

Warum OT– Sicherheit heute unverzichtbar ist

Ob Wasserwerk, Kläranlage, Industrie-, Energie- oder Entsorgungsbetrieb:

Industrielle Anlagen und Prozessnetze (OT) sind das Rückgrat unserer Daseinsvorsorge. Wenn kritische Anlagen ausfallen, steht nicht nur ein Betrieb still – das öffentliche Leben kommt innerhalb kürzester Zeit zum Erliegen.

Gleichzeitig steigt die Bedrohungslage rasant: Jeden Tag entstehen hunderttausende neue Schadsoftware-Varianten, gezielte Angriffe auf kritische Anlagen nehmen zu, Erpressungen durch Schadsoftware oder Cyberangriffe sind längst auch in der OT zur Realität geworden. Zahlreiche OT-Infrastrukturen werden bereits angegriffen – Tendenz steigend.

Die Folgen sind gravierend:

- **Produktions– und Betriebsausfälle nicht selten mehrere Monate**
- **Erheblicher wirtschaftlicher Schaden**
- **Im schlimmsten Fall: Beeinträchtigung von Versorgungssicherheit und Gemeinwohl**
- **Imageverlust**



Laut Bundesamts für Sicherheit in der Informationstechnik (BSI) liegt die **Anzahl neuer Schadsoftware-Varianten bei weit über 250.000 pro Tag!**

OT ist nicht IT—und braucht eigene Sicherheitskonzepte

Ein häufiger Reflex lautet: „Das muss doch die IT-Abteilung mit übernehmen.“ Doch genau hier liegt ein Kernproblem.

IT– und OT-Welten unterscheiden sich grundlegend:

- In der IT steht hauptsächlich die **Vertraulichkeit** von Daten im Fokus.
- In der OT geht es um **Verfügbarkeit, Betriebssicherheit, Daseinsvorsorge**—teilweise sogar Gefahr für **Leib und Leben**.

OT-Umgebungen bestehen zudem aus langlebigen Komponenten wie SPSen, Feldgeräten oder Frequenzumrichtern, oft mit proprietären Protokollen und hohen Echtzeitanforderungen. Hierfür sind in den IT-Abteilungen keine Kompetenzen (und Ressourcen) vorhanden. Klassische IT-Sicherheitslösungen lassen sich hier nicht einfach übertragen – ungeplante Updates oder Fehlkonfigurationen können Anlagenstillstände verursachen.

Kurz gesagt: OT-Sicherheit erfordert spezielles Know-how, Erfahrung und ein tiefes Verständnis industrieller Prozesse.

Rechtliche Anforderungen: Mittlerweile Pflicht

Parallel zur technischen Entwicklung wurden die rechtlichen Rahmenbedingungen in den letzten Jahren deutlich verschärft:

- IT-Sicherheitsgesetz / KRITIS: Nachweis- und Auditpflichten für große Betreiber
- NIS-2: Erweiterte Pflichten zur Informations- und Cybersicherheit - neben den großen Betreibern nun auch für viele kleine und mittlere Unternehmen
- Für jegliche Anlage aus kritischen Sektoren gilt: der geforderte „Stand der Technik“ als Mindestmaß (oft definiert u.a. in Branchenspezifischen Sicherheitsstandards B3s)

Streben Sie schon heute **mindestens den „Stand der Technik“** an – nicht aus Angst, sondern aus Verantwortung für Betriebssicherheit, Versorgungssicherheit und Zukunftsfähigkeit. Spätestens im Schadensfall prüfen Sachverständige, Versicherer oder Gerichte genau gegen diesen Stand der Technik. Die Frage lautet dann nicht mehr, ob ein Angriff passiert ist – sondern ob angemessen vorgesorgt wurde.



Auch wenn es noch um Details in der deutschen Gesetzgebung zur Umsetzung der NIS-2-Richtlinie geht, können (und sollten!) **wichtige technische und organisatorische Sicherheitsanforderungen schon heute angegangen werden!**

ISMS: Oft Pflicht – aber immer ein sinnvoller Weg

<

Ein formales Informationssicherheits-Managementsystem (ISMS) ist laut BSI nicht zwingend vorgeschrieben. In der Praxis zeigt sich jedoch klar: Ohne ein strukturiertes ISMS lassen sich NIS-2-Anforderungen und der Stand der Technik kaum angemessen umsetzen.

Ein pragmatisches, OT-gerechtes ISMS – norm- und B3S-konform – schafft Struktur, Transparenz und belastbare Nachweise und kann als Nachweis des geforderten Standes der Technik dienen.

Warum SEGNO der richtige Partner ist

Viele Systemintegratoren sind technisch exzellent – aber nicht auf OT-Sicherheit spezialisiert. SEGNO verbindet tiefes Verständnis industrieller Anlagen mit spezialisiertem OT-Sicherheits-Know-how.

Von der OT-Statusanalyse über NIS-2-Kompatibilitäts-Checks bis hin zum ISMS begleitet SEGNO Betreiber darüber hinaus **ganzheitlich**, strukturiert und auf Augenhöhe – angemessen skaliert nach Bedarf, Risiko und Anlagengröße.

Unser Team vereint praktische OT-Erfahrung mit dem Blick langjähriger Berater und ehemaliger BSI-Auditoren. So verstehen wir nicht nur technische Anforderungen, sondern auch Prüfungsmaßstäbe, Nachweispflichten sowie organisatorische Erwartungen von Anlagenverantwortlichen, Aufsichtsbehörden, Auditoren oder Versicherern.

SEGNO unterstützt Sie dabei.



SEGNO Industrie Automation GmbH

Admiralstraße 54

28215 Bremen

kontakt@segno.de

www.segno.info