SPG SPECIFIC GROUP

LSZ FUTURE CONNECTIONS

OT-Compliance unter NIS2

Herausforderungen an IT/OT-Schnittstelle und Legacy-Systeme

Mag. Dzevad Mujezinovic, CIPP/E, CISM

Cyber Crime Forum Graz 29.09.2025

Einführung

- NIS2 = EU-Richtlinie (2022/2555)
- Ersetzt NIS1, gilt ab Oktober 2024 / Nationales Recht???
- Ziel: Einheitliches, hohes Cybersicherheitsniveau in Europa
- Gilt für wesentliche & wichtige Einrichtungen (Energie, Transport, Wasser, Gesundheit, Infrastruktur, Produktion)
- Erfasst IT- und OT-Systeme

Warum OT besonders betroffen ist?

- Angriffe auf OT haben reale Auswirkungen: Produktionsstillstände, Versorgungsausfälle, Sicherheitsrisiken
- OT = Steuerung und Überwachung physischer Prozesse (SCADA, DCS, PLCs, Robotik)
- Unterschiede zur IT: OT = Verfügbarkeit & Safety, IT = Vertraulichkeit & Integrität

Herausforderungen IT/OT-Schnittstelle

- **Sicherheitslücken:** Fernwartung, IIoT, Cloud-Anbindungen

- Unterschiedliche Sicherheitslogiken in IT & OT

- NIS2 (ErwGr. 89, Art. 21): Netzwerksegmentierung, Zugriffskontrollen, Monitoring

- Praxis: IT & OT-Teams oft in Silos → **fehlende Abstimmung/Zusammenarbeit**

NIS2-Pflichten für OT (Art. 21)

- Risikomanagement & Sicherheitsrichtlinien für OT anpassen
- Incident Handling & Meldungen (24h Frühwarnung, 72h Bericht)
- Business Continuity & Disaster Recovery
- Supply-Chain-Security (Hersteller, Integratoren, Wartungsfirmen)
- Zugriffskontrolle & Kryptografie
- Schulung & Sensibilisierung der Mitarbeiter

ISMS & Informations Security Governance

- ISMS muss erweitert werden: OT in die Policies integrieren
- Governance-Strukturen: Rollen & Verantwortlichkeiten definieren
- Benennung von OT-Sicherheitsbeauftragten
- Schnittstellen-Management zwischen IT-Security & OT-Security
- **Ziel:** Einheitliches Sicherheitsmanagement für IT & OT (soweit möglich)

Exkurs: Asset-Management in der OT

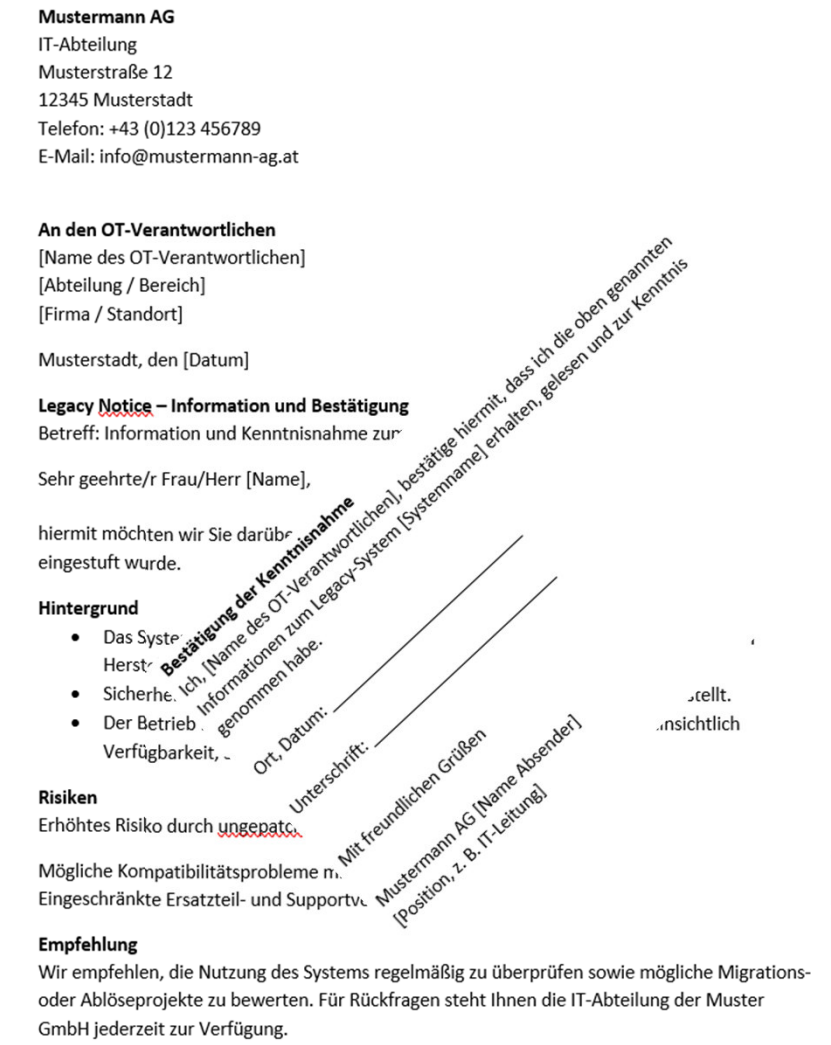
- **Grundlage für Risikoanalysen** nach NIS2 (Art. 21)
- Erhebung: Inventarisierung **aller** OT-Assets (das sind alle Geräte, Systeme und Komponenten, die in industriellen Umgebungen für die Steuerung, Überwachung und Automatisierung von Prozessen eingesetzt werden
- Dokumentation: Hersteller, Version, Patch-Status, Kritikalität
- Methoden: passive Netzwerkanalyse, manuelle Ergänzungen, CMDB
- Pflege: Inventar regelmäßig aktualisieren
- **Nutzen:** Transparenz, Incident Response, Audit-Nachweise

