrer Rechtsabteilung!

SIEMENS

Warum ist Cybersecurity keine Option ?

Produkte werden immer komplexer

Früher

Autos zum Beispiel bestanden aus mechanischen und elektrischen Komponenten und es gab nur eine Art von Motor: Verbrennungsmotoren.

Heute

Autos sind komplexe mechatronische Systeme. Sie sind computergesteuerte Systeme von Systemen, die von einer Vielzahl von Motoren angetrieben werden.

SIEMENS

Die Entwicklung von Produkten wird immer komplexer

Früher

Die Produkte wurden für den einmaligen Gebrauch entwickelt und es gab wenig bis gar keine Vorschriften für die Reparierbarkeit oder das Recycling.

Heute

Unternehmen müssen Vorschriften berücksichtigen, die die Kreislaufwirtschaft fördern, und Produkte so gestalten, dass sie wiederverwendbar, abbaubar und recycelbar sind.

Die Nutzung von Produkten wir immer komplexer

Früher

One size fits all –
ein Medikament für alle Patienten.

Heute

Personalisierte Medizin, einschließlich aller relevanten Daten wie persönliche und operative Daten, Kundenfeedback, Dokumentation, Tracking und Tracing.

SIEMENS

Die Produktion wird immer komplexer

Früher

Große Chemieanlagen produzierten jahrzehntelang mit minimalen Änderungen.

Heute

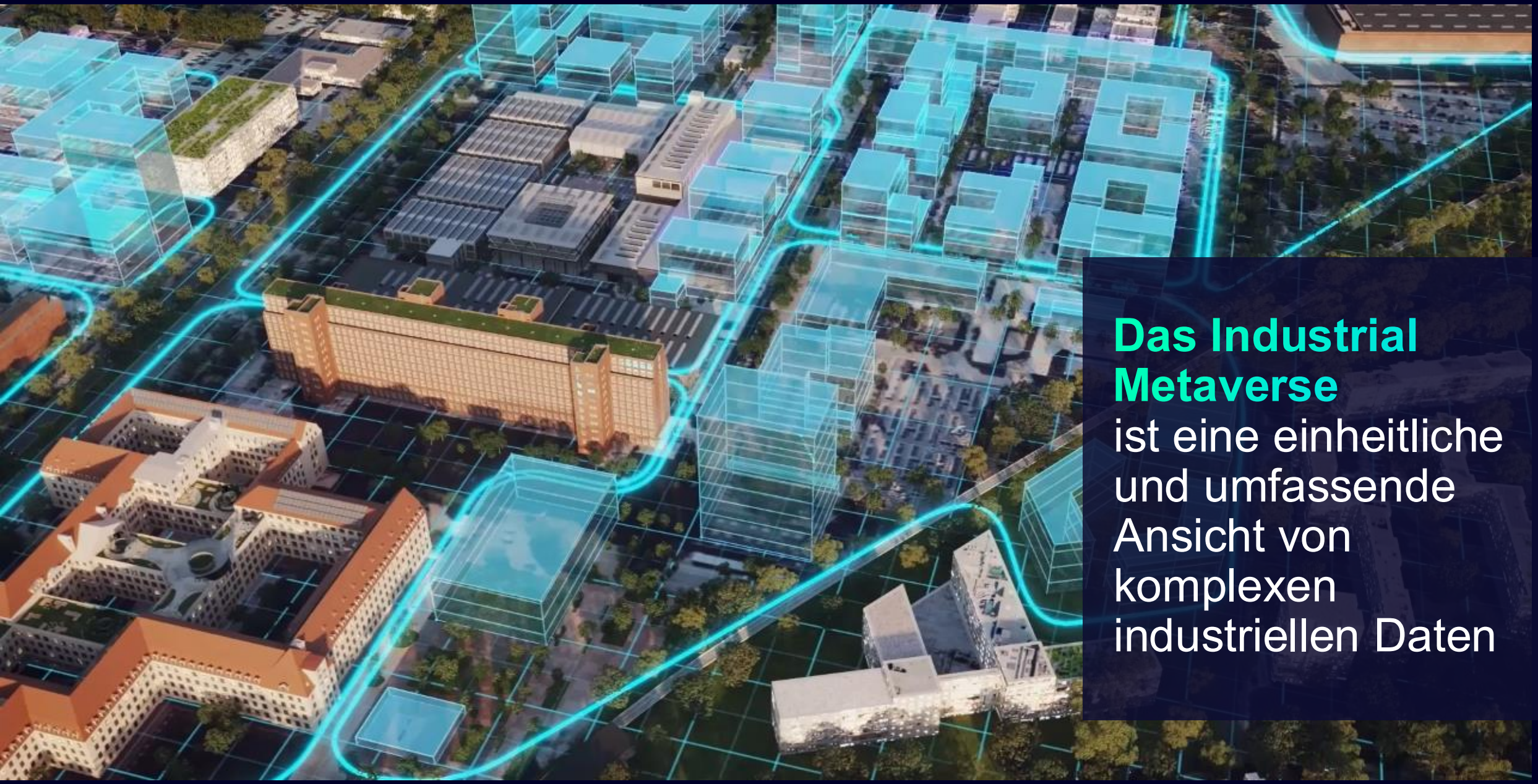
Hohe Nachfrage nach Modernisierung und flexibler und **nachhaltiger** Produktion.

