Der Arbeitskreis wurde im Herbst 2017 gegründet. Er bietet IT-Leitern und IT-Fachleuten aus saarländischen Industrie- bzw. produzierenden Unternehmen eine Plattform zur Diskussion IT-sicherheitsrelevanter Themen, zum vertrauensvollen Erfahrungsaustausch und zum Wissenstransfer und -aufbau. Ein besonderer Schwerpunkt liegt dabei 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 KORAMIS GmbH.
Das vorliegende Positionspapier ist das Ergebnis intensiver Diskussionen und Erfahrungen der Mitglieder des Arbeitskreises zu einem ganzheitlichen IT-Security Ansatz mit dem Mensch als Schlüsselfaktor.

KORAMIS · Nemak · Energie SaarLorLux · SHS - STAHL-HOLDING-SAAR · ZF · Gusswerke Saarbrücken

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

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

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

Positionspapier des Arbeitskreises Industrial IT-Security

Digitalisierung und Security in der Industrie – kein Widerspruch!

Europäische Union
EUROPÄISCHER FONDS FÜR REGIONALE ENTWICKLUNG

Staatskanzlei SAARLAND

Awareness

Grundlegende Voraussetzung für IT-Sicherheit

Geschäftserfolg und Geschäftsziele hängen, bedingt durch die fortschreitende Digitalisierung, zunehmend von der IT-Sicherheit ab. Betrachtet man die stetig zunehmende Bedeutung von IT in den Produktionsprozessen (Operational IT-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). Damit einher geht die Verknüpfung mit der klassischen IT in der Unternehmensverwaltung, wie beispielsweise. ERP, CRM, MES. Das dadurch steigende potenzielle Risiko von Cyber-Angriffen verlangt einen Schutz der gesamten Infrastruktur.

Grundlegende Anforderungen, um sich vor Cybergefahren zu schützen

- Die Geschäftsleitung gibt Sicherheitsziele in Form einer Leitlinie vor.
- Das Management erklärt sein Commitment mit den in der Leitlinie formulierten Zielen.
- Die Verfügbarkeit und Widerstandsfähigkeit von Produktionsanlagen, insbesondere der industriellen Steuerung, ist gewährleistet.
- Produktionsrelevante Daten sind vor Manipulation geschützt.
- Es ist sichergestellt, dass schützenswerte Informationen und Daten nicht in falsche Hände gelangen.

Schlüsselfaktor bei der IT-Sicherheit ist der Mensch

- Technik alleine reicht nicht aus - Schlüsselfaktor ist der Mensch
- Awareness/Sensibilisierung im Thema IT Sicherheit – signifikante Verbesserung mit moderatem Aufwand
- Führungs- und Unternehmenskultur – mit gutem Beispiel vorangehen

Im Rahmen des Arbeitskreises „Industrial IT-Security“ sind wir zu der Überzeugung gelangt, dass diese Sicherheitsziele nur im Rahmen eines ganzheitlichen Top-Down-Ansatzes zu erreichen sind.

Bei der Umsetzung ist zu berücksichtigen, dass die Sicherheitsziele NICHT alleine durch technische Maßnahmen und Vorkehrungen erreichbar sind. Der Schlüsselfaktor in einem wirksamen Sicherheitskonzept ist der Mensch, der als Anwender und Umsetzer die vorhandenen Systeme bedient und unter Umständen in diese eingreift.

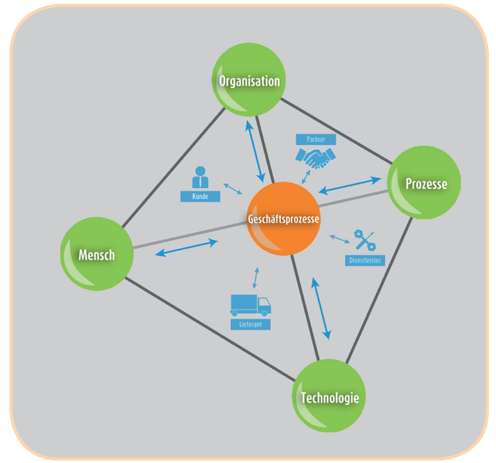
Daher ist dringend zu empfehlen den Faktor Mensch, also bei den Mitarbeitern ein Bewusstsein und eine Sensibilisierung im Hinblick auf das Thema IT-Sicherheit zu schaffen. Diese Awareness ist dabei in der Regel mit moderatem Aufwand umsetzbar und schafft gleichzeitig eine signifikante Verbesserung im Bereich IT-Sicherheit.

