Der Arbeitskreis Industrial IT-Security wurde im Herbst 2017 gegründet. Er bietet eine interdisziplinäre Plattform zum regelmäßigen Austausch Security-relevanter Themen für interessierte Stakeholder aus IT und OT/Industrie. Dabei stehen ein vertrauensvoller Erfahrungsaustausch, Wissenstransfer und -aufbau im Fokus. Ein besonderer Schwerpunkt liegt auf Anwendungsfällen aus der Praxis, der Bearbeitung von Problemstellungen in Unternehmen und der Erarbeitung gemeinsamer Konzepte für alle sicherheitsrelevanten Herausforderungen der Industrie. Der Arbeitskreis wird von saarland.innovation&standort e.V. organisiert und steht unter der fachlichen Leitung der K4 DIGITAL.

Ziel des Arbeitskreises ist es, Erfahrungen zu teilen und Best-Practices zu erarbeiten. Er dient gleichzeitig zur Schaffung von Awareness und Wissenstransfer für interessierte Firmen der Region, z. B. durch Veröffentlichungen.

K4 DIGITAL · Energie SaarLorLux · Nemak Innovative Lightweighting · RHENUS AUTOMOTIVE · TLT-Turbo · SHS - STAHL-HOLDING-SAAR · HYDAC · EVS

Kontakt

saarland.innovation&standort e. V.
Sabine Betzholz-Schlüter
Franz-Josef-Röder-Straße 9
66119 Saarbrücken

Telefon: 0681 9520-474
Telefax: 0681 5846125
E-Mail: sabine.betzholz-schlueter@saaris.de
Internet: ikt.saarland/leistungen/cyber-security/

Diese Publikation ist ein gemeinsames Ergebnis des Arbeitskreises Industrial IT-Security.

saaris / ikt. saarland
saarland.innovation&standort e.V.

Wettbewerbsfaktor Industrial Cyber Security

Vom Chaos zu Security 4.0

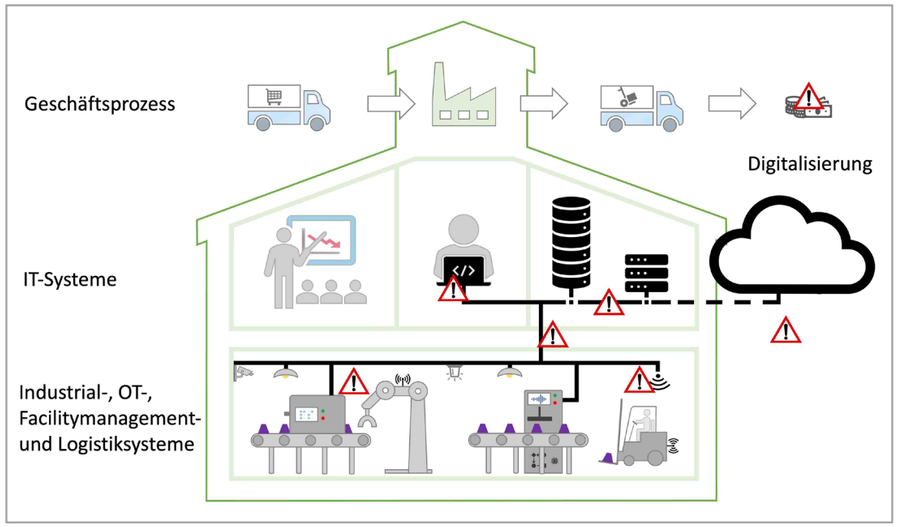
Ministerium für Wirtschaft, Innovation, Digitales und Energie
SAARLAND

BIG PICTURE – Industrie im Wandel ist eine Aufgabe der Geschäftsführung

Die Zukunftsfähigkeit und Wettbewerbsfähigkeit von Unternehmen verlangen digitale Geschäftsmodelle. Geschäftserfolg und Geschäftsziele hängen damit wesentlich von der IT-Sicherheit ab. Betrachtet man die stetig zunehmende Bedeutung von IT in den Produktionsprozessen (Industrial- oder Operational-IT, nachstehend OT), gilt dies insbesondere für die Anlagen, Maschinen und Sensoren. Sie werden durch vernetzte Kommunikation und Datenspeicherung in der Cloud zu smarten Maschinen/cyberphysischen Systemen und damit Bestandteil des Internet der Dinge (IoT). Entscheider stehen vor dramatisch veränderten Herausforderungen, da die aktuellen Security Konzepte der IT den entstehenden OT-Anforderungen nicht gerecht werden. Insellösungen sind nicht zielführend.

Übergreifende, gemeinsame Lösungsansätze sind von essenzieller Bedeutung. Kritische Erfolgsfaktoren für einen ganzheitlichen Schutz sind die Handlungsfelder Mensch, Organisation, Prozesse und Technologie und deren Zusammenwirken miteinander.