SIEMENS

Unser Antrieb leitet uns seit mehr als 175 Jahren:

We create technology **to transform the everyday, for everyone.**

SIEMENS



Das Industrial Metaverse
ist eine einheitliche und umfassende Ansicht von komplexen industriellen Daten

SIEMENS

Die technologischen Kernelemente
vom Industrial Metaverse

Industrial Metaverse

Digital Twin

Artificial Intelligence

IT-OT-Integration

Industrial Cybersecurity

SIEMENS

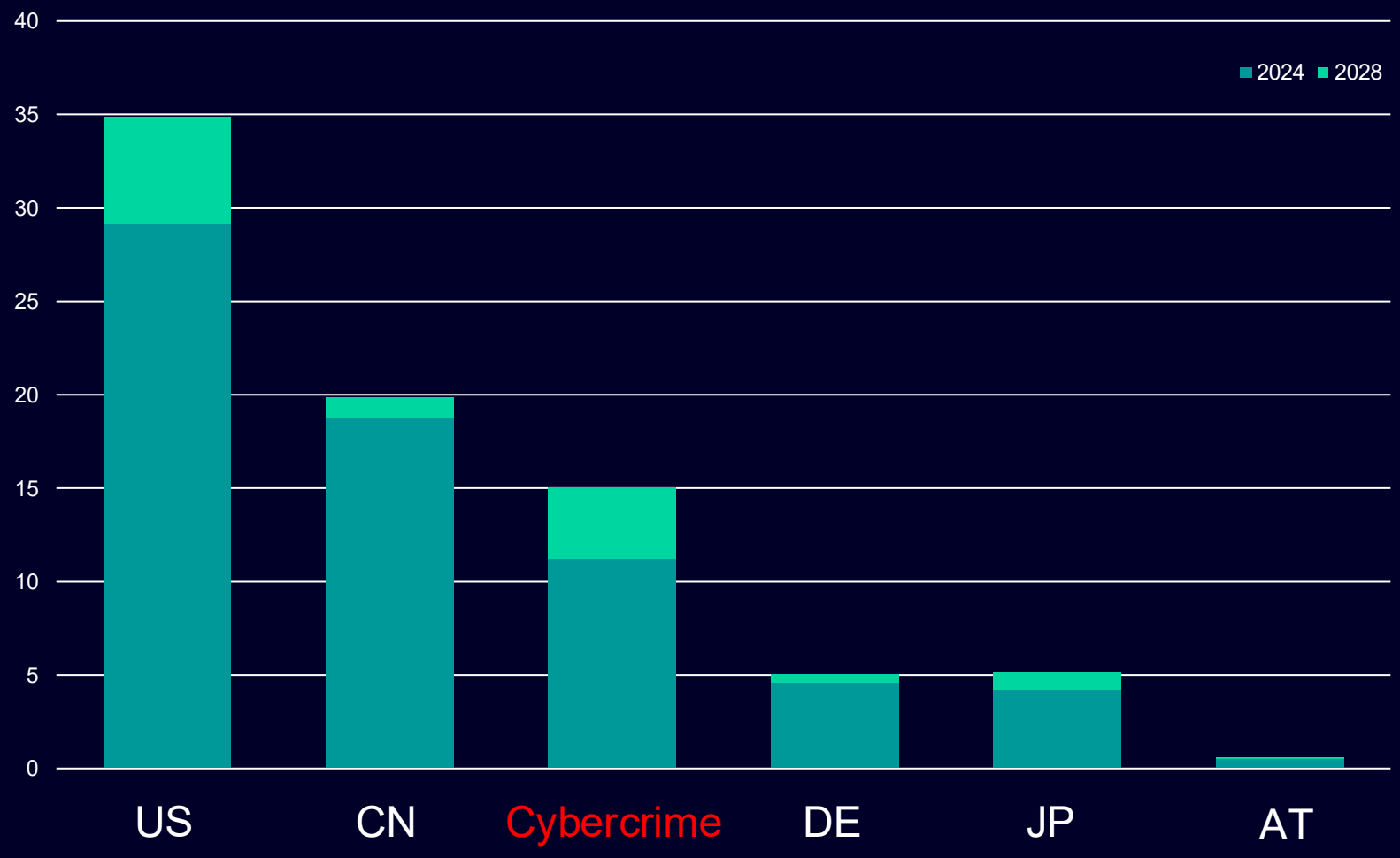
Die technologischen Kernelemente
vom Industrial Metaverse

