BearingPoint

Sichere Produktion im vernetzten Zeitalter: Schwachstellen erkennen, Angriffsflächen reduzieren

- Sicherheit in (I)IoT-Netzwerken –

Breakout-Session

LSZ: Industry Summit

27. November 2025

Caroline Neufert, Alexander Schwemberger

AGENDA

1. **Herausforderungen**
2. Regulatorische Anforderungen
3. Interaktive Session: Use Cases & Lösungsansätze
4. Fazit & Ausblick

1. Einführung – in a nutshell

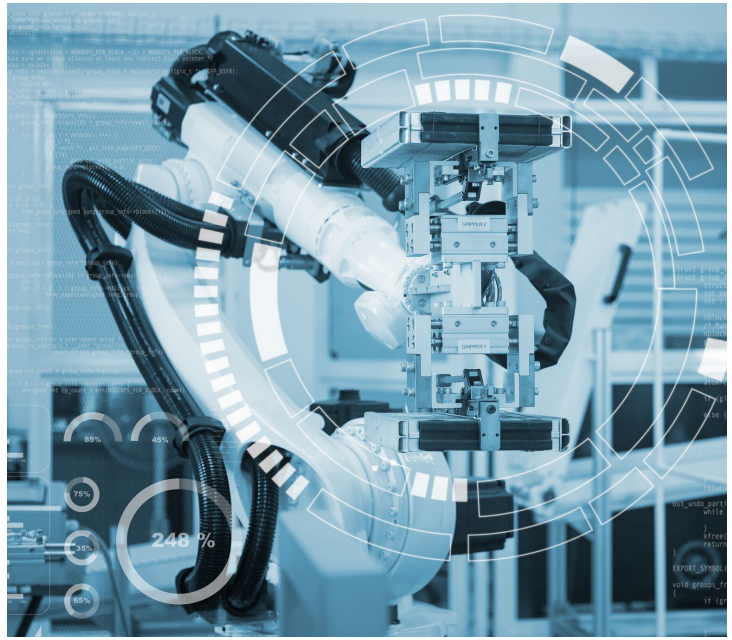
Effiziente Fertigung und Automatisierung
OT, IoT und IIoT ermöglichen vernetzte Maschinen und Systeme, die Produktionsprozesse automatisieren und optimieren

Vorausschauende Wartung
Echtzeitdaten von Sensoren helfen, Wartung rechtzeitig durchzuführen und Ausfallzeiten zu reduzieren

Cybersecurity Herausforderungen
Die steigende Vernetzung erhöht die Angriffsfläche, weshalb Sicherheitsmaßnahmen in der Produktion essenziell sind

Risikomanagement
Unternehmen können Vorteile nutzen und Risiken aktiv managen, um Produktionsausfälle und Datenverlust zu vermeiden

Sicherheitsstrategien
Proaktive Strategien wie Security by Design und Zero Trust sind essentiell für sicheren Einsatz vernetzter Systeme



Bedrohungslage (IT-bezogen)

