IoT Security

Cyber Security

bildet das unverzichtbare Fundament der Digitalisierung

Jakob Hohl
Siemens Schweiz AG
Consultant Industry Services

SIEMENS

«Cyber Security bildet das unverzichtbare Fundament der Digitalisierung.»

Jakob Hohl – Consultant Industry Services

SIEMENS

SIEMENS

Wir übernehmen Verantwortung für die Zukunft der Schweiz. Seit 1894.

Seit 1894 prägt Siemens in der Schweiz mit führenden Technologielösungen für Industrie- und Infrastrukturbetriebe massgeblich die Industrialisierung des Landes.

Wir sind Teil der Schweizer Gesellschaft und unser Handeln ist in gemeinschaftlichen Zielen und Werten verankert. Als wichtiger Impulsgeber übernehmen wir aktiv Verantwortung für die Entwicklung des Landes und tragen unsere Innovationskraft in die ganze Welt.

Agenda

- Entwicklungen im OT Bereich
- Praxisbeispiel: Schutz vor “Malerarbeiten
- Defens in Depth – Schutz der OT

Die Bedrohung ist real und nimmt immer mehr zu

61%

der intelligenten Fabriken waren bereits von einen Cybersicherheitsvorfall betroffen

Quelle:
Fertigungsautomatisierung
Intelligente Fabriken sind zunehmend Cybersicherheitsrisiken ausgesetzt

33%

aller Cybersicherheitsvorfälle ereignen sich in Industireanlagen

Quelle:
PMMI Whitepaper 2021 – Risikoeinschätzung
(PMMI 2021 Assess your risk white paper)

65%

aller Ransomware-Angriffe ereignen sich in Industieanlagen

Quelle:
Dragos Jahresrückblick 2021 – Cybersecurity von ICS/OT-Systemen
(Dragos 2021 ICS/OT Cybersecurity year in review)

75%

der IT-Architekturen verfügten 2021 über externe Verbindungen zur Fertigungsebene

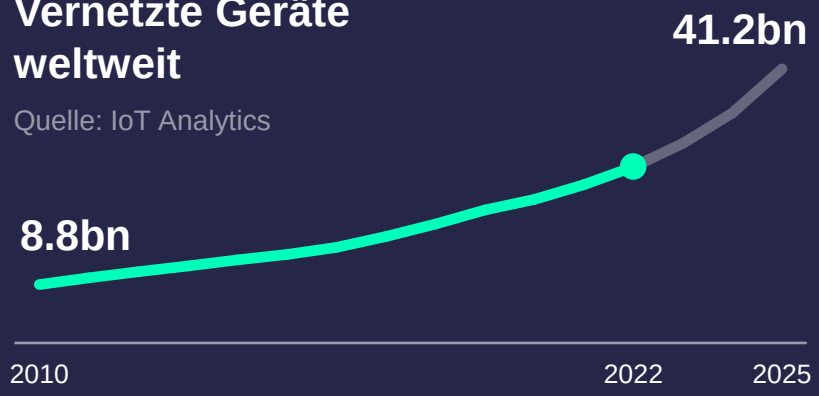
Quelle:
Dragos Jahresrückblick 2021 – Cybersecurity von ICS/OT-Systemen
(Dragos 2021 ICS/OT Cybersecurity year in review)

SIEMENS

Exponentieller Anstieg von Sicherheitslücken durch die Digitalisierung erhöht die Angriffsfläche

Vernetzte Geräte weltweit

Quelle: IoT Analytics



740,000
registrierte Geräte bei Siemens in GJ22

+9% im Vergleich zu GJ21

Quelle: ITAM[1)]

Veröffentlichte Sicherheitslücken

Quelle: NIST

13%
aller veröffentlichten Sicherheitslücken von Software-produkten im Jahr 2021 wurden als ‚kritisch' eingestuft

Quelle: BSI

Vernetzte Geräte X **Veröffentlichte Sicherheitslücken**

Obwohl nicht alle Sicherheitslücken alle Geräte betreffen, ist davon auszugehen, dass durch die Kombination von zunehmender Konnektivität und veröffentlichten Sicherheitslücken ein Multiplikationseffekt entsteht.

