STAR GROUP

CYBERSECURITY
FÜR IHRE PRODUKTIONSANLAGEN

Sicher. Gesetzeskonform. Zukunftsfähig.

NACHHALTIGE SICHERHEIT FÜR PRODUKTIONS- UND BETRIEBSPROZESSE BEGINNT BEI SAR

Die fortschreitende Digitalisierung industrieller Anlagen, Produktionsumgebungen und Infrastrukturen schafft erhebliche Effizienz- und Wettbewerbsvorteile. Vernetzte Maschinen, automatisierte Prozesse und der kontinuierliche Datenaustausch zwischen IT- und OT-Systemen sind heute fester Bestandteil moderner Industrieumgebungen.

Gleichzeitig wächst jedoch die Cyberangriffsfläche deutlich. Insbesondere OT-Umgebungen (Operational Technology), die nicht für eine vernetzte Nutzung ausgelegt wurden, sind zunehmend Ziel von Ransomware, Malware und Sabotage. Die Folgen reichen von Produktionsausfällen und Qualitätsverlusten bis hin zu Sicherheits- und Reputationsschäden.

Dieses Whitepaper zeigt, warum klassische Sicherheitskonzepte nicht mehr ausreichen und wie Produktionsanlagen mit einem ganzheitlichen Cybersecurity-Ansatz nachhaltig schützt.

CYBERBEDROHUNGEN IN INDUSTRIELLEN OT-UMGEBUNGEN

Operational Technology (OT) umfasst Systeme und Netzwerke zur Steuerung, Überwachung und Automatisierung physischer Prozesse, darunter unter anderem:

- SPS/PLC zur Steuerung von Roboterarmen und Fließbändern
- SCADA Systeme zur Überwachung von Produktionslinien
- HMI (Mensch Maschine Schnittstellen) zur Maschinenbedienung
- Energie-, Wasser- und Versorgungsanlagen
- Transport und Logistik (z. B. Verkehrsleitsysteme, Zug und Flottenüberwachung)
- Kritische Infrastrukturen (Wasserversorgung, Abwasserbehandlung, Prozessleitsysteme)

Im Gegensatz zur klassischen IT liegt der Fokus in OT-Umgebungen nicht auf Daten, sondern auf **Verfügbarkeit, Integrität und Sicherheit von Prozessen**. Störungen oder Manipulationen wirken sich unmittelbar auf Produktion, Lieferfähigkeit und Versorgungssicherheit aus.

Cyberangriffe zielen zunehmend direkt auf industrielle Prozesse. Manipulierte Steuerungen, veränderte Parameter oder gezielte Abschaltungen können die physische Produktion unmittelbar und nachhaltig beeinträchtigen.

Mit der zunehmenden Vernetzung wachsen die Risiken erheblich:

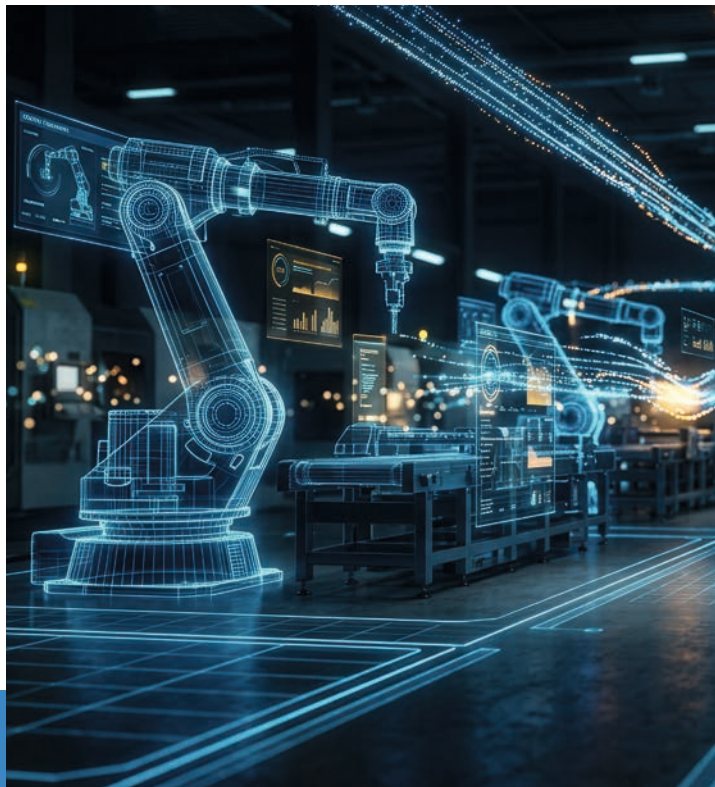
- **Erweiterte Angriffsflächen** durch Fernzugriffe, Cloud Anbindungen und externe Dienstleister
- **Mangelnde Transparenz** über Assets und Kommunikationsbeziehungen
- **Veraltete Systeme** mit eingeschränkten Update Möglichkeiten
- **Hohe Auswirkungen** selbst bei kurzen Ausfällen