Industrial Metaverse

Industrial Cybersecurity

SIEMENS

Bruttoinlandsprodukt in Billionen US$



Gefährdungen existieren,
Risiken kann man managen!

SIEMENS

Risikoanalyse (mit Illustrationen)

Risiko

Extremes Risiko

Eine Person betritt den Käfig und füttert den Löwen

Wahrscheinlichkeit	4
Auswirkung	4
Wahrscheinlichkeit x Auswirkung	16

Hohes Risiko

Eine Person mit Schutzausrüstung betritt den Käfig und füttert den Löwen

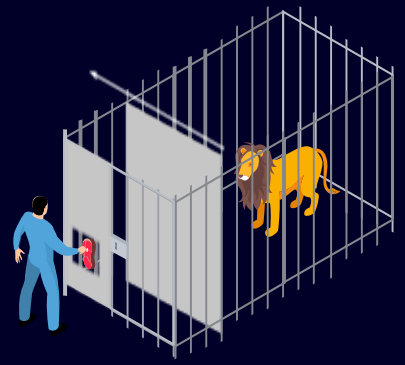
Wahrscheinlichkeit	
Auswirkung	
Wahrscheinlichkeit x Auswirkung	

Tolerierbares Risiko

Eine Person füttert den Löwen durch eine speziell entwickelte Futteröffnung

Wahrscheinlichkeit	2
Auswirkung	2
Wahrscheinlichkeit x Auswirkung	4

imales Risiko



e Person füttert den Löwen inem speziell konstruierten terkäfig

hrscheinlichkeit	1
swirkung	1
hrscheinlichkeit x swirkung	1

Kosten

SIEMENS

Security by law?

SIEMENS

Unterschied Richtlinie / Verordnung / Gesetz

EU – Directive (Richtlinie)

- Verbindlich bezüglich der Ziele, lässt den Staaten Freiheit, wie sie diese umsetzen
- Muss in nationales Recht umgesetzt werden (nat. Gesetz/Verordnung)
- Frist zur Umsetzung (meist 2 Jahre)

EU – Regulation (Verordnung)

- Verbindlich in allen Teilen
- Gilt **sofort** und unmittelbar in allen EU-Mitgliedstaaten
- Ist wie ein direkt anwendbares Gesetz auf EU-Ebene
- → Muss nicht in nationales Recht umgesetzt werden

EU – Act (Verordnung)

- Verbindlicher Rechtsakt der Europäischen Union, der in seiner Gesamtheit gilt
- Wird von den EU-Institutionen (Parlament, Rat, Kommission) nach den EU-Verträgen erlassen

Österreich:
Gesetz: durch Parlament → NISG 2026
Verordnungen: zB durch Ministerium konkretisieren Gesetze

SIEMENS

EU-Gesetzgebung zur Cybersicherheit adressiert die gesamte Lieferkette

	EU NIS2 Richtlinie[1] (Netzwerk und Informations Systeme)	EU Maschinen Verordnung[2] (Verordnung 2023/1230)	EU Cyber Resilience Act[3] (CRA)
Primäre Zielgruppe	Betrieb, Endkunde	OEMs, Maschinenbauer	Hersteller von PDEs „Produkten mit digitalen Elementen“
Hauptfokus	Cybersecurity-Risikomanagement und Berichterstattung über Vorfälle	Safety & Cybersecurity	Cybersicherheit für den gesamten Lebenszyklus solcher Produkte (CE-Kennzeichnung)
In Kraft ab	18. Oktober 2024	20. Januar 2027	Meldepflichten: 11. September 2026 Vollständige Verpflichtungen: 11. Dezember 2027