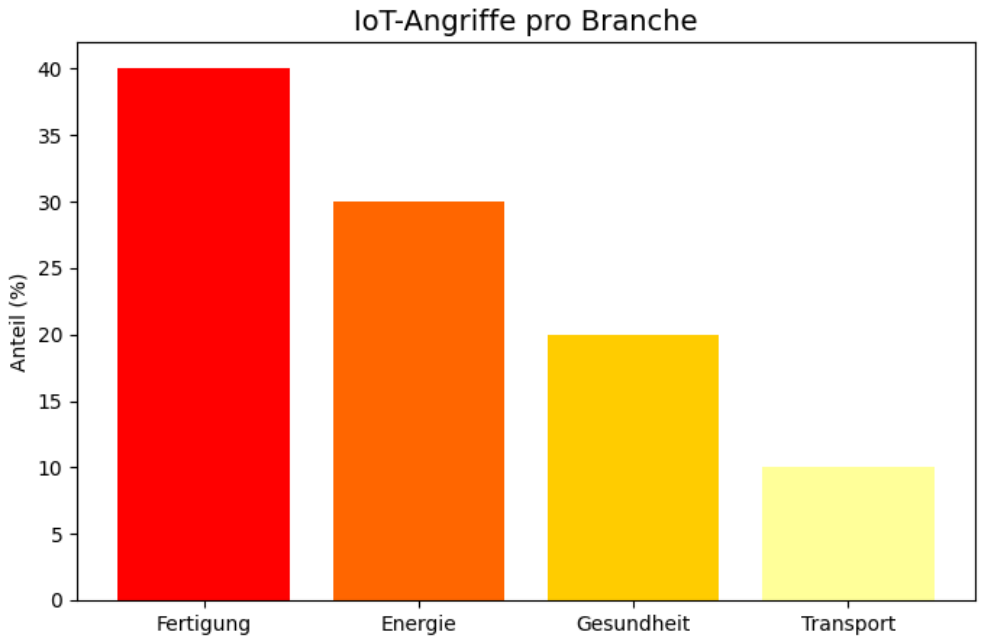
7/10

Betroffene Industrieunternehmen

Ca. 270 Mrd EUR

Jährlicher Schaden in D

Thema	Anstieg	Branche
IoT-Angriffe	+400 %	Alle, besonders Fertigung
Angriffe im Energiesektor	+387 %	Kritische Infrastruktur
Ransomware	+ 87 %	Industrieziele
täglich **119 neue Sicherheitslücken**	+ 24%	Alle Industrien
Zahl aktiver Angreifergruppen	+71 %	29 Gruppen fokussieren OT-/ICS-Systeme



Quellen: SANS ICS Survey, IBM X-Force, Kaspersky ICS Report, Allianz Cyber Risk Report, BITKOM, Statista VDMA & ENISA

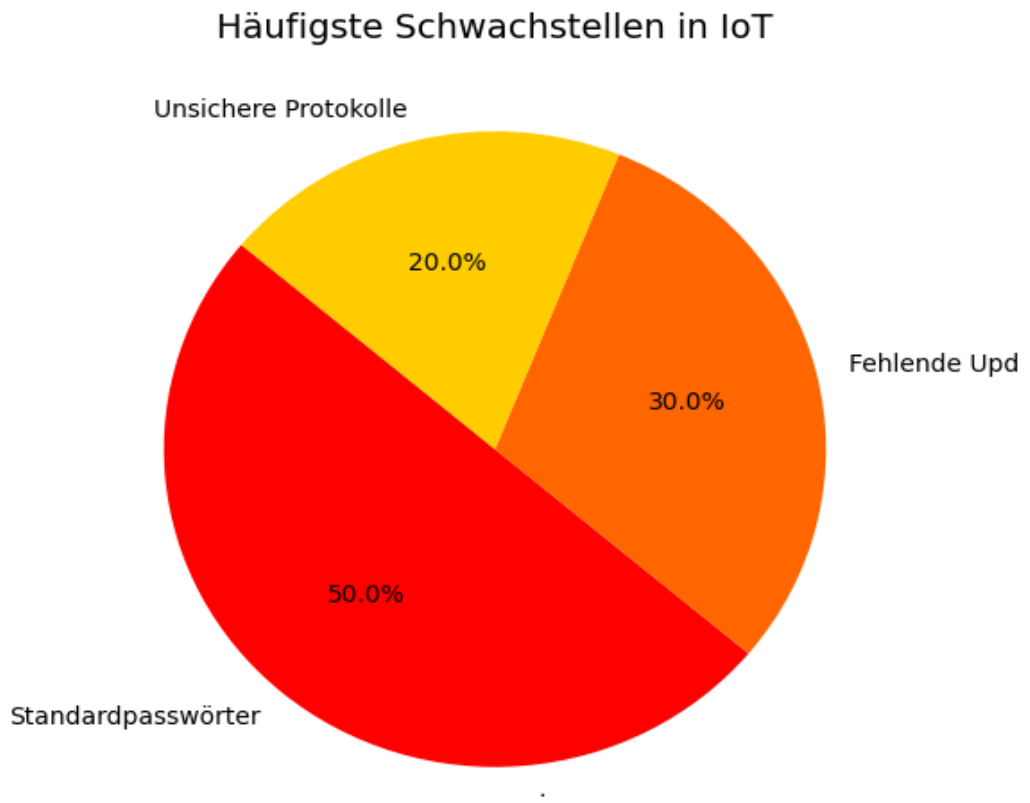
„Standard“- Schwachstellen

Technologische Schwachstellen

- Standardpasswörter („admin/admin“) – Botnetze wie Mirai
- Ungepatchte Firmware (60% der Vorfälle)
- Mangelnde Segmentierung (77,8% der Netzwerke)
- Legacy-Systeme ohne Updatefähigkeit
- 70 % der Schäden entstehen durch indirekte Folgen wie Produktionsausfälle und Lieferkettenprobleme
- OT/IT-Konvergenz erhöht Komplexität
- Gerätevielfalt & fehlende Standards

Organisatorische Schwachstellen

- Unklare Rollen und Verantwortlichkeiten
- Fehlende Schulungen



IT-Herausforderungen zusammengefasst

Sichtbarkeit & Skalierung

Tausende von neuen Sensoren und Geräten müssen verwaltet und überwacht werden. Die schiere Masse macht einheitliche Sicherheit extrem komplex.

