Repository of Hochschule Hannover

HOCHSCHULE
HANNOVER
UNIVERSITY OF
APPLIED SCIENCES
AND ARTS

IT-Sicherheit in Produktionsanlagen - Eine Einführung in die OT-Security für kleine und mittlere Unternehmen - 2. vollständig überarbeitete Auflage

Karl-Heinz Niemann

Suggested citation:

Niemann, Karl-Heinz. 2025. "IT-Sicherheit in Produktionsanlagen - Eine Einführung in die OT-Security für kleine und mittlere Unternehmen - 2. vollständig überarbeitete Auflage." 2nd ed. Hannover: Hochschule Hannover. https://doi.org/10.25968/opus-4009.

Abstract

Die erste Ausgabe dieses Whitepapers geht zurück auf das Jahr 2016. Viele Dinge haben sich seitdem geändert. So hat sich für die „IT-Sicherheit in Produktions-anlagen" der Begriff „OT-Security" etabliert. Dieses Dokument trägt noch die Titel der ersten Version, da es sich um eine Neuauflage handelt. Dennoch wir im Dokument der Begriff „OT-Security" verwendet. Aber es ist noch mehr passiert. Die Norm IEC 62443 entstand und entsteht noch immer. Der Gesetzgeber hat mit neuen Vorgaben wie NIS2-Richtlinie, CER-Richtlinie, Cyber-Resilience-Act und Maschinenverordnung Planern, Betreibern und Herstellern neue Aufgaben beschert. Cyber-Vorfälle werden häufiger, auch in der Produktion. Der Begriff OT-Security entsteht. Demografischer Wan-del und geändertes Studierverhalten junger Menschen erzeugen Lücken in den Projektabteilungen, die sich wahrscheinlich auch nicht schnell wieder schließen lassen.

Gerade für KMU entstehen so neue Herausforderungen. Die Erfüllung wachsender Anforderungen bei verschärfter Bedrohungslage und schrumpfender Belegschaft. Dieses Whitepaper soll diese Unternehmen bei der täglichen Arbeit im Bereich der OT-Security unterstützen und Wege für eine an die Unternehmensgröße angepasste OT-Security aufzeigen.

Ich freue mich, dass ich Ihnen nach nunmehr fast zehn Jahren eine aktualisierte Fassung des Whitepapers vorlegen kann. Der Firma Wago GmbH & Co. KG danke ich für die Unterstützung bei Erstellung dieses Dokuments und für die anregende Diskussion und die geduldige Kommentierung der Entwürfe.

Terms of use **UrhG**

This document is made available under these conditions:
Urheberrechtlich geschützt
For more information see:
https://rightsstatements.org/page/InC/1.0/

IT-Sicherheit in Produktionsanlagen

Eine Einführung in die OT-Security für kleine und mittlere Unternehmen

2. vollständig überarbeitete Auflage

Prof. Dr. Karl-Heinz Niemann – Hochschule Hannover
in Kooperation mit der Wago GmbH & Co. KG

Autor:
Prof. Dr. Karl-Heinz Niemann
Email: Karl-Heinz.Niemann@Hs-Hannover.de
ORCID ID: https://orcid.org/0000-0001-8931-6789

DOI: https://doi.org/10.25968/opus-4009

© 2025 WAGO GmbH & Co. KG Alle Rechte vorbehalten.

WAGO GmbH & Co. KG
Hansastraße 27
D-32423 Minden

Tel.: +49 (0) 571/8 87 – 0
Fax: +49 (0) 571/8 87 – 1 69
E-Mail: info@wago.com
Web: www.wago.com

Haftungsausschluss: Die diesem Dokument zu Grunde liegenden Informationen wurden mit größtmöglicher Sorgfalt recherchiert zusammengestellt. Dennoch wird dieses ohne eine Gewährleistung zur Verfügung gestellt. Der Autor lehnt ausdrücklich jede Art von vertraglicher oder gesetzlicher Haftung für dieses Dokument ab. In keinem Fall ist der Autor für Schäden verantwortlich, die durch Fehler oder fehlende Informationen in diesem Dokument entstehen könnten. Logos und Markennamen werden ohne Hinweis auf ggf. bestehende Schutzrechte verwendet.