Damit Awareness oder das Bewusstsein für IT-Sicherheit zum Teil der Unternehmenskultur wird, ist es zwingend erforderlich, dass die Führungsebene hier mit gutem Beispiel vorangeht und die in der Sicherheitsleitlinie formulierten Ziele sowie die daraus abgeleiteten Maßnahmen in ihrem Handeln vorlebt.

Ganzheitlicher Security Ansatz

Voraussetzung für wirksame IT-Sicherheit

Der Arbeitskreis „Industrial Security“ propagiert einen ganzheitlichen Ansatz, der Organisation – Prozesse – Technologie und Mensch betrachtet.
Dazu gehört auch die Berücksichtigung der Wertschöpfungskette vom Hersteller über den Integrator bis hin zum Betreiber.
Der empfohlene Ansatz findet sich unter anderem in der Norm IEC 62443 wieder und basiert auf sieben Säulen.



Die sieben Säulen

- Zugang zu Systemen und Anlagen muss reguliert werden.
- Änderungen und Anpassungen müssen nachvollziehbar sein.
- Produktionsprozesse und Daten müssen vor Manipulationen geschützt werden.
- Produktions- und Know-how Daten müssen gegen Missbrauch geschützt werden. Eine Klassifikation von Daten ist dabei hilfreich.
- Übertragung von Daten erfolgt nach Minimalprinzip. Es werden nur Daten zur Verfügung gestellt, die tatsächlich benötigt werden.
- Störungen und Vorfälle müssen unverzüglich erkannt, behoben und dokumentiert werden.
- Das notwendige Personal, Kompetenzen und die benötigen Ressourcen müssen vorhanden sein.

Vorgehensweise zur Umsetzung einer optimierten IT-Sicherheit

Zur Erreichung der Ziele sind geeignete technische und organisatorische Maßnahmen auszuwählen und umzusetzen. Neben geeigneten Prozessen und einer entsprechenden Aufbauorganisation ist folgende Vorgehensweise dabei hilfreich:

- Identifikation der monetär kritischen und wichtigen Produktionsprozesse inklusive der zugeordneten IT und OT Systeme.
- Bewertung der Widerstandsfähigkeit (Resilienz) in Hinblick auf den Schutzbedarf.
- Umsetzung geeigneter Schutzmaßnahmen.
- Implementierung eines eines kontinuierlichen Verbesserungsprozesses (KVP).
- Einführung von Leistungskennzahlen (KPI) zur Erfolgskontrolle von Maßnahmen.

Praxistipps

Aus der praktischen Erfahrung und wirtschaftlicher Sicht empfiehlt sich eine angemessene, gleichmäßige Bearbeitung aller Anforderungen (Pareto Prinzip 80:20).
Die Menschen müssen die technischen und organisatorischen Rahmenbedingungen, sowie die daraus resultierenden Prozesse kennen, verstehen und anwenden.
Dazu sind folgende Punkte unabdingbar:

Regelmäßige Sensibilisierungsmaßnahmen

- Pflichtveranstaltungen für Neueinstellungen
- Ansprechen von Security in Abteilungsmeetings
- Regelmäßige Infos in und über interne Kommunikationskanäle
- Informationen auf Unternehmens/Mitarbeiter-Monitoren
- Intranet
- Newsletter

Regelmäßige Weiterqualifikation

- Technologische Weiterentwicklung
- Best Practice und Methodenkompetenz