Keywords
- Cybersecurity
- Anlagensicherheit
- NIS-2-Richtlinie



© markus dehlzeit - stock.adobe.com

Wenn Cyberangriffe zu Safety-Risiken werden

OT-Security als integraler Bestandteil des sicheren Anlagenbetriebs

Die Prozessindustrie befindet sich in einer Phase tiefgreifender regulatorischer und technologischer Veränderungen. Mit der europäischen NIS-2-Richtlinie sowie den deutschen Regelwerken KAS-51 und TRBS 1115 1 wird Cybersicherheit nicht mehr als isolierte IT-Disziplin verstanden, sondern als zwingender Bestandteil des sicheren Betriebs industrieller Anlagen. Für Betreiber bedeutet das: OT-Security wird zur Führungsaufgabe, und zwar mit klaren technischen, organisatorischen und dokumentatorischen Anforderungen.

Regulatorische Anforderungen: Cyber-Resilienz als gemeinsames Ziel

Die NIS-2-Richtlinie definiert europaweit Cyberresilienz-Mindeststandards u. a. für Chemieunternehmen mit mehr als 50 Mitarbeitern. Betreiber sind seit Dezember 2025 zu einem systematischen Risikomanagement verpflichtet. Insbesondere die Verfügbarkeit kritischer Systeme und die Fähigkeit, Cyberangriffe zu erkennen, abzuwehren und deren Auswirkungen zu begrenzen, werden gefordert. NIS-2 zwingt damit Unternehmen, Cyber Security auf ein professionelles, dokumentiertes und überprüfbares Niveau zu heben.

KAS-51 und TRBS 1115 1 adressieren spezifische Anforderungen für störfallrelevante und arbeitssicherheitskritische Anlagen, um Personen und Umwelt zu schützen. Beide Regelwerke verlangen explizit, dass Betreiber Manipulationen an PLT Sicherheitseinrichtungen, Prozessleitsystemen und relevanten Hilfssystemen verhindern müssen. KAS-51 als nationale Leitlinie für Störfallbetriebe fordert eine Bewertung von Cyberrisiken für Sicherheitsfunktionen und Schutzsysteme in Anlagen. TRBS 1115 1 konkretisiert die Betriebssicherheitsverordnung im Hinblick auf Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen.

Für Betreiber bedeutet das: Security-Risiken werden zu Safety-Risiken, sobald sie die Wirksamkeit sicherheitsgerichteter Funktionen beeinflussen können.

Warum OT-Security ein Safety-Thema ist

Safety-Einrichtungen sind Cyberbedrohungen ausgesetzt. Während in der IT neben der Verfügbarkeit in der Regel die Vertraulichkeit das höchste Schutzziel ist, gilt in der OT: Integrität hat höchste Priorität. Ein Cyberangriff, der eine PLT-Schutzeinrichtung manipuliert, ist sicherheitstechnisch von den Auswirkungen her gleichzusetzen mit einem Hardware-Defekt oder einer Fehlparametrierung. Solche Eingriffe können im einfachsten Fall die Produktion unterbrechen und im schlechtesten Fall die Verhinderung von Störfällen unterdrücken. Damit wird OT-Security zu einem Pflichtbestandteil des Safety Lifecycle nach IEC 61511.

Typische OT-Besonderheiten wie Lebenszyklen von 15–25 Jahren, proprietäre Protokolle und fehlende Security Stacks, Validierungs- und Herstellerfreigaben als Änderungsrestriktion oder die Gefahr von Anlagenstillständen durch Patches verlangen andere Maßnahmen als die, die in der IT zum Standard geworden sind.

Patch-Risikoanalyse: strukturiert, nachvollziehbar, regulatorisch belastbar

Patchen bringt zwei Probleme mit sich. Erstens: Um zu patchen, müssen Systeme häufig heruntergefahren werden. Zweitens: Es ist sehr schwierig vorherzusehen, ob das Gesamtsystem nach einem Patch-Vorgang noch gleich funktionieren wird wie davor. Deshalb ist die risikobasierte Patch-Entscheidung ein zentrales Element der OT-Security. Das in der NAMUR-Empfehlung AK Praxis AK 4.18 beschriebene Vorgehen bietet hierfür einen etablierten Rahmen.

Wesentliche Schritte dabei sind:

- 1. Analyse der Schwachstelle: Welche Funktionen sind betroffen? Wie kritisch ist die Ausnutzbarkeit?
- 2. Bewertung der Exposition: Netzwerkpfade, externe Schnittstellen, Remote-Zugänge.
- 3. Entscheidung über Patchbarkeit: Berücksichtigung von Validierung, Herstellerfreigaben und Produktionsfenstern.
- 4. Kompensierende Maßnahmen wie z. B. Netzwerksegmentierung und Isolierung betroffener Komponenten, Härtung (Abschalten unnötiger Dienste, Ports, Protokolle), Application Whitelisting oder Restriktion von Kommunikationspfaden.
- 5. Dokumentation und Wirksamkeitskontrolle: Entscheidungen müssen nachvollziehbar sein: Warum wurde nicht gepatcht? Welche Alternativen wurden geprüft? Wie wird die Wirksamkeit überwacht?