Netzwerk-Konvergenz

Die Trennung von IT (Büro) & OT (Produktion) löst sich auf. Risiken aus der IT gehen direkt in die OT und gefährden physische Prozesse.

Legacy-Systeme

Viele Maschinen (SPS, SCADA) sind Jahrzehnte alt, ungepatcht und waren nie für eine Verbindung mit dem Internet konzipiert.

AGENDA

1. Herausforderungen
2. **Regulatorische Anforderungen**
3. Interaktive Sessions: Use Cases & Lösungsansätze
4. Fazit & Ausblick

Regulatorische Anforderungen

- Compliance ist nicht gleich Sicherheit, kann aber helfen -

NIS2

Erweiterter Anwendungsbereich
18 Wirtschaftssektoren mit erweiterten Sicherheitsanforderungen

Ziel der Richtlinie
Erhöhung der Resilienz kritischer Infrastrukturen und Verbesserung der Zusammenarbeit zwischen EU-MS

Zentrale Sicherheitsanforderungen
Risikobasiertes Cybersecurity-Management (inkl. Governance, Rollen/Verantwortung), Integration in Unternehmensführung und Meldepflichten bei Sicherheitsvorfällen, Lieferkettensicherheit, Audits, Notfalltests, Kryptografie, MFA, Schulung

Strenge Sanktionen
Verstöße können Bußgelder bis zu 10 Mill. Euro oder 2 % des Jahresumsatzes betragen

Cyber Resilience Act

Mindestanforderungen für Cybersicherheit für alle vernetzten Produkte auf dem EU-Markt (digitale Elemente). Meldepflicht von Sicherheitsvorfällen CE-Kennzeichnung für IoT-Produkte

Security by Design und Default
Produkte müssen nach den Prinzipien „Security by Design“ und „Secure by Default“ entwickelt werden

Herstellerpflichten und Updates
Hersteller müssen Risiken bewerten, Schwachstellen beheben und Sicherheitsupdates über die Lebensdauer bereitstellen

Umsetzung und Sanktionen
Die schrittweise Umsetzung bis 2027 sieht Strafen von bis zu 2,5 % des Jahresumsatzes bei Verstößen vor

MVO (EU) 2023/1230

Die MVO ab 20. Januar 2027 ist spezifisch für Maschinen -> Safety + Cybersecurity CE-Kennzeichen

Maßnahmen
Maschinen müssen so konstruiert sein, dass sicherheitsrelevante HW/SW und Daten vor Manipulation geschützt sind, Protokollierung, sichere Steuerungen, KI-Integration- Menschliche Kontrolle bleibt Pflicht, Systeme müssen Eingriffe in sicherheitsrelevante Komponenten erkennen und dokumentieren. Härtung, NW-Segmentierung

Lieferkette: Hersteller, Händler, Importeure und Betreiber sind verpflichtet, keine unsicheren Maschinen in Verkehr zu bringen

Meldepflicht primär gegenüber nationalen Marktüberwachungsbehörden bei Produktmängeln

Relevante Sicherheitsstandards I

Merkmal	IEC 62443 (Gesamte Normenreihe)	ISO/IEC 27001	CIS Controls
Primärer Fokus	Cybersicherheit industrieller Automatisierungs- & Steuerungssysteme (IACS)	Informationssicherheits-Managementsystem (ISMS) für Organisationen	Priorisierte technische Sicherheitskontrollen zur Reduzierung häufiger Cyberangriffe
Anwendungsbereich	Betreiber (Asset Owners), Systemintegratoren (System Integrators) und Hersteller (Product Developers) von industriellen Steuerungssystemen , OT-Umgebungen, industrielle Systeme, kritische Infrastrukturen	Alle Arten von Organisationen (öffentlich, privat, gemeinnützig), unabhängig von Größe, Art oder Branche, die ihre Informationen schützen wollen	Alle Organisationen – besonders geeignet für Organisationen, die eine Grundlagen-Sicherheit aufbauen oder die Umsetzung priorisieren wollen
Konzept	Defense in Depth (Verteidigung in der Tiefe) und Zones & Conduits zur Segmentierung des IACS-Netzwerks. Definiert Security Levels (SL) für spezifische Sicherheitsanforderungen	Plan-Do-Check-Act (PDCA)-Zyklus für das ISMS. Der Risikobasierte Ansatz ist zentral für die Auswahl der Maßnahmen.	Pragmatische, priorisierte Maßnahmen („Cyber Defense Best Practices“)
Struktur	Besteht aus einer Normenreihe mit vier Hauptbereichen (General, Policies & Procedures, System, Components & Requirements), die sich an die verschiedenen Akteure richtet	Hauptnorm, die die Anforderungen für das ISMS festlegt (Kapitel 4–10) und einen Anhang (Anhang A) mit einer Liste von Sicherheitsmaßnahmen (Controls)	18 CIS Controls mit Safeguards (IG1–IG3)