Vorwort des Autors

Liebe Leser,

die erste Ausgabe dieses Whitepapers geht zurück auf das Jahr 2016 [NIE2017]. Viele Dinge haben sich seitdem geändert. So hat sich für die „IT-Sicherheit in Produktionsanlagen“ der Begriff „OT-Security“ etabliert. Dieses Dokument trägt noch die Titel der ersten Version, da es sich um eine Neuauflage handelt. Dennoch wir im Dokument der Begriff „OT-Security“ verwendet. Aber es ist noch mehr passiert. Die Norm IEC 62443 entstand und entsteht noch immer. Der Gesetzgeber hat mit neuen Vorgaben wie NIS2-Richtlinie, CER-Richtlinie, Cyber-Resilience-Act und Maschinenverordnung Planern, Betreibern und Herstellern neue Aufgaben beschert. Cyber-Vorfälle werden häufiger, auch in der Produktion. Der Begriff OT-Security entsteht. Demografischer Wandel und geändertes Studierverhalten junger Menschen erzeugen Lücken in den Projektabteilungen, die sich wahrscheinlich auch nicht schnell wieder schließen lassen.

Gerade für KMU entstehen so neue Herausforderungen. Die Erfüllung wachsender Anforderungen bei verschärfter Bedrohungslage und schrumpfender Belegschaft. Dieses Whitepaper soll diese Unternehmen bei der täglichen Arbeit im Bereich der OT-Security unterstützen und Wege für eine an die Unternehmensgröße angepasste OT-Security aufzeigen.

Ich freue mich, dass ich Ihnen nach nunmehr fast zehn Jahren eine aktualisierte Fassung des Whitepapers vorlegen kann. Der Firma Wago GmbH & Co. KG danke ich für die Unterstützung bei Erstellung dieses Dokuments und für die anregende Diskussion und die geduldige Kommentierung der Entwürfe.

Hannover im September 2025

Inhaltsverzeichnis

1. Einführung 6
2. Der aktuelle Stand der OT-Security 7
   2.1. Bekannte Sicherheitsvorfälle in Produktionsanlagen 7
   2.2. Künftige Herausforderungen an die OT-Security in der Produktion 9
   2.3. Handlungsfelder in Bezug auf die OT-Security in der Produktion 11
3. Normen, Standards, Richtlinien 14
   3.1. Normen und Standards für den Office Bereich (IT-Security) 15
   3.2. Normen und Standards für den Produktionsbereich (OT-Security) 16
      3.2.1. IEC 62443 Normreihe 17
      3.2.2. VDI/VDE Normreihe 2182 21
      3.2.3. VdS 10020 24
      3.2.4. Leitlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) 24
      3.2.5. Leitlinien von Herstellerorganisationen 25
      3.2.6. Normen für den maritimen Sektor 25
      3.2.7. Sonstige branchenspezifische Normen 26
      3.2.8. Zusammenfassung Normen und Standards 26
4. Rechtliche Vorgaben 28
   4.1. Vorgaben auf EU-Ebene 28
      4.1.1. CER-Richtlinie 28
      4.1.2. NIS-Richtlinie 29
      4.1.3. NIS2-Richtlinie 29
      4.1.4. Cyber-Resilience-Act 31
      4.1.5. Maschinenverordnung 32
   4.2. Nationale deutsche Vorgaben 32
      4.2.1. IT-Sicherheitsgesetz und BSI Kritisverordnung 33
      4.2.2. KRITIS-Dachgesetz 34
      4.2.3. NIS2-Umsetzungsgesetz 34
5. Maßnahmen zur Umsetzung der OT-Security in der Produktion 35
   5.1. Management Commitment 35
   5.2. Organisation der Zuständigkeiten und Prozesse 36
   5.3. Erstellung von Richtlinien 37
   5.4. Personal 37
   5.5. Beschaffung und Bereitstellung von Wissen 38
   5.6. Identifizierung, Bewertung und Schutz der Assets 39
   5.7. Regelung des externen Zugriffs auf Produktionsanlagen 44
   5.8. Datensicherung 46
   5.9. Behandlung von Störungen und Ausfällen 47

5.10. OT-Security-Vorfälle erkennen 48
6. Ausblick 49
7. Abbildungsverzeichnis 51
8. Tabellenverzeichnis 52
9. Index 53
10. Literaturverzeichnis 55

1. Einführung

Als dieses Dokument in seiner ersten Auflage vor neun Jahren erschien, wurde noch der Begriff „IT-Sicherheit in Produktionsanlagen“ als Titel gewählt. In der Zwischenzeit haben sich neue Begriffe wie Cyber-Security, Industrial Security, ICS-Security aber auch OT-Security etabliert. In diesem Dokument wird der Begriff „OT-Security“ verwendet, um das Anwendungsgebiet klar zu kennzeichnen. Unter OT versteht man die „Operational Technology“, welche die Automatisierungskomponenten und Netzwerke umfasst.