DIE BESONDERE BEDROHUNGSLAGE IN OT-UMGEBUNGEN

OT-Systeme wurden lange Zeit isoliert betrieben und galten daher als vergleichsweise sicher. Diese Annahme ist heute nicht mehr gültig. Wesentliche Gründe dafür sind:

- Zunehmende Vernetzung von OT- und IT-Systemen
- Fernwartungszugänge und externe Dienstleister
- Einsatz mobiler Endgeräte und Wechselmedien
- Veraltete, nicht patchbare Systeme

Moderne Cyberangriffe zielen zunehmend auf **Sabotage, Erpressung und Produktionsausfälle** ab. Klassische IT Sicherheitsmechanismen wie Virenscanner oder Firewalls stoßen in OT-Umgebungen dabei schnell an technologische und operative Grenzen.



TYPISCHE HERAUSFORDERUNGEN FÜR UNTERNEHMEN

Viele Unternehmen stehen bei der OT Cybersecurity vor ähnlichen Herausforderungen:

- Fehlende Transparenz über Systeme und Kommunikationsbeziehungen
- Hohe Anforderungen an Verfügbarkeit und Echtzeitfähigkeit
- Lange Lebenszyklen von Anlagen und Steuerungen
- Begrenzte Wartungsfenster
- Steigende regulatorische Anforderungen (z. B. NIS2, IEC 62443)

Insbesondere Betreiber Kritischer Infrastrukturen (KRITIS) unterliegen erweiterten gesetzlichen Vorgaben, darunter erhöhte Sicherheits , Dokumentations und Meldepflichten. Sicherheitsvorfälle in OT-Umgebungen müssen innerhalb definierter Fristen gemeldet werden. Fehlende Transparenz oder unzureichende Überwachung gefährden dabei nicht nur den Betrieb, sondern können auch rechtliche und wirtschaftliche Folgen nach sich ziehen.

ANFORDERUNGEN AN MODERNE INDUSTRIELLE CYBERSECURITY

Um diesen Risiken wirksam zu begegnen, benötigen Unternehmen spezialisierte Sicherheitslösungen, die den besonderen Anforderungen industrieller Umgebungen gerecht werden. Eine reine Übertragung klassischer IT Security Ansätze ist nicht ausreichend. Erforderlich sind speziell auf OT zugeschnittene Konzepte, die sich in fünf zentrale Säulen gliedern:

Transparenz und Inventarisierung
Vollständige Sichtbarkeit aller Systeme, Geräte und Datenverbindungen – ohne Beeinträchtigung des laufenden Betriebs.

Kontinuierliches Monitoring
Permanente Überwachung des Netzwerkverkehrs zur frühzeitigen Erkennung von Abweichungen vom Normalbetrieb.

Anomalie- und Angriffserkennung
Identifikation ungewöhnlicher Kommunikationsmuster, Manipulationen und potenzieller Angriffe.

Intelligente Alarmierung
Priorisierte und verständliche Aufbereitung relevanter Sicherheitsereignisse für schnelles, zielgerichtetes Handeln.