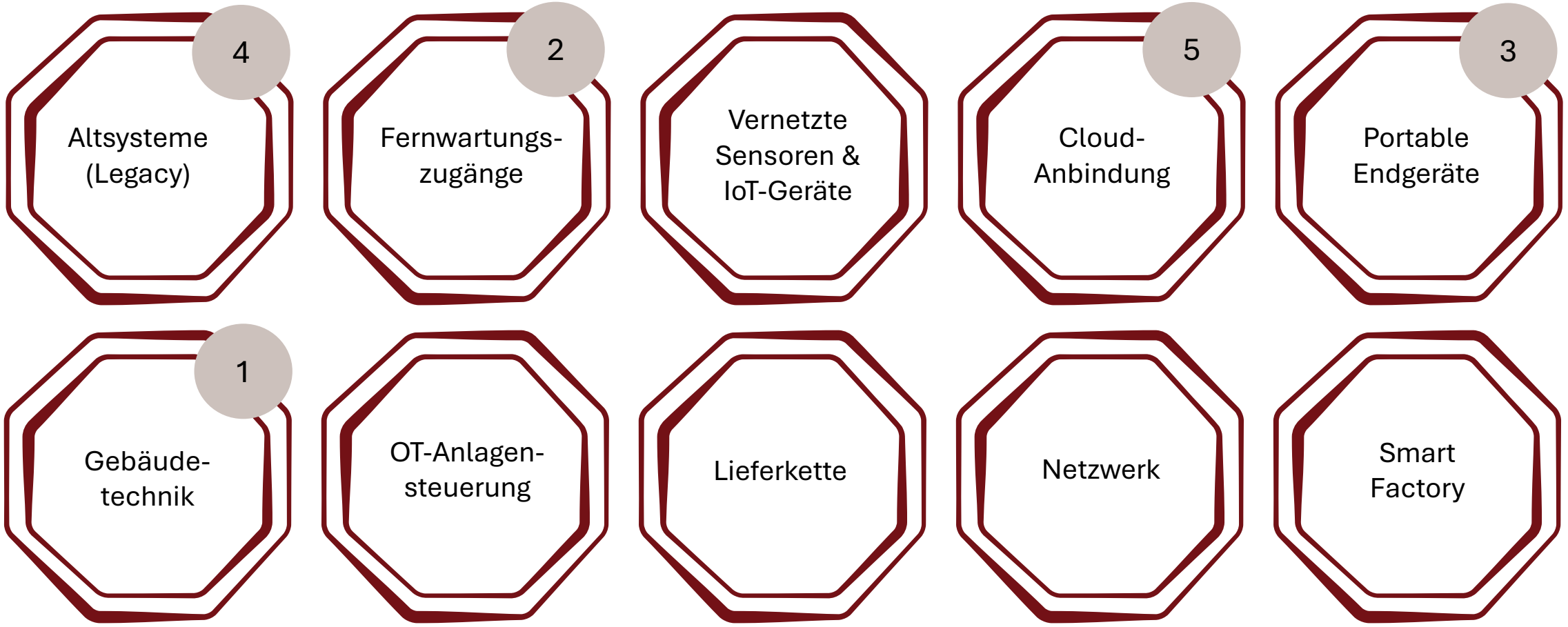
Relevante Sicherheitsstandards II

Merkmal	IEC 62443 (Gesamte Normenreihe)	ISO/IEC 27001	CIS Controls
Wichtige Inhalte	- Definition von Sicherheitsniveaus (SL 1 bis SL 4) - Technische Sicherheitsanforderungen an Komponenten und Systeme (z. B. Authentifizierung, Datenfluss) - Prozesse für sichere Produktentwicklung und Betrieb - Risikobewertung speziell für IACS-Umgebungen	- Kontext der Organisation und interessierte Parteien - Führung und Verpflichtung des Managements - Risikobeurteilung und Risikobehandlung - Anhang A-Maßnahmen (z. B. Zugangskontrolle, Kryptographie, physische Sicherheit)	- Inventar - Härtung - Schwachstellenmanagement - Monitoring - Incident Response - MFA
Zielgruppen	Betreiber, Integratoren, Hersteller industrieller Systeme	Organisationen, die ein ISMS betreiben oder zertifizieren wollen	IT-Teams, KMU, Unternehmen ohne großes Sicherheitsprogramm
Reifegrad / Komplexität	Hoch, technisch spezifisch für OT	Hoch, organisatorisch/strategisch	Mittel – schnell umsetzbare technische Maßnahmen
Zertifizier-barkeit	Teilweise (z. B. 62443-2-4, 62443-3-3)	Ja	Nein, aber auditfähig