Zielgruppe dieses Dokuments sind kleine und mittlere Unternehmen (KMU), welche auf der Suche nach einem einfachen und skalierbaren Vorgehensmodell für die Sicherstellung der OT-Security in ihrem Produktionsbereich sind.

Um Leser für die Notwendigkeit der OT-Security zu sensibilisieren, werden in Kapitel 2 Sicherheitsvorfälle dargestellt, welche Produktionsanlagen betreffen. Es zeigt sich, dass Cyber-Angriffe auf Produktionsanlagen heute kein Zufall mehr sind, sondern auf einem gezielten Vorgehen beruhen. Darüber hinaus sind viele Vorfälle auch Nebeneffekte aus Angriffen auf die IT des Unternehmens, die sich in den Bereich der Produktion ausgebreitet haben.

Danach folgt in Kapitel 3 ein Überblick über die wichtigsten Normen und Empfehlungen zum Themenfeld „OT-Security“.

Kapitel 5 entwickelt anhand eines Zehn-Punkte-Plans ein Konzept für den Aufbau eines OT-Security-Systems für kleine und mittlere Unternehmen (KMU). Dabei liegt der Schwerpunkt nicht nur auf den technischen, sondern insbesondere auch auf den häufig vernachlässigten organisatorischen Maßnahmen.

Kapitel 4 gibt einen Überblick über die Anforderungen, die sich aus der EU- und der nationalen Gesetzgebung ableiten. Hier sind insbesondere NIS-2-Richtlinine, CER-Richtlinie, Cyber-Resilience-Act und Maschinenverordnung zu nennen

Abschließend gibt Kapitel 6 einen Ausblick auf künftige Anforderungen und Lösungen im Kontext von der vertikalen und horizontalen Integration.

2. Der aktuelle Stand der OT-Security

Dieses Kapitel gibt einen Überblick über den aktuellen Stand der OT-Security. Ausgehend von bekannten Sicherheitsvorfällen werden die Herausforderungen für aktuelle Produktionsanlagen abgeleitet. Die Top-10-Bedrohungen des BSI dienen hierfür als Basis.

2.1. Bekannte Sicherheitsvorfälle in Produktionsanlagen

Die Anforderungen in Bezug auf die OT-Security ändern sich stetig. In der Vergangenheit waren IT-Sicherheitsvorfälle in der Produktion in der Regel „Kollateralschäden“ gewöhnlicher Schadsoftware, die eher zufällig in eine Produktionsanlage geraten ist. Einer der ersten bekannten Vorfälle dieser Art war der Befall verschiedener Werke der Firma Daimler Chrysler (heute Mercedes Benz) im Jahr 2005 durch die Schadsoftware „Zotob“ [PAK2005]. Dabei waren weltweit 13 Werke des Unternehmens betroffen. Der entstandene Schaden wurde zum damaligen Zeitpunkt auf 14 Mio. US$ geschätzt [TOF2009].

Weitere Vorfälle zeigen, dass zunehmend auch Schadsoftware zum Einsatz kommt, die sich explizit gegen Produktionsanlagen richtet. Der bisher prominenteste Fall „Stuxnet“ [FAL2011] [LAN2013] richtete sich gegen eine iranische Anreicherungsanlage für Uran. Die U.S.A und Israel werden in diesem Fall als vermutliche Urheber genannt [BRO2011]. Daneben sind weitere Vorfälle dokumentiert, die keiner staatlichen Intervention zugeordnet werden können. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) berichtet zum Beispiel von einem dedizierten Angriff auf einen Hochofen in Deutschland, der zu dessen Havarie führte [BSI2014]. Darüber hinaus existiert inzwischen Schadsoftware, die gezielt Komponenten von Automatisierungssystemen angreift. Die Schadsoftware „Industroyer“ [CHE2017] adressiert industrielle Protokolle, wie z. B.:

- IEC 60870-5-101
- IEC 60870-5-104
- IEC 61850
- OLE for Process Control Data Access (OPC DA)

Das ICS-CERT berichtet ebenfalls über eine Schadsoftware, welche OPC-Server befällt [CERT2018]. Im Jahr 2024 wird ein Angriff auf das Modbus-Protokoll durch die Gruppe FrostyGoop [GRA2024] dokumentiert.