Audit-Nachweise für NIS2-Behörden

- Risikomanagement-Dokumentation inkl. IT/OT-Schnittstellen & Legacy-Systeme
- OT-Asset-Inventar mit Patch-Status
- Aktualisierte ISMS-Policy inkl. OT-Governance
- Security-Richtlinien & Prozesse (Zugangsmanagement, Segmentierung)
- Incident-Response-Plan (24h/72h Meldeprozesse)
- Business Continuity & Notfallpläne
- Lieferanten- und Wartungsverträge mit Sicherheitsanforderungen
- Trainings- und Schulungsnachweise

Legacy-Systeme: Achillesferse der OT

- Lebensdauer 20–30 Jahre, kein Security by Design
- Hersteller-Support ausgelaufen, proprietäre Protokolle
- NIS2 fordert Schutz: auch Altgeräte müssen abgesichert werden
- Lösungen: Segmentierung, Whitelisting, Monitoring, strikte Fernwartung, Ablösungs-Roadmap



Mustermann AG
IT-Abteilung
Musterstraße 12
12345 Musterstadt
Telefon: +43 (0)123 456789
E-Mail: info@mustermann-ag.at

An den OT-Verantwortlichen
[Name des OT-Verantwortlichen]
[Abteilung / Bereich]
[Firma / Standort]

Musterstadt, den [Datum]

Legacy Notice – Information und Bestätigung
Betreff: Information und Kenntnisnahme zur

Sehr geehrte/r Frau/Herr [Name],

hiermit möchten wir Sie darüb
eingestuft wurde.

Hintergrund

- Das Syste
  Herst
- Sicherhe
- Der Betrieb
  Verfügbarkeit,

Bestätigung der Kenntnisnahme
Ich, [Name des OT-Verantwortlichen], bestätige hiermit, dass ich die oben genannten Informationen zum Legacy-System [Systemname] erhalten, gelesen und zur Kenntnis genommen habe.

Ort, Datum: _____

Unterschrift: _____

tellt.
nsichtlich

Mit freundlichen Grüßen

Mustermann AG [Name Absender]
[Position, z. B. IT-Leitung]

Risiken
Erhöhtes Risiko durch ungepatc

Mögliche Kompatibilitätsprobleme m
Eingeschränkte Ersatzteil- und Supportv

Empfehlung
Wir empfehlen, die Nutzung des Systems regelmäßig zu überprüfen sowie mögliche Migrations- oder Ablöseprojekte zu bewerten. Für Rückfragen steht Ihnen die IT-Abteilung der Muster GmbH jederzeit zur Verfügung.

Tipps aus der Praxis

- **Aktualisieren ISMS & Informations Security Governance**
- Ordnen Sie Ihre OT-Kontrollen je nach Ihrer Gerichtsbarkeit Rahmenwerken wie ISA/IEC 62443, MV, etc.
- Systeme & Schnittstellen inventarisieren
- Risiken bewerten und Maßnahmen planen
- Netzwerke segmentieren & Legacy-Systeme absichern
- Etablieren Sie sicheres Fernzugriffsmanagement
- Dokumentation für Audit vorbereiten
- Bewahren Sie detaillierte Nachweise über die Umsetzung der Kontrollen auf, einschließlich Protokollen, Netzwerkkarten und Zugriffskontrollrichtlinien.
- Schulungen & Übungen durchführen

Fazit

- NIS2 = Pflicht & Chance für Resilienz
- Baustellen: IT/OT-Schnittstellen absichern, Legacy-Systeme kontrollieren
- **Asset-Management & Governance als Schlüssel für OT-Sicherheit**
- Unternehmen müssen Transparenz schaffen, Verantwortlichkeiten definieren, Audit-Nachweise bereitstellen

Kontakt

Specific-Group Austria GmbH

Hoher Markt 5

1010 Wien

https://www.specific-group.com

Mag. Dzevad Mujezinovic, CIPP/E, CISM
Managing Director GRC Consulting
Head of GRC Services

Dzevad.mujezinovic@specific-group.com

SPG ist Ihr pragmatischer und praxisorientierter Partner, der Compliance und Information-Security einfach und effektiv macht. Wir kombinieren technische Expertise, langjährige, branchenübergreifende Erfahrung und operative Exzellenz.

Mission Statement