OT100-WS OT Security Industrieanlagen effektiv vor Cyberattacken schützen

Kurzbeschreibung:

Moderne Produktionsanlagen sind durch ihren hohen Vernetzungsgrad und die Einbindung von Standard-IT-Komponenten zunehmend Cybersicherheitsrisiken ausgesetzt. Gleichzeitig lassen sich etablierte Maßnahmen der IT-Sicherheit in diesem Umfeld nicht uneingeschränkt anwenden. Warum das so ist und wie industrielle Cybersicherheit effektiv umgesetzt werden kann, erfahren Sie in diesem **Web-Seminar**.

Zielgruppe:

- CISOs und andere IT-Sicherheitsverantwortliche produzierender Unternehmen
- IT- und Cybersecurity-Experten
- Verantwortliche für Produktionsanlagen
- Ingenieure und Techniker aus dem Bereich Automatisierungstechnik
- OT-Verantwortliche
- Produkt- / Entwicklungsverantwortliche bei Herstellern von Automatisierungstechnik

Voraussetzungen:

Um den Kursinhalten und dem Lerntempo im Web-Seminar **OT Security – Industrieanlagen effektiv vor Cyberattacken schützen** gut folgen zu können, sind folgende Kenntnisse von Vorteil:

- Grundlegende IT-Kenntnisse
- Grundkenntnisse im Bereich IT-Security

Sonstiges:

Dauer: 1 Tage

Preis: 0 Euro plus Mwst.

Ziele:

Moderne Produktionsanlagen sind zunehmend Cybersicherheitsrisiken ausgesetzt. Das Web-Seminar **OT Security – Industrieanlagen effektiv vor Cyberattacken schützen** gibt Ihnen einen ersten Überblick, wie Cybersicherheit im Kontext industrieller Produktion bewertet und verbessert werden kann.

Die Teilnehmer erfahren u.a.

- wie wesentliche Bedrohungen angemessen eingeordnet werden können
- welche typische Schwachstellen es gibt und was deren (mögliche) Auswirkungen sind
- in welchem Rahmen etablierter IT-Security-Ansätze in der OT anwendbar sein können
- welche Grundprinzipien sich in der industriellen Cybersicherheit etabliert haben

Inhalte/Agenda:

- **Bekannte Vorfälle und aktuelle Bedrohungen**
  - Historie: Stuxnet, Industroyer, Triton / Trisis
  - Ramsomware (z.B. Vorfall bei Norsk Hydro)
  - Incontroller/Pipedream-Malware
- **Verbreitete OT-Security Mythen**
  - Sicherheit durch proprietäre Systeme and Protokolle
  - Schutz durch Air Gaps, Firewalls und serielle Kommunikation
  - (unaufgefordert) sichere Umsetzung durch Hersteller / Integratoren
  - Vollständige Absicherung durch Safety-Systeme
- **Typische Schwachstellen und Security-Herausforderungen (aus der Beratungspraxis)**
  - Fehlende/eingeschränkte Netzwerksicherheit (Segmentierung, Modems, Wifi, etc.)
  - Unzureichend abgesicherter Fernzugriff (intern/extern)
  - Unsichere Nutzung von mobilen Geräten (Engineering Laptops, etc.) und Usb-Sticks
  - Eingeschränkte physische Sicherheit der OT-Infrastruktur
- **Unterschiede zwischen IT- und OT-Security-Maßnahmen**
  - Malwareschutz
  - Netzwerksegmentierung
  - Vulnerablity Scans
  - Security Patching
  - Security-Monitoring und Incident Response
  - Security Awareness
- **Effektive Steigerung der industriellen Cybersicherheit**
  - Perimetersicherheit
  - Gezielte Härtung
  - Datensicherung und -Wiederherstellung
  - Grundlegende Angriffserkennung und Incident Response
- **Q & A Session**