Eine neue Dimension von Cyber-Angriffen auf Automatisierungssysteme und kritische Infrastruktur markiert ein Angriff auf das Energieversorgungssystem der Ukraine am 23.12.2015 [CERT2016]. Nahezu zeitgleich wurden drei Energieversorger angegriffen, was zu einem Ausfall der Energieversorgung für 225 000 Kunden führte. Bei dem Angriff wurden Leistungsschalter im Energieversorgungsnetz durch Remote-Zugriff unkontrolliert bedient. Gleichzeitig wurden auf Steuerungsrechnern Datenbestände gelöscht, so dass diese nicht mehr einsatzfähig waren.

Mit dem Aufkommen von Verschlüsselungstrojanern wie WannaCry und Petya/NotPetya wird Ransomware seit dem Jahr 2017 [SCH2018] zu einem bis heute andauerndem Problem für IT- und OT-Systeme. Infektionen der IT breiten sich in vielen Fällen auch in die OT aus, wie das Beispiel der Colonial Pipeline in den U.S.A gezeigt hat [CYB2020]. Ein Cyberangreifer nutzte einen Spear-Phishing-Link, eine auf eine bestimmte Person bezogene Betrugsmail, um sich zunächst Zugang zum IT-Netzwerk des Unternehmens zu verschaffen, bevor er zum OT-Netzwerk wechselte. Der Bedrohungsakteur setzte dann Ransomware ein, um Daten in beiden Netzwerken zu verschlüsseln. Zu den spezifischen Anlagen, die im OT-Netzwerk einen Verfügbarkeitsverlust erlitten, gehörten Bedien- und Beobachtungsstationen (HMI), Server zur Aufzeichnung historischer Daten und Polling-Server. Durch den Verlust der Bedienfunktion war die Pipeline nicht mehr zu betreiben und musste abgeschaltet werden.

Nach dem Angriff auf die Firma SolarWinds im Jahr 2020 [ALK2021] gewann das Thema „Sicherheit in der Lieferkette“ an Bedeutung. Bei diesem Vorfall infiltrierten Angreifer die Softwareentwicklungsprozesse des US-Unternehmens SolarWinds und bauten eine Schadsoftware namens „Sunburst“ in ein Update der Netzwerkmanagement-Plattform Orion ein. Dieses Update wurde an 18.000 Kunden weltweit ausgeliefert. Durch die Schadsoftware erhielten die Angreifer Zugang zu den IT-Systemen der Kunden [FOR2025]. In einer Studie der Firma Ottorio [OTO2022] sahen dann auch 53% der befragten Personen in einer Studie der Fa das höchste Risiko in einem Supply-Chain-Angriff. Die TÜV-Cybersecurity-Studie [TÜV2025] besagt, dass in 10 % der Vorfälle der Angriff über einen Kunden oder Lieferanten erfolgte. Der VDMA adressiert dieses Thema „Supply-Chain-Security“ über ein entsprechendes Muster-Lastenheft [VDM2023]. Weitere Informationen zum Thema „Security in der Lieferkette“ finden sich auch in [LEL2021].

Neben industriellen Automatisierungssystemen sind Komponenten der Gebäudeautomation in gleicher Art betroffen. Im Jahr 2013 wurde ein Fall dokumentiert, bei dem Heizungsanlagen ohne ausreichenden Schutz zum Zwecke der Fernwartung mit dem Internet verbunden wurden [EIK2013], [STA2013]. Durch eine mangelnde Absicherung konnten externe Personen Zugriff auf diese Anlagen erhalten. Trotz Veröffentlichung der Schwachstelle in der Fachpresse und Behebung durch den Hersteller, waren auch nach zwei Jahren noch eine große Zahl von verwundbaren Heizungsanlagen im Internet ungeschützt zugänglich [STA2015]. Die Nutzer haben die bereitgestellten Sicherheits-Updates nicht installiert, die Geräte sind weiterhin verwundbar. Die Autoren Li et al. fassen in einer Studie aus dem Jahr 2023 die Security-Situation im Bereich der Gebäudeautomation zusammen [LI2023] und berichten eine Reihe von Cyber-Vorfällen aus dem Bereich der Gebäudeautomation, wie in Abbildung 1 dargestellt.

