VEREIN DEUTSCHER INGENIEURE
Bezirksverein München, Ober- und Niederbayern e.V.
Arbeitskreis Unternehmer und Führungskräfte

Cyber Security im Produktionsumfeld | Themenabend 22.07.2026

Bei Cyber Security denken viele zunächst an klassische IT-Themen wie Laptops oder Phishing-Mails. Doch welche Auswirkungen haben Cyber-Bedrohungen in der Industrie? Was bedeutet Cyber Security im Produktionsumfeld konkret? Und wie lässt sich die Sicherheit von Produktionsanlagen gewährleisten?

Beim Themenabend des **VDI Arbeitskreises „Unternehmer und Führungskräfte“** zeigte der Referent **Konstantin Rogalas** von der Firma Honeywell in seinem Vortrag, warum Cyber Security in industriellen Produktionsumgebungen über klassische IT-Sicherheit hinausgeht und es wurde viel diskutiert.

Manipulierte Sensorwerte, Steuerbefehle oder Anlagenkomponenten können Produktionsausfälle, Umweltschäden und Gefahren für Menschen verursachen. In der Operational Technology stehen daher funktionale Sicherheit, Kontrollierbarkeit und Anlagenverfügbarkeit im Vordergrund.

ICS/OT Security

- IT + PHYSIK
  - Digitale Systeme, die physische Objekte betätigen

1) Funktionale Sicherheit (Safety)
2) Integrität der Beobachtbarkeit (inputs: Sensoren)
3) Integrität der Kontrolierbarkeit (outputs: Aktoren)
4) Verfügbarkeit
5) Integrität
6) Vertraulichkeit

Priorität umgekehrt

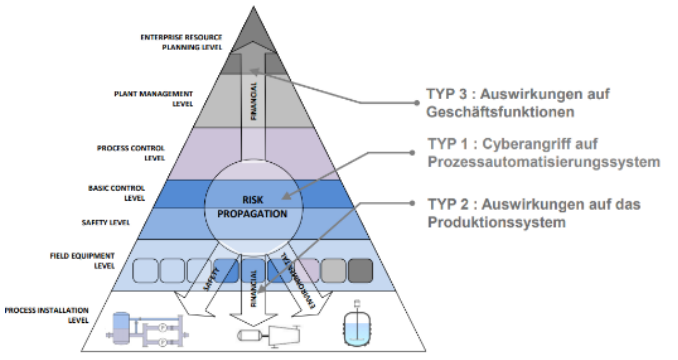
Einblicke gab es in die **NIS2-Richtlinie,** ein EU-weites Cybersicherheitsgesetz. Mit der deutschen Umsetzung von NIS2 werden neben kritischen Infrastrukturen auch viele mittelständische Industrieunternehmen sowie produktionsnahe IT- und OT-Dienstleister reguliert. Die Geschäftsführung trägt die Verantwortung für ein angemessenes Risikomanagement und hat sich entsprechende Fachkenntnisse anzueignen.

Zentrale Maßnahmen sind die Absicherung von Lieferketten und Fernwartung, Mehrfaktor-Authentifizierung, Netzwerksegmentierung sowie ein vollständiges Inventar aller OT-Komponenten. Hinzu kommen eine kontinuierliche Anomalieerkennung und OT-spezifische Notfallpläne. Klassische IT-Reaktionen wie das sofortige Abschalten eines Systems können in der Produktion zusätzliche Gefahren auslösen. Deshalb ist klar zu regeln, wie Anlagen kontrolliert in einen sicheren Zustand gebracht werden. Gesetzliche Meldefristen sind in die Prozesse zu integrieren.

Für die Aufrechterhaltung und Wiederherstellung der Produktion werden getrennte Backups von Steuerungsprogrammen, manueller Notbetrieb, redundante Kommunikationswege, Ersatzkomponenten und eine definierte Wiederanlaufreihenfolge benötigt. Schulungen und regelmäßige Notfallübungen ergänzen die technischen Maßnahmen.

Konstantin Rogalas stellte abschließend zwei Bewertungsansätze von Honeywell vor, die Compliance- und Risikoanalysen mit einem priorisierten Maßnahmenplan verbinden. Die csHAZOP-Methode untersucht, welche Cyberangriffe Prozessrisiken auslösen können, und bewertet die Folgen für Menschen, Umwelt, Betrieb und Finanzen.

DREI VERSCHIEDENE OT RISIKO-ENGAGEMENTS



OT-Cyber Security wird als Teil des gesamten betrieblichen Risikomanagements verstanden.

Dipl.-Math. Petra Jacob,
Beirätin VDI Arbeitskreis Unternehmer und Führungskräfte

VEREIN DEUTSCHER INGENIEURE | Bezirksverein München, Ober- und Niederbayern e.V.
Westendstraße 199 (TÜV) | 80686 München | +49 89 5791-2200 | www.VDI-Sued.de
Amtsgericht München VR 4284 | Vorstandsvorsitz: Andreas Wüllner, Prof. Dr. Peter Pfeffer (stv.)