AGENDA

1. Herausforderungen
2. Regulatorische Anforderungen
3. Interaktive Session: **Use Cases & Lösungsansätze**
4. Fazit & Ausblick

Priorisierte Use Cases



Use Case - Vernetzte Gebäudetechnik (HLK, Zutrittskontrolle, Video) im gleichen Netz wie OT

Beschreibung
- IT- und OT- und Gebäudetechnik-Netz wurden aus Kostengründen zusammengelegt oder schlecht segmentiert

Bedrohung (Auszug)
- Angreifer knackt einfache IP-Kamera oder Smarte Thermostate → Pivot in die Prod

Schwachstellen (Auszug)
- Flache Netzwerkarchitektur („Flat Network“)
- IoT-Geräte mit bekannten Default-Credentials

Mögliche Lösungsansätze
- **Netzwerksegmentierung & Zonenmodell**
  - Trennung von OT, HLK, und IT in separate VLANs oder physische Segmente
  - Einsatz von Firewalls oder Layer-3-Switches (nur notwendige Protokolle)
  - Orientierung an IEC 62443-Zonen- und Conduit-Konzept
- **Zero Trust & Zugriffskontrolle**
  - Kontinuierliches Asset Discovery und Anomalieerkennung → Claroty
  - Authentifizierung aller Geräte (z. B. 802.1X, Zertifikate)
  - Rollenbasierte Zugriffskontrolle für Management-Interfaces
  - Keine Default-Passwörter, starke Passwortrichtlinien
- **Protokoll-Härtung**
  - Deaktivierung unsicherer Protokolle (z. B. Telnet, SNMPv1)
  - Nutzung verschlüsselter Kommunikation (TLS, VPN für Remote-Zugriffe)
- Regelmäßige Pen-Tests mit Red-/Purple-Teaming speziell für konvergente Netze
- Monitoring & Anomalieerkennung
- **Patch- und Update-Management**
- **Physische Sicherheit**
  - Absicherung von Netzwerkkomponenten (Switches, Controller) gegen unbefugten Zugriff
  - Zutrittskontrolle zu Technikräumen

Organisatorische Maßnahmen
- **Risikomanagement**
- **Governance & Verantwortlichkeiten (**RACI-Matrix für OT, HLK, IT, CISO für OT/IT)
  - Definition von Sicherheitsrichtlinien für alle beteiligten Systeme
  - Incident Response & Notfallpläne
- **Dienstleistermanagement:** Sicherheitsanforderungen in Verträgen (z. B. nach IEC 62443-2-4)
- **Schulung & Awareness**

Use Case - Fernwartungszugänge

Beschreibung
- Externe Dienstleister (z.B. OEMs) erhalten VPN- oder Cloud-Zugang zur Anlage
- Wartungsfirmen greifen per VPN oder Software auf Anlagen

Bedrohung (Auszug)
- Angreifer nutzt kompromittierten Wartungsaccount ins Produktionsnetz (Supply-Chain-Angriff, siehe SolarWinds), Cloud Kompromittierung
- IoT-Sensoren überwachen Maschinenzustände (Man-in-the-Middle-Attack)

Schwachstellen (Auszug)
- Schwache/ keine MFA oder zu viele/hohe Rechte
- Immer-offene VPN-Tunnel, fehlende Sitzungsüberwachung
- Gleiche Zugangsdaten bei vielen Kunden
- Unverschlüsselte Datenübertragung
- Kaum Monitoring

Mögliche Lösungsansätze

Technologische Maßnahmen
- Zero-Trust-Fernwartungslösungen (z. B. Secure Remote Access), Jump Server, Verschlüsselung
- Session-basierte, zeitlich überwachte Zugänge mit Recording, MFA
- Just-in-Time & Just-Enough-Access, Privileged Access Management → Cyolo
- Regelmäßige Updates, Sicherheitszertifikate
- Protokoll- und Port-Restriktion
- Audits, Pentest