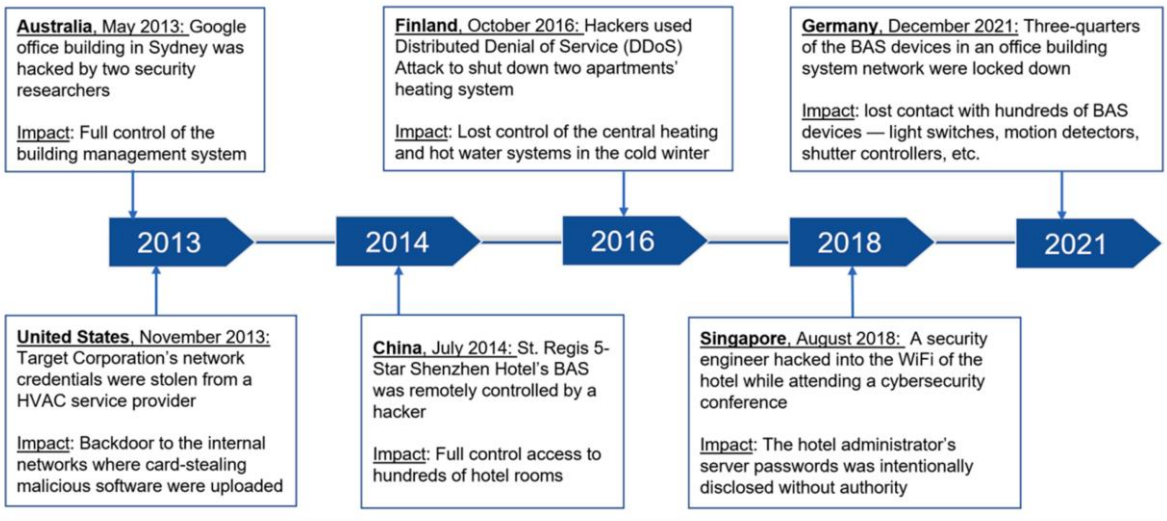

Abbildung 1: Cyber-Vorfälle aus dem Bereich der Gebäudeautomation [LI2023]

Es ist zu erkennen, dass der Bereich Gebäudeautomatisierung Ziel von Angreifern ist. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat das Thema Gebäudeautomation inzwischen im Rahmen des BSI-Grundschutzes adressiert und entsprechende Grundschutzmodule für das technische Gebäudemanagement [BSI_INF.13], [BSI_INF.13U] und die Gebäudeautomation [BSI_INF.14], [BSI_INF.14U] herausgegeben, die in der Version von 2023 vorliegen.

Auch der maritime Sektor muss sich den Herausforderungen der Cyber-Security stellen. Die auf Schiffen eingesetzten Automatisierungssysteme sind zwar für diesen speziellen Einsatzzweck ertüchtigt und zertifiziert, dennoch basieren sie in der Regel auf konventionellen Automatisierungssystemen. Somit gelten für diese Systeme die gleichen Bedrohungen, wie auch für konventionelle Automatisierungssysteme [JEN2015]. Durch zusätzliche elektronische Systeme für die Navigation und Kollisionsvermeidung wird die Angriffsfläche für potenzielle Angreifer zudem größer [DIR2015]. Eine umfassende Übersicht über Angriffe im maritimen Sektor gibt die „Maritime Cyber Attack Database“ [NHL2025]. Den zunehmenden Herausforderungen im maritimen Bereich wird im Rahmen der Klassifizierung von Schiffen durch entsprechende Standards begegnet [UR_E26], [UR_E27].

Nach diesem allgemeinen Überblick wird sich dieses Dokument im Weiteren mit produktionstechnischen Anlagen der Prozess- und der Fertigungsindustrie befassen.

2.2. Künftige Herausforderungen an die OT-Security in der Produktion

Es ist davon auszugehen, dass sich die künftige Bedrohungslage für Automatisierungssysteme weiter zuspitzen wird. Darauf weisen die Anzahl und Entwicklung im Zeitablauf der dokumentierten Angriffe hin. Die mit der Digitalisierung von Produktionsprozessen einhergehende zunehmende Vernetzung zur Realisierung einer

horizontalen und vertikalen Integration von Produktionsprozessen wird zu weiteren Angriffsmöglichkeiten führen.