Automatisierungssysteme bzw. die Fertigungsebene (OT) insgesamt müssen geschützt werden

Cybersecurity for Industry

[1)] IT Asset Management

Graph: https://www.statista.com/statistics/500755/worldwide-common-vulnerabilities-and-exposures/
Text: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=6

SIEMENS

Die Security-Anforderungen eines industriellen Steuerungssystems unterscheiden sich deutlich von denen der Office IT

IT Security		Industrial Security
Vertraulichkeit		**Verfügbarkeit und Sicherheit**
3-5 Jahre	**Asset-Lebenszyklus**	20-40 Jahre
Erzwungene Migration (z.B. neuer PC, Smartphone)	**Software-Lebenszyklus**	Nutzung solange Ersatzteile verfügbar
Hoch (> 10 Security-Programme auf Büro-PCs)	**Möglichkeit, zusätzliche Security-Software aufzuspielen**	Gering (alte Systeme ohne freien Arbeitsspeicher)
Gering (hauptsächlich Windows 10)	**Heterogenität der Systeme**	Hoch (von Windows 95 bis zu 10)
Standardansatz (zentralisiertes und erzwungenes Patchen)	**Schutzstrategie**	Fall- und risikobasiert

SIEMENS

Vernetzte Fabriken sind für die Abwehr von Cyberangriffen schlecht ausgerüstet

91%

sind der Ansicht, dass IT-Welt und Fertigungsebene (OT) für die Cybersicherheit von Maschinen gemeinsam verantwortlich sein sollten [1)]

90%

der erkannten OT-Sicherheits-probleme sind auf mangelnde Sichtbarkeit über OT-Netzwerke hinweg zurückzuführen [1)]

50%

der Sicherheitsaudits auf der Fertigungsebene decken eine ungeeignete Netzwerk-segmentierung auf [2)]

81%

der vorhandenen Sicherheits-zentralen (SOCs) sind nicht ausreichend auf die Anforderungen des Geschäfts abgestimmt [3)]

4

Vier Hauptgründe warum die OT-Sicherheit immer noch unzureichend ist:

- **Lebenszyklus der Anlagen**
- **Heterogenität**
- **Fokus auf Verfügbarkeit**
- **Risikobasierter Schutz**

Kunden brauchen Unterstützung in Form von durchgängigen OT-Sicherheitsservices & -lösungen

[1)] Bericht zum Status von Operational Technology (OT) und Cybersecurity, Fortinet 2020 2020 State of Operational Technology and Cybersecurity Report (fortinet.com)
[2)] Dragos Jahresrückblick 2022 – Cybersecurity von ICS-Systemen (Dragos 2022 ICS/OT Cybersecurity year in review) Dragos_Year-In-Review-Report-2022.pdf,
[3)] Steigerung der Effektivität von Sicherheitszentralen, Ponemon Institut 2019 Microsoft Word - 2019 Devo Study Final4.docx

SIEMENS

Praxisbeispiel:
Schutz vor „Malerarbeiten“

SIEMENS

Was hat ein Farbeimer mit einem Cyber Angriff zu tun?

Defens in Depth

SIEMENS

Ein ganzheitlicher Cybersecurity-Ansatz

Defense in Depth

basierend auf IEC 62443

Siemens Produkte und Systeme mit integrierter Security

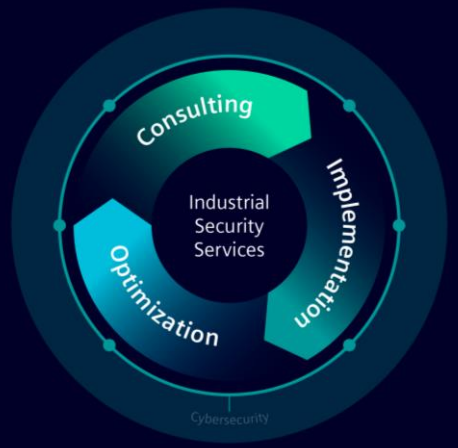
Know-how and copy protection	Authentication and user management	Firewall and VPN	System hardening, continuous monitoring and anomaly detection	Certified Hardware