Zeit

[1] NIS2-Richtlinie: neue Vorschriften für die Cybersicherheit von Netz- und Informationssystemen | Gestaltung der digitalen Zukunft Europas
[2] Regulation - 2023/1230 - EN - EUR-Lex (europa.eu)
[3] Cyberresilienzgesetz (Cyber Resilience Act) | Gestaltung der digitalen Zukunft Europas

SIEMENS

OT-Cybersicherheitsgesetzgebung* weltweit
Relevante globale Rahmenbedingungen

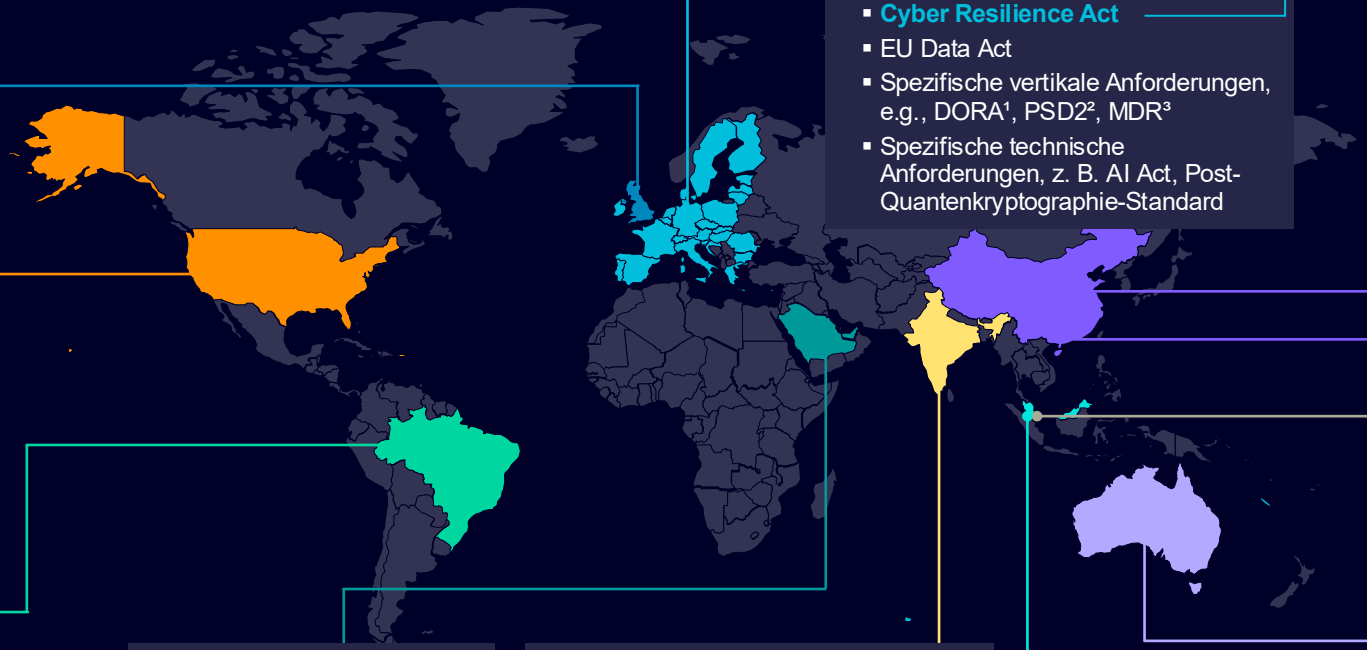
Europa
- Überarbeitete Richtlinie zur Sicherheit von Netzwerk- und Informationssystemenn (NIS 2)
- Cybersecurity Act (CSA)
- **Cyber Resilience Act**
- EU Data Act
- Spezifische vertikale Anforderungen, e.g., DORA[1], PSD2[2], MDR[3]
- Spezifische technische Anforderungen, z. B. AI Act, Post-Quantenkryptographie-Standard

CE

UK
- durch Brexit angelehnt an NIS1, Entwicklung einer eigenen Cyber Security and Resilience Bill (CS&R)

USA
- Schutz kritischer Infrastruktur mit NERC-CIP
- Exekutivanordnungen (z. B. EO 14028)
- Gesetz zur Verbesserung der IoT-Cybersicherheit

Brasilien
- Cybersicherheitsanforderungen für Produkte mit interner Verbindung



Saudi Arabien
- ECC[4] der NCA[5]
- UAE NESA[6] Standards, die für Regierungsstellen und kritische Infrastrukturen ausgegeben wurden