Organisatorische Maßnahmen
- **Risikomanagement**
- **´Genehmigungsprozess**
  - Freigabe jedes Fernwartungszugangs
  - Dokumentation des Zwecks und der Dauer
- **Vertragliche Sicherheitsanforderungen**
  - Anforderungen an Dienstleister (z. B. IEC 62443-2-4)
  - Verpflichtung zu sicheren Endgeräten und VPN-Nutzung
- **Schulung & Awareness**
- **Notfall- und Incident-Management**

Use Case - USB-Sticks und portable Wartungs-Laptops

Beschreibung
- Klassische Inbetriebnahme und Fehlerdiagnose über USB oder direkte Ethernet-Verbindung mit Engineer-Laptop
- Dienstleister nutzen Tablets/Smartphones für Arbeitsanweisungen, Tickets, Augmented Reality

Bedrohung (Auszug)
- Infizierter USB-Stick oder kompromittierter Laptop bringt Malware ein
- Infiziertes Smartphone verbindet sich mit Werks-WLAN → Malware ins OT-Netz

Schwachstellen (Auszug)
- USB-Ports an PLCs/HMIs nicht deaktiviert oder überwacht
- Keine Whitelisting von autorisierten Wartungsgeräten
- Kein separates Gast-WLAN für mobile Geräte
- Bluetooth in Nähe von Maschinen

Mögliche Lösungsansätze

Technologische Maßnahmen
- USB Device Control /Encryption / Port Security
- Hardened Maintenance Laptop
- Physische / SW-basierte USB-Port-Sperren + zentrale Freigabe
- Endpoint Detection & Response (EDR) auf allen Wartungsrechnern
- Digitale Signatur und Hash-Check von Engineering-Dateien
- Dediziertes, segmentiertes „Mobile-OT-WLAN“ mit NAC
- MDM mit App-Whitelisting und Remote-Wipe
- Deaktivierung nicht benötigter Funkstandards in der Halle
- Audits, Pentest
- Logging/ Monitoring

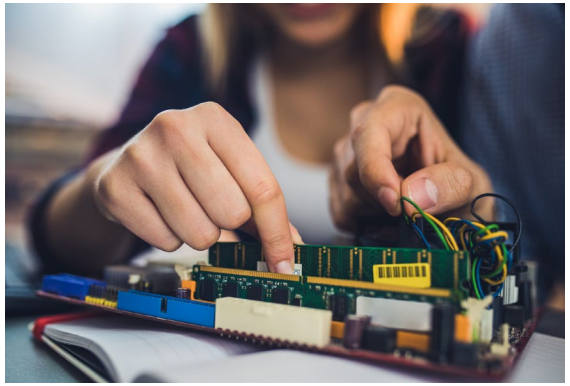
Organisatorische Maßnahmen
- **Risikomanagement**
- **IAM**
  - Klare Policies für Nutzung von USB & Wartungsgeräten
  - Inventarisierung & Lifecycle-Management
  - Freigabeprozess für Software und Daten
  - Dokumentation des Zwecks und der Dauer
- **Vertragliche Sicherheitsanforderungen**
  - Anforderungen an Dienstleister (z. B. IEC 62443-2-4)
  - Verpflichtung zu sicheren Endgeräten und VPN-Nutzung
- **Schulung & Awareness**
- **Notfall- und Incident-Management**

Use Case – Altsysteme/Legacy

Beschreibung
- Steuerungen und HMI-Systeme aus den 2000er-Jahren noch im Einsatz
- Legacy-PLC & Windows XP/7 in der Fertigung
- Keine Sicherheits-Updates mehr vom Hersteller verfügbar

Bedrohung (Auszug)
- Kompromittierung über Ransomware oder gezielte APT-Angriffe
- Kompletter Produktionsstillstand möglich

Schwachstellen (Auszug)
- Veraltete Betriebssysteme ohne Patch-Management
- Direkte Anbindung ans Werksnetz oder sogar Internet (Fernwartung)
- Standard-/leere Passwörter



Mögliche Lösungsansätze

Technologische Maßnahmen:
- Air-Gapped Micro-Segmentierung (z. B. Industrial Firewalls/ Datendioden)
- Virtuelles Patching & Application Whitelisting
- Austauschplanung + schrittweise Migration mit OT-Security-by-Design
- Hardening
- Hardware Root of Trust: Vertrauensanker in der Hardware
- Legacy-Systeme in separate, isolierte Netzsegmente
- Minimale Kommunikationspfade (Least Connectivity)
- IAM: Keine lokalen Adminrechte (sofern möglich), Multi-Faktor-Authentifizierung für Fernzugriffe, Jump-Server/Zugangsproxy für externe Wartung
- Redundanz & Ausfallsicherheit
- Backup & Recovery