Siemens Industrial Security Services

Transparenz über den aktuellen Security-Status

Erhöhtes Security-Level durch das Schließen von Sicherheitslücken

Langfristiger Schutz durch kontinuierliches Security-Management



SIEMENS

Ein ganzheitlicher Cybersecurity-Ansatz mit Defense in Depth

Security threats demand action

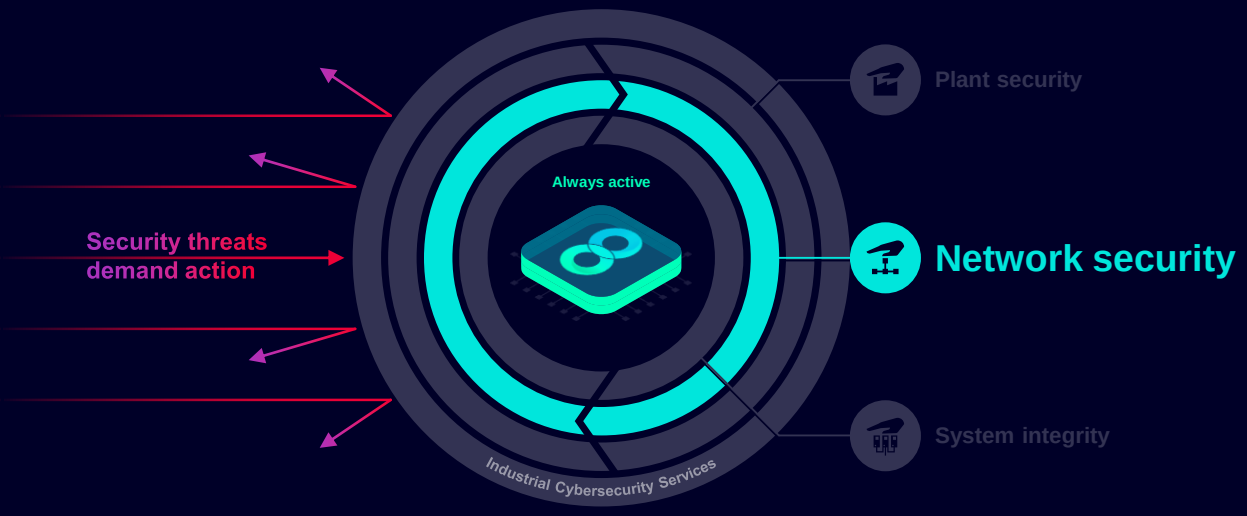
Anlagensicherheit
- Physischer Zugangsschutz
- Security Richtlinien
- Security Monitoring
- Security Assessments

Netzwerksicherheit
- Zellenschutz, Perimeter Netzwerk und vertrauenswürdige Zonen
- Firewalls und VPN

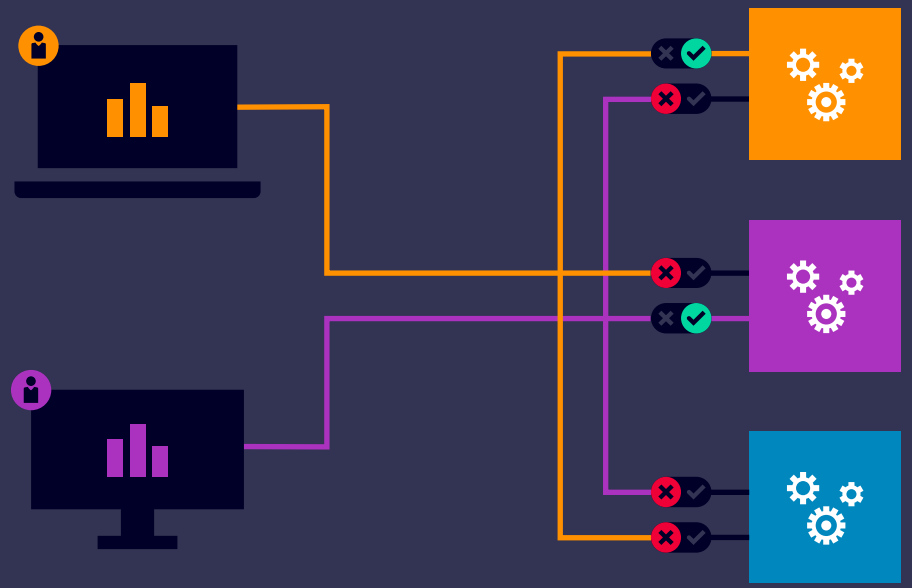
Systemintegrität
- Systemhärtung
- Patch-Management
- Authentifizierung und Zugriffsschutz

SIEMENS

Defense in Depth
gestärkt durch Zero Trust Prinzipien



Klassischer Zellenschutz wird durch Zero Trust Prinzipien erweitert



SIEMENS

Wie wir Sie unterstützen

Konzeptionelle Unterstützung durch Defense in Depth

Durchführen von Cyber Security Assessments

Umsetzung und Unterstützung durch unsere Techniker in Ihrem Unternehmen

Erfahrungen mit „Fremdsystemen“

Experten für alle Themen rund um Netzwerk und Cyber Security im OT Umfeld

Ganzheitliche Betrachtung Ihrer Anlagen und Anlagenteile

Vielen Dank!

SIEMENS

Kontakt

Siemens Schweiz AG

Jakob Hohl
Consultant Industry Services

Freilagerstrasse 40
8047 Zürich
Schweiz

Telefon +41 79 306 85 58

E-Mail jakob.hohl@siemens.com

LinkedIn

SIEMENS