Welchen Einfluss NIS2 auf OT-Umgebungen hat

Know-how to go

Daniel Jedecke,
Maximilian Haselberger

Maximilian Haselberger

Senior Consultant

- Ausgebildeter Fachinformatiker für Anwendungsentwicklung
- Durchführung zahlreicher Penetrationstests mit Fokus auf industrieller Sicherheit
- Beratung und Auditierung im Bereich der kritischen Infrastrukturen nach § 8a BSIG
- Durchführung von Open-Source-Intelligence-Analysen (OSINT)
- Diverse Fachvorträge über OSINT
- Forschung im Bereich der Satellitensicherheit

Agenda

1. Einführung
2. Abgrenzung IT/OT
3. Herausforderungen im OT-Umfeld
4. Technische Sicherheitsmaßnahmen im OT
5. Technische Maßnahmen im Fokus der NIS2

1. Einführung

Einführung

- NIS2 betrifft vornehmlich die IT …

  => … viele von NIS2 betroffene Betriebe betreiben aber auch große OT- Umgebungen!

2. Abgrenzung IT/OT

Wie grenzen sich **IT** und **OT** ab?

Information Technology

Technologien zur Verarbeitung von Informationen, bestehend meist aus Computern, Geräten und Servern, die im Sinne der Geschäftsziele betrieben werden und miteinander verbunden sind.

- Bürokommunikation, Unternehmenssteuerung, digitale Geschäftsprozesse
- Fokus auf einfache Nutzung und Vertraulichkeit von Informationen
- **Beispiele**: Server, Apps, LAN/WAN, …

Operational Technology

Systeme zur computer-gestützten Automation der Überwachung, Steuerung und Regelung von Prozessen, bestehend aus Hardware und Firmware.

- ICS (Industrial Control Systems)
- Fokus auf Verfügbarkeit und Betriebssicherheit der Systeme
- **Beispiele**: Cyber Physical Systems (CPS), DCS, PCS, Domänenspezifische/ proprietäre (Übertragungs-)Protokolle, Embedded Sytems, …

Absolute Trennschärfe zwischen IT und OT ist nicht gegeben.
Beispiele Grenz-/Schnittstellenbereiche: Data Analytics/KI/Big Data, Leitsysteme, Netzwerkinfrastruktur

TREND IT/OT-Konvergenz …

IT/OT-Konvergenz

IT/OT-Konvergenz bezeichnet die zunehmende technische Verzahnung von Systemen der Betriebstechnologie (OT) mit Systemen der Informationstechnologie (IT).

Hierbei wird die IT zunehmend zur Überwachung und Steuerung von Ereignissen, Prozessen und Geräten genutzt und besetzt damit die Domäne der OT.

Auch dient sie der Aufbereitung von Daten aus der OT und bildet das Bindeglied in die ERP-Abläufe der Organisation.

… und einhergehende **KOMPLIKATIONEN**

Historisch getrennte Domänen

- Unterschiedliche **Technologien**, Standards, Protokolle, Prozesse und Architekturen
- **Fokus IT**: stetige Verbesserung von Workflows, Innovation, Benutzererfahrung, kurze Modernisierungszyklen, Trend zur „Agilisierung“
- **Fokus OT**: stabile Regelkreise und zuverlässige automatisierte Steuerung industrieller Prozesse, Nutzung langlebiger Industriemaschinen mit extrem langen Innovationszyklen
- Wenig **Wissen** über die jeweils andere Domäne und deren Praktiken
- Wenig gegenseitiges **Verständnis** für Ziele sowie Rahmenbedingungen
- Wenig abteilungsübergreifende Koordination und **Zusammenarbeit**
- Unterschiedliche Prägungen; **unterschiedliche Fachkulturen; fehlende gemeinsame Sprache**

Security & KRITIS

- **Neue Angriffsvektoren auf OT-Systeme durch zunehmende Vernetzung. OT-Systeme sind darauf nicht ausgerichtet.** Proprietäre Protokolle und Legacy-Schnittstellen ohne Vorkehrungen für Authentisierung und Vertraulichkeit
- Geringer Bezug zur IT(!)-Sicherheit
- **Eingeschränkte Reaktionsfähigkeit** auf neue Bedrohungen
- Unterschiedliche **Gewichtung von Schutzzielen**
- **Störanfälligkeit** industrieller Prozesse; geringe Fehlertoleranzen
- Schwerwiegende Auswirkungen bei Systemausfällen; hohe Wiederanlaufzeiten
- I. d. R. kein gemeinsames Risiko- und Incident Management