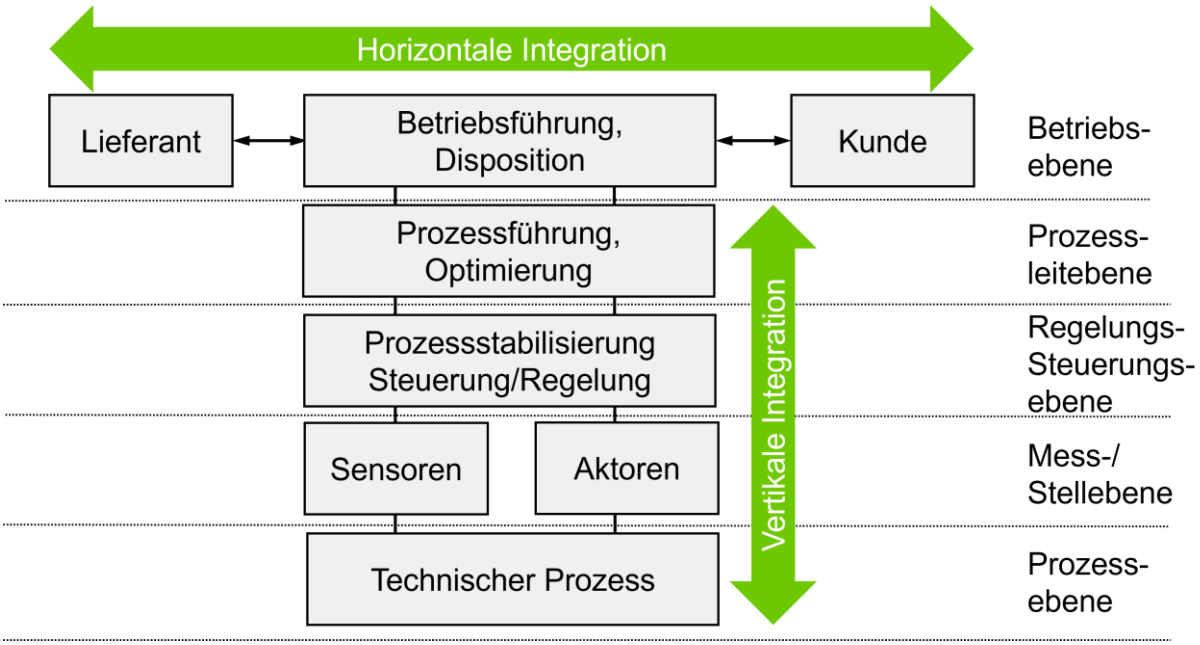

Abbildung 2: Horizontale und vertikale Integration

Abbildung 2 zeigt am Beispiel einer klassischen Automatisierungsanlage die horizontale und vertikale Integration, die im Folgenden näher erläutert werden sollen:

Horizontale Integration: Dieser Begriff beschreibt die digitale Vernetzung von Lieferketten, die über die Unternehmensgrenzen hinwegreichen. Durch diese Vernetzung erhöht sich die Angriffsfläche der beteiligten Unternehmen, da ein Datenaustausch, z. B. von Qualitätsdaten, bis in den Produktionsbereich reichen kann. Darüber hinaus spielt auch der Aspekt der Datenhoheit der beteiligten Unternehmen eine Rolle. Konzepte für einen im Sinne der OT-Security „sicheren“ Datenaustausch unter Wahrung der Datenhoheit finden sich z. B. in [KAL2024], [VOß2024], [KAL2025].

Vertikale Integration: Die vertikale Integration beschreibt die zunehmende Durchgängigkeit der industriellen Kommunikation im Produktionsbereich. In der Vergangenheit wurden Informationen, die in der Mess- und Stellebene erzeugt oder konsumiert wurden in der Steuerungs- und Regelungsebene verarbeitet. Es haben also nur benachbarte Ebenen Informationen miteinander ausgetauscht. Im Rahmen der vertikalen Integration werden nun auch Informationen aus der Mess- und Stellebene mit der Betriebsebene oder sogar mit der Cloud ausgetauscht. Dies ist z. B. der Fall, wenn ein Sensor