Organisatorische Maßnahmen
- Risikomanagement & Legacy Inventar
- Lifecycle Management
- Incident Response & Business Continuity
- Change Management
- Schulung & Awareness

Use Case - Cloud-Anbindung der Produktion (MES/ERP in Azure/AWS)

Beschreibung
- Produktionsdaten werden in Echtzeit in die Cloud gespiegelt (Industrie 4.0)
- Direkte API-Anbindung oder Site-to-Site-VPN

Bedrohung (Auszug)
- Cloud-Konto wird gehackt → Angreifer kann Produktionsparameter verändern oder Sabotage durchführen

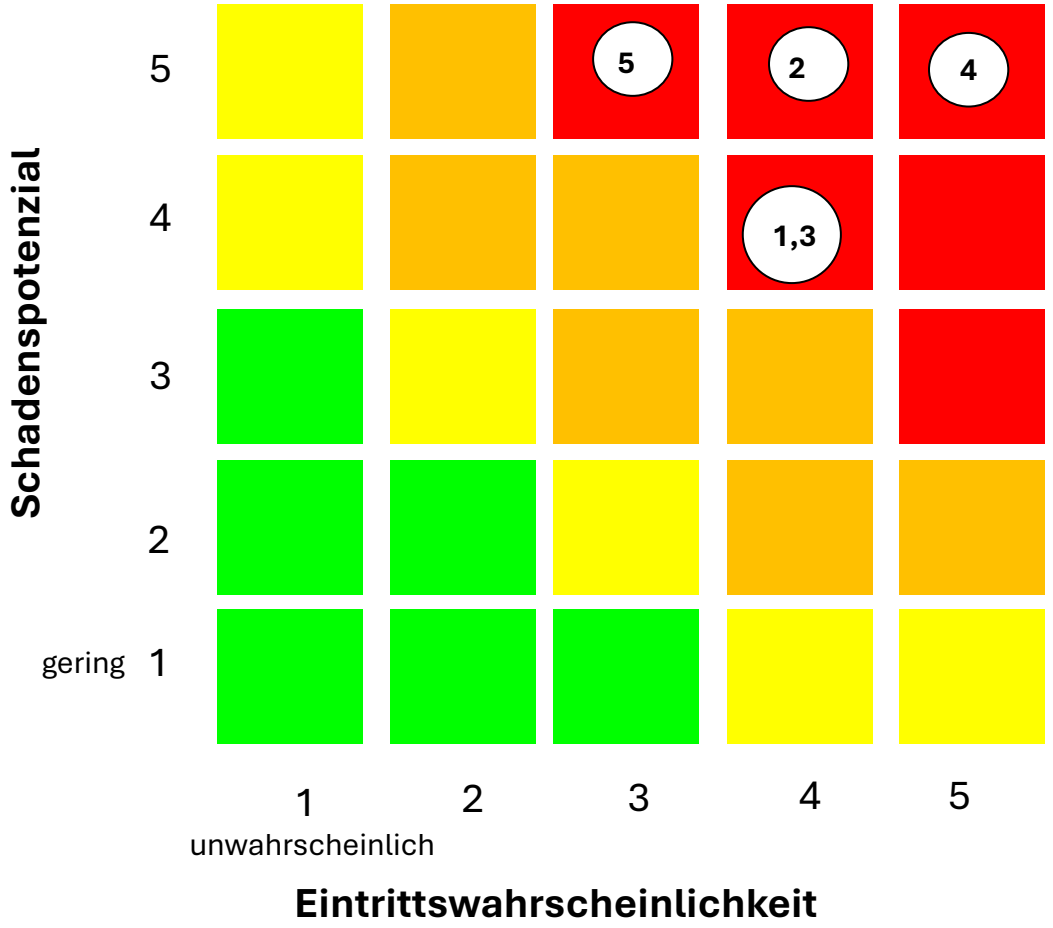
Schwachstellen (Auszug)
- Übermäßige Berechtigungen der Service-Accounts
- Fehlende Verschlüsselung kritischer Steuerbefehle