3. Bestehende Herausforderungen im OT-Umfeld

Die TOP 10 der ICS-Bedrohungen 2022 (gemäß BSI)

- Mehr Angriffe seit 2019
  - Infektion mit Schadsoftware über Internet und Intranet
  - Kompromittierung von Extranet und Cloud-Komponenten
  - Internet-verbundene Steuerungskomponenten
  - Einbruch über Fernwartungszugänge
  - Soft- und Hardwareschwachstellen in der Lieferkette
- Gleiche Bedrohungslage wie 2019
  - Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
  - Menschliches Fehlverhalten und Sabotage
  - Social Engineering und Phishing
  - (D)DoS-Angriffe
  - Technisches Fehlverhalten und höhere Gewalt

Bestehende Herausforderungen

- Wenig geschultes IT-Security-Personal
- Hersteller leben noch nicht „Security by Design“
- Langlebigkeit der Maschinen
- Viele typische Maßnahmen der NIS2 sind nicht direkt umsetzbar

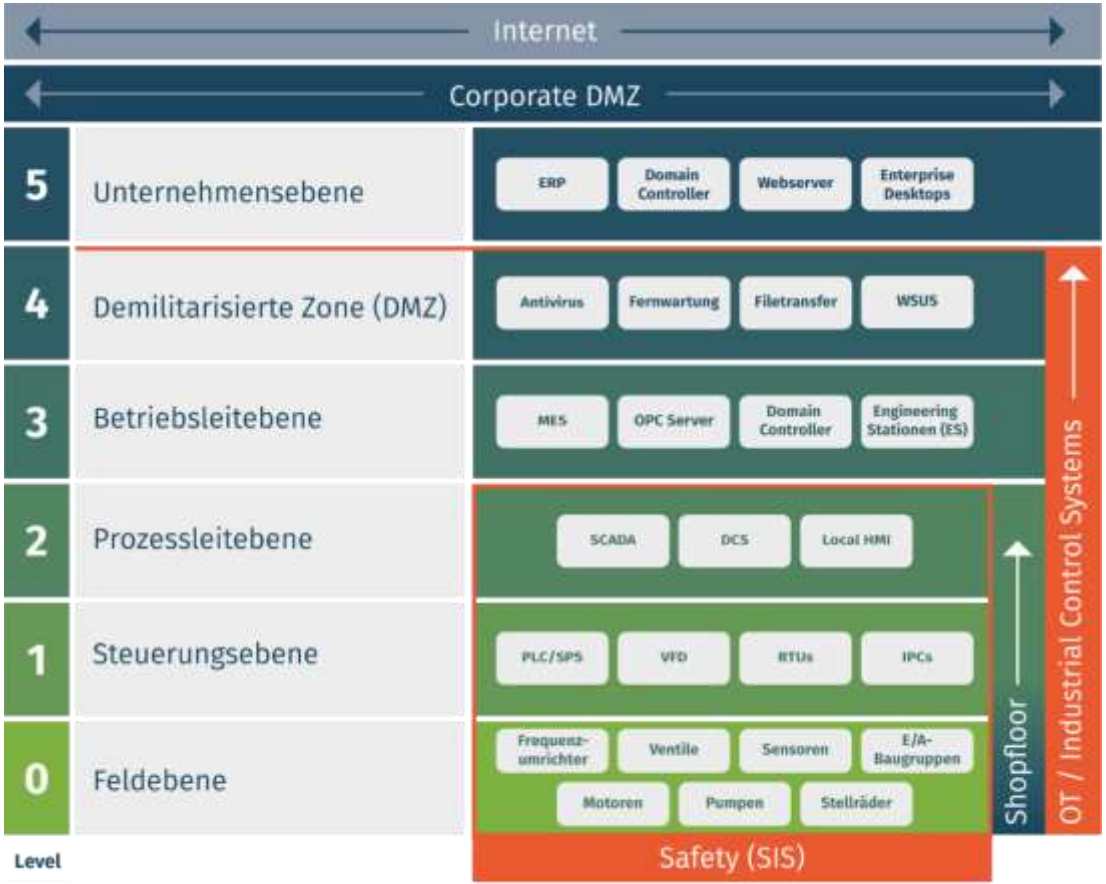
4. Technische Sicherheitsmaßnahmen im OT