Indien
- Verstärkte regulatorische Aktivitäten
- Schutz der nationalen kritischen Infrastruktur
- Zertifizierungs- und Kennzeichnungs-anforderungen in Schlüsselsektoren

China
- Cybersicherheitsrecht, Datenschutzgesetz (PIPL), Kryptographierecht
- Spezifische technische Anforderungen, z. B. GB/T 40050, GB/T 29246

Hong Kong
- Kritische Infrastruktur (CS), Gesetzentwurf zum Schutz kritischer Informationsinfrastruktur, vollständige Umsetzung bis 2026

Singapur
- Schutz kritischer Informationsinfrastruktur nach dem Cybersicherheitsgesetz (CSA)

Australien
- obligatorische Cybersicherheitsrichtlinie für kritische Infrastrukturen, SoCI Act 2018

Malaysia
- Nationale Cybersicherheitsbehörde ("NACSA") und Cybersicherheitsgesetz 2024 (Gesetz 854)

1 DORA: Digital Operational Resilience Act; **2** PSD2: revised Payment Services Directive; **3** MDR: Medical Device Regulation **4** EEC: Essential Cybersecurity Controls; 5 NCA: National Cybersecurity Authority; 6 National Electronic Security Authority

* Kein Anspruch auf Vollständigkeit

Wo liegen die Herausforderungen in Gebäudetechnik u. Industrie?

SIEMENS

IT und OT - ähnliche Verantwortung andere Perspektive

IT (Informationstechnologie)

Vertraulichkeit

Integrität

Verfügbarkeit

- Starker Fokus auf Cybersecurity
- Gut bekannte und gelistete Assets
- Toleranz für kurze Verzögerungen oder Ausfälle
- Erneuerung der Assets alle 3-5 Jahre
- Angreifer konzentrieren sich auf das Stehlen, Verschlüsseln oder Leaken von Daten

vs.

Priorisierung

OT (Operative Technologie)

Verfügbarkeit

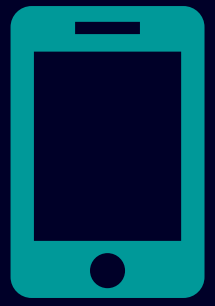
Integrität

Vertraulichkeit

- (Noch) geringer Fokus auf Cybersecurity
- Viele Assets sind weder bekannt noch aufgeführt
- Keine Toleranz für Verzögerungen oder Ausfälle
- Erneuerung der Assets alle 15-20 Jahre
- Angreifer konzentrieren sich auf Störung der Produktion / des Betriebs

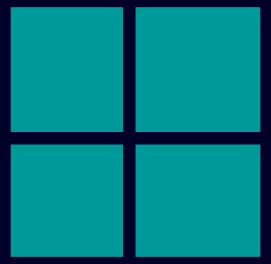
SIEMENS

IT ist (nicht) OT
Wie oft werden Produkte und Systeme upgedatet?



Telefon & Apps

Jede Woche



Betriebssystem

Jeden Monat

Auto

Alle 3-6 Monate

Industrie

"Never touch a running system"

SIEMENS

OT-Security – Schritt für Schritt

Frage 1
Wo stehe ich? Wohin möchte ich?

Phase 2
Was sind meine (kritischen) Assets?

Phase 3
Wie kann ich mich/meine Produktion sichern?

Phase 4
Wie erkenne ich Gefahren?

Phase 5
Was tue ich bei einem Cyberangriff?

Phase 6: Kontinuierliche Verbesserung

SIEMENS

Hands On

09.04.2026

SIEMENS

OT-Security – Schritt für Schritt

Frage 1
Warum ist das Thema (so) kritisch?

Frage 2
Welche Gefahren gibt es konkret?

Frage 3
Wie kann man sich effektiv sichern?

Frage 4
Was müssen wir regulatorisch beachten?

Frage 5
Wie kommen wir pragmatisch in Handeln?

Cybersecurity ist kein Projekt, sondern ein kontinuierlicher Prozess zur Gewährleistung des Betriebs und der Sicherheit.

SIEMENS

Vielen Dank

SIEMENS

Kontakt

Dipl.-Ing. Adrian Pinter, COSM
Zonemanager Cybersecurity EMEA

Siemens Aktiengesellschaft Österreich
Strassgangerstraße 315
8054 Graz
Österreich

Mobil +43 (664) 88552673
E-Mail adrian.pinter@siemens.com

SIEMENS