Ziel ist stets, das Risiko so weit zu reduzieren, dass der sichere Betrieb gewährleistet bleibt — mit oder ohne Patch.

Remote Access: der Diskussionspunkt zwischen Safety und Security

Remote-Zugänge werden in vielen Anlagen eingesetzt, um Überwachungs- und Wartungsaufgaben zu erledigen. Insbesondere für Safety-Systeme ist der Remote-Zugang jedoch ein notwendiges Übel und äußerst umstritten.

Typische Schwachstellen:

- „vergessene“ Zugänge aus der Errichtungsphase,
- fehlende Kontrolle über Dienstleister,
- Absicherung des Kanals, aber nicht der Gegenstelle,
- unzureichende Protokollierung sicherheitsrelevanter Eingriffe.

Ein sicherheitskonformes Remote-Access-Konzept umfasst:

- vollständige Inventarisierung aller Zugänge,
- starke Authentisierung und rollenbasierte Freigaben,
- Zugriff nur für geschultes, vertrauenswürdiges Personal,
- Integration in Management of Change und Sicherheitsnachweisführung,
- lückenlose Protokollierung aller Eingriffe in sicherheitsrelevante Systeme.

Damit wird Remote Access zu einem Safety-relevanten Prozess, nicht zu einer x-beliebigen IT-Dienstleistung.

Segmentierung im Brownfield: pragmatisch statt perfekt

Die Maßnahme der Segmentierung bzw. Mikrosegmentierung soll Bedrohungen und unerwünschte Auswirkungen auf möglichst kleine Bereiche des Gesamtsystems beschränken.

Historisch gewachsene OT-Netzwerke sind oft schlecht dokumentiert. Ein wirksamer Einstieg beginnt mit:

- passiver Netzwerkanalyse,
- Sichtung vorhandener Netzwerkpläne,
- Gesprächen mit Instandhaltung und Betrieb,
- Abstimmung der Netzwerksegmente mit Notfallplänen (was muss im Notfall unbedingt kommuniziert werden).

Darauf aufbauend werden Zonen und Conduits nach ISA/IEC 62443 definiert. Entscheidend ist eine risikobasierte Priorisierung: Maßnahmen mit hohem Sicherheitsgewinn und geringem Eingriff werden zuerst umgesetzt.

Angriffserkennung: Frühwarnsystem oder Einfallstor?

Moderne OT-Anomalie-Erkennungssysteme können Muster erkennen, anhand derer Angriffe identifiziert werden können:

- ungewöhnliche Prozesswerte,
- unerwartete Änderungen an Safety-Parametern,
- untypische Kommunikationsmuster,
- Abweichungen in Sequenzen oder Verriegelungslogiken.

Angriffserkennungssysteme haben den Vorteil, dass alle Anomalien erkannt werden. Also auch solche, die eine Fehlkonfiguration oder





Der OT-Security-Kongress „IMI: IT meets Industry“ bringt seit vielen Jahren Experten aus Industrie und Forschung zusammen.



IMI: IT meets Industry Congress in Mannheim.

Systemstörung als Ursache haben und nicht einen Cyber-Angriff. Safety-Steuerungen sollten möglichst wenig vernetzt sein. Um nicht unnötige Einfallstore zu öffnen, wird Angriffserkennung primär für stark vernetzte oder integrierte Sicherheitssteuerungen empfohlen.

Beim gesamten Maßnahmenkonzept zur Cyber Security ist oft die größte Schwachstelle nicht die Technik, sondern fehlende Prozesse. Transparenz gegenüber dem Management inklusive einer Kosten-Nutzen-Bewertung ist ein wichtiger Erfolgsfaktor.

25 Jahre OT-Security: Was bleibt, was kommt

Die IT/OT-Konvergenz hat die industrielle Automatisierung grundlegend verändert. Heute prägen Zero-Trust-Ansätze, Segmentierung und kontinuierliches Monitoring die Praxis, während Angriffe häufiger werden — insbesondere durch Ransomware-Akteure. Damit wird OT-Security zur notwendigen Voraussetzung für funktionale Sicherheit. Die Integration von OT-Security in den Safety Lifecycle ist kein „Nice-to-have“, sondern eine regulatorische und technische Notwendigkeit. Cyberangriffe können sicherheitsgerichtete Funktionen beeinträchtigen — und damit Störfälle auslösen.

Trotz aller technologischen Entwicklungen bleibt ein Prinzip unverändert: Die richtige Strategie entscheidet. OT-Security bedeutet, Komplexität zu beherrschen — nicht, sie zu erhöhen. Oder wie ich es formuliere: OT-Security = Kompetenz/Komplexität. Künstliche Intelligenz wird dabei eine doppelte Rolle spielen: Sie unterstützt bei der Erkennung von Angriffen und Schwachstellen, schafft aber zugleich neue Angriffsflächen.



Erwin Kruschitz,
Mitgründer und CEO von Anapur. Experte für Safety, Cyber Security und GMP; Mitglied und Leiter von NAMUR-Arbeitskreisen

Wiley Online Library

Anapur AG, Mannheim
Tel.: +49 621 397 29 619
info@anapur.de · www.anapur.de

© Bilder Anapur