Was ist Industrial/OT Security

- Industrial Security beschreibt den Schutz von Produktions- und Industrieanlagen, aber auch von Systemen, welche keine klassischen IT-Systeme als Grundlage haben, vor Gefahren und Bedrohungen

- Themengebiet ist breit und umfasst mehrere Richtungen
  - Cyber Security
  - Safety
  - Arbeitsschutz
  - Umweltschutz

Typischer Aufbau



© www.sichere-industrie.de

Klassische IT-Sicherheitsmaßnahmen

- Netzwerksegmentierung
- Überwachung und Detektion (IDS/IPS)
- Zugriffskontrollen und Authentifizierung (vor allem Fernzugriff)
- Patch-Management und Updates (je nach Exponiertheit)
- Implementierung von Sicherheitsrichtlinien und -Prozessen (spezielle Vorgaben für Dienstleister und Hersteller)
- Schulung und Sensibilisierung der Mitarbeiter

Abwehr im Kontext Industrieanlagen

- Klare Trennung der Netzwerke (PURDUE Model)
- Absicherung und Überwachung von Remotezugriffen auf die Anlagen
- Steuerung für Dienstleister
- Detektion und Reaktion von möglichen Angriffen
- Notfallmanagement aufbauen
- Offline-Datensicherung durchführen

Die Folgekosten eines Vorfalls betragen oft ein Vielfaches der Investitionen in Präventivmaßnahmen.

5. Technische Maßnahmen im Fokus der NIS2

Wenig Änderung, mehr Fokus

- Die relevanten Änderungen für Maßnahmen in der technischen Sicherheit im Kontext der NIS2 finden sich vor allem
  - im Risikomanagement
  - bei der Vorfallserkennung und -meldung
  - in der Netzwerksegmentierung
  - in der Kryptografie
  - in der Wiederherstellung
  - in der Lieferkettensicherheit

Risikomanagement

- Unternehmen müssen robuste Risikomanagementmaßnahmen implementieren, die auf ihre OT- und IT-Systeme angewendet werden.
  - Identifizierung von Risiken
  - Implementierung von Sicherheitsmaßnahmen

- Herausforderung aus der Praxis:
  - Assetmanagement
  - Fehlende Risikomanagementprozesse
  - Ressourcen

Netzwerksegmentierung

- Es gibt einen stärkeren Fokus auf Segmentierung bzw. Trennung von Netzwerken

- Herausforderung aus der Praxis:
  - Netzwerke sind in der Praxis oft schlecht getrennt
  - Vorhandene Systeme können auf Grund der Technik manchmal nicht sicher identifiziert werden
  - Vorhandene Netzwerke sind häufig zu groß,
    da organisch gewachsen
  - Isolierung von risikobehafteten Systemen ist ohne Risikomanagement nicht kurzfristig möglich,
    insbesondere im Bereich der Remotewartung

Vorfallserkennung

- Auch die Sicherheitspraktiken der Lieferanten und Partner müssen nun bewertet werden, um sicherzustellen, dass diese ebenfalls robust sind.
  - Das Beispiel ***xz-utils*** gibt hierbei besonders zu denken …

- Herausforderung aus der Praxis:
  - Vollständiges Assetmanagement
  - **Aktive** Steuerung von Lieferanten durch vollständige Unterlagen und Dokumente

5. Fazit

Fazit

- NIS2 erweitert den Anwendungsbereich und betrifft damit neue Sektoren. **Verstärkter Ressourcenmangel,** insbesondere für OT Security, ist damit vorprogrammiert
- Durch die höheren Sanktionen **steigt der Druck** auf Unternehmen erheblich, während zur Umsetzung durch die Tiefe **mehr Aufwand** benötigt wird

Daraus folgt:

- Unternehmen müssen *jetzt* handeln! Unsere Erfahrung zeigt, ein **Verständnis der eigenen Infrastruktur** in Verbindung mit **einem guten Risikomanagement** sind eine große Hilfe.

HISOLUTIONS

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com