Digitalisierung erfordert eine durchgehende Vernetzung von Geschäftsprozessen bis zu Herstellungs- und Lieferketten. Dadurch wird das Gesamtsystem fehleranfälliger. Ehemals unkritische Komponenten können zu massiven Störungen der Wertschöpfungskette führen.



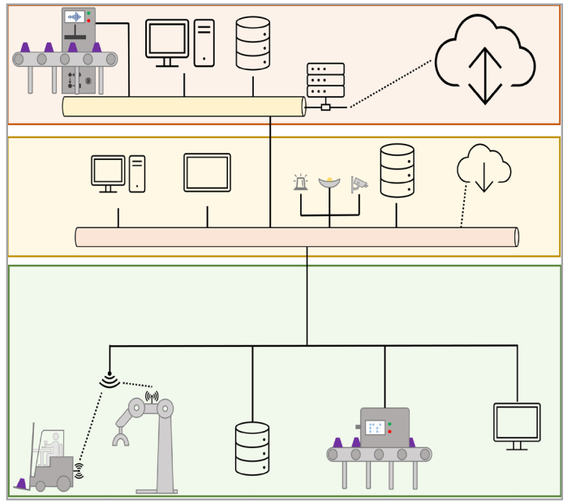
Eine besondere Bedeutung kommt dem Design der Infrastruktur zu, die allen Anforderungen der verschiedenen Handlungsfelder gerecht werden muss. Teilaspekte der Security finden sich in den aufgezeigten Bereichen wieder. Durch das Zusammenwachsen und im Sinne einer ganzheitlichen Betrachtung ist die Gesamtverantwortung eindeutig eine Geschäftsführeraufgabe. Es entstehen Anforderungen

- durch regulatorische Rahmenbedingungen, wie z.B. IT-Sicherheitsgesetz 2.0 oder branchenrelevante Vorgaben (KRITIS),
- durch Störfallverordnung KAS 51,
- an Safety (Betriebssicherheit),
- durch und an die Digitalisierung der Wertschöpfungsketten (Anforderungen an die Lieferketten).

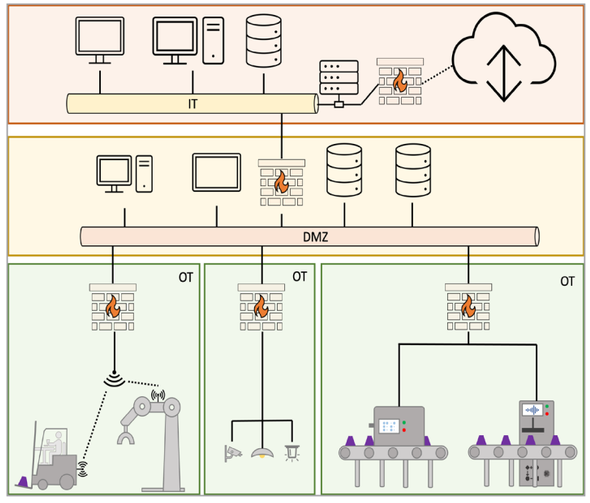
Diese müssen dem Stand der Technik u.a. zur Reduzierung möglicher Haftungsrisiken oder zur Aufrechterhaltung des Versicherungsschutzes genügen.

Vom Chaos zur geordneten Struktur

Voraussetzung für wirksame IT-Sicherheit



Die unterschiedlichen Prozessanforderungen von Unternehmen finden sich oft nicht in der technischen Netzwerkstruktur wieder. Durch unzureichende Prozess-Segmentierung steigt das Risiko enorm, bereits durch einen Vorfall hohen wirtschaftlichen Schaden oder Reputationsverlust auszulösen.



Diese Risiken können durch geeignete Strukturierung und Zonierung gemäß der IEC 62443 (zones and conduits) reduziert werden. Daraus ergibt sich als Beispiel die im rechten Bild dargestellte Referenzarchitektur.

Empfehlungen für eine Best-Practice-Referenzarchitektur

1. Identifikation & Dokumentation der IT-Assets & Systeme – Was ich nicht kenne, kann ich nicht schützen!
2. Zuordnung zu den Geschäftsprozessen herstellen und Bedeutung für diese bewerten – Was sind meine Kronjuwelen?
3. Risikominimierung durch Security Maßnahmen gestalten – Zeit und Geld sinnvoll investieren!
   - OT-DMZ (Demilitarisierte Zone), Prozess-Segmentierung (zones & conduits)
   - Endpoint Protection
   - Monitoring
   - etc.

   Zu beachten ist dabei, dass Security Maßnahmen im Kontext eines passenden Betriebskonzeptes für das jeweilige Unternehmen ausgewählt werden!

Die umgesetzten Security Maßnahmen müssen kontinuierlich auf Wirksamkeit geprüft und in einem kontinuierlichen Verbesserungsprozess (KVP) nachgeschärft oder angepasst werden.

Security ist kein Selbstzweck, sondern Sicherung der Zukunfts- und Wettbewerbsfähigkeit von Unternehmen.