Mögliche Lösungsansätze

Technologische Maßnahmen
- Trennung von OT, IT und Cloud über DMZ/Zonen wie:
  - OT-Control Zone, Separate OT-Cloud-Tenant mit eigenen Security-Controls
  - Uni-direktionale Datenübertragung (Datendioden oder MQTT mit nur Publish-Rechten)
- Zero Trust Connectivity
  - mTLS zwischen Edge und Cloud
  - Geräte-Identitäten (X.509, TPM-basierte IDs), Transaktionssignierung und Command Whitelisting auf Leitrechner-Ebene
  - Least Privilege für alle Cloud-Ressourcen mit IAM (Azure AD, AWS IAM)
  - Keine statischen Keys (nur Managed Identities / IAM Roles)
- Monitoring & Detection
- Protokoll- und API-Härtung
- Pentesting & Audits
- Patch- und Update-Management
- **Redundanz & Ausfallsicherheit (**Edge-Gateway-Cluster, Lokale Caches für MES/ERP-Funktion bei Cloud-Ausfall)
- **Datensicherheit**
  - Verschlüsselung: (At Rest: Cloud KMS (AES-256), In Transit: TLS 1.2/1.3)
  - Data Loss Prevention (DLP) für Produktion
  - Backup & Recovery

Organisatorische Maßnahmen
- Risikomanagement
- Governance & Verantwortlichkeiten
- Incident Response & Business Continuity
- Change & Releasemanagement
- Dienstleistermanagement: Sicherheitsanforderungen in Verträgen (z. B. nach IEC 62443-2-4)
- Schulung & Awareness

Risikobewertung (Beispiel)



Risikobewertung

1: Use Case Gebäudetechnik → Risiko 16

2: Use Case Fernwartung → Risiko 20

3: Use Case USB → Risiko 16

4: Use Case Altsysteme → Risiko 25

5: Use Case Cloud→ Risiko 15 -20

- Kleines Risiko, keine Maßnahmen nötig
- Mittleres Risiko, Maßnahmen zur Risikominimierung prüfen
- Hohes Risiko, Maßnahmen zur Risikominimierung erforderlich
- Risiko nicht akzeptabel, Maßnahmen zur Risikominimierung zwingend

AGENDA

1. Herausforderungen
2. Regulatorische Anforderungen
3. Use Cases & Lösungsansätze
4. **Fazit & Ausblick**

4. Fazit

Chancen und Risiken der Vernetzung
Die Vernetzung in der Produktion eröffnet große Chancen, bringt aber auch erhebliche Sicherheitsrisiken mit sich, die Unternehmen beachten müssen

Proaktive Sicherheitsstrategie
Unternehmen sollten technische, organisatorische und regulatorische Sicherheitsmaßnahmen integrieren, um Bedrohungen effektiv zu begegnen

Compliance als Wettbewerbsvorteil
Die Einhaltung von NIS2, CRA, MVO und DSGVO ist gesetzlich verpflichtend und stärkt gleichzeitig die Marktposition von Unternehmen

Best Practices für Sicherheit
Zero Trust und Security by Design minimieren Angriffsflächen und erhöhen die Resilienz gegenüber Cyberangriffen

Investition in Zukunft
Sicherheitsinvestitionen schützen Systeme und sichern die Zukunft der Produktion.

- NIST PQC Algorithmen (Kyber, Dilithium)
- KI-basierte Threat Hunting in Echtzeit
- Digitaler Zwilling für Sicherheits-Simulation
- AI Robotics

Resilienz durch Design

Checkliste

1. Governance & Risikomanagement (Standards nutzen)
2. Asset-Inventar führen
3. Netzwerk segmentieren
4. IAM, Multifaktor für alle Zugänge, Zero Trust
5. Patch-Management auch für OT
6. Secure by Design/ Default Architektur
   - Level 0: Sensor/Aktor (Secure Element)
   - Level 1: Edge-Gateway (OPC UA, TSN)
   - Level 2: Fog/Cloud (SBOM, Zero-Trust)
   - Level 3: SIEM (Splunk/Elastic)
7. Incident Management / 24h-Vorfall-Meldeprozess
8. Monitoring / Schwachstellenmanagement
9. Lieferanten auditieren
10. Security Awareness, Schulungen
11. Regelmäßige Penetrationstests (OT-Red/Blue-Team)
12. Notfallplan üben (jährlich!)

Sicherheit in der OT / IIoT ist kein einmaliges Projekt, sondern ein kontinuierlicher Prozess, der Technologie, Prozesse und Menschen gleichermaßen umfassen muss.

BearingPoint

Vielen Dank.

BearingPoint
Caroline Neufert, Senior Manager
Tel. +49 174.335 1127
Mail Caroline.Neufert@bearingpoint.com

BearingPoint
Alexander Schwemberger, Sales Manager
Tel. +43 664 8831 8503
Mail Alexander-Schwemberger@bearingpoint.com