Integration in bestehende Prozesse
Nahtlose Einbindung der OT Cybersecurity in bestehende Betriebs , Wartungs und Sicherheitsprozesse.

Die ganzheitliche Umsetzung dieser Handlungsfelder schafft eine belastbare Sicherheitsbasis für industrielle IT- und OT-Umgebungen. Cybersecurity wird damit vom rein technischen Schutzmechanismus zu einem strategischen Faktor für stabile Prozesse und regulatorische Sicherheit.

SAR ALS PARTNER FÜR OT CYBERSECURITY

Mit **IRMA® (Industrie Risiko Management Automatisierung)** bietet SAR eine speziell für OT-Umgebungen entwickelte Cybersecurity Lösung.

IRMA® schützt Produktionsanlagen durch passive, kontinuierliche Netzwerküberwachung, ohne den laufenden Betrieb zu beeinträchtigen. Cyberbedrohungen werden frühzeitig erkannt und Risiken gezielt minimiert. Der ganzheitliche Sicherheitsansatz basiert auf vier zentralen Schritten:

Analysieren

Automatische Identifikation aller vernetzten Assets in IT und OT-Umgebungen.

Verwalten

Strukturierte Klassifizierung und Gruppierung von Systemen für hohe Transparenz.

Bewerten

Echtzeit Erkennung von Bedrohungen, Anomalien und Schwachstellen inklusive Risikobewertung.

Visualisieren

Übersichtliche Dashboards und intelligente Alarmierung für schnelle Reaktionen.

VORTEILE FÜR BETREIBER INDUSTRIELLER ANLAGEN

Der Einsatz von IRMA® bietet Unternehmen zahlreiche operative und strategische Vorteile:

- ✓ **Echtzeit Bedrohungserkennung:** Sofortige Erkennung von Angriffen und Sicherheitsvorfällen vor Produktionsausfällen.
- ✓ **Automatisierte Asset Transparenz:** Vollständiger Überblick über alle verbundenen Systeme – auch in komplexen OT-Umgebungen.
- ✓ **Minimierung von Produktionsausfällen:** Frühzeitige Alarmierung ermöglicht rechtzeitige Gegenmaßnahmen.
- ✓ **Unterstützung regulatorischer Anforderungen:** Hilfestellung bei der Umsetzung von NIS2, KRITIS, DORA oder IT SiG 2.0.
- ✓ **Schutz auch für nicht patchbare Systeme:** Wirksame Absicherung älterer Steuerungen und Betriebssysteme durch passive Überwachung.
- ✓ **Unterstützung bei Compliance und Audits:** Transparenz, Dokumentation und Reporting erleichtern die Nachweisführung.
- ✓ **Nachhaltige Risikoreduktion:** Kontinuierliche Risikotransparenz als Basis fundierter Sicherheitsentscheidungen.
- ✓ **Einfache Implementierung:** Schnelle Integration ohne aufwendige Umbauten oder Produktionsunterbrechungen.
- ✓ **Zukunftssicherheit:** Skalierbare Sicherheitsarchitektur für wachsende Digitalisierungsanforderungen.

SAR IT-SERVICES

Cybersecurity in industriellen IT- und OT-Umgebungen ist ein zentraler Erfolgsfaktor für stabile, sichere und zukunftsfähige Produktions- und Betriebsprozesse. SAR verbindet fundiertes IT Security Know how mit tiefem Verständnis industrieller Abläufe und entwickelt ganzheitliche Sicherheitskonzepte, die sich nahtlos und ohne Betriebsunterbrechung integrieren lassen. Unternehmen profitieren von praxisnahen Lösungen zur nachhaltigen Risikoreduktion, zur Unterstützung regulatorischer Anforderungen und für langfristige Planungssicherheit. Mit langjähriger Erfahrung im Bereich IT Services ist die SAR GmbH ein verlässlicher Partner für eine wirkungsvolle und zukunftsorientierte Cybersecurity-Strategie.

Vereinbaren Sie jetzt Ihren Beratungstermin unter **www.sar.biz**

SAR Elektronic GmbH
Gobener Weg 31
84130 Dingolfing

its@sar.biz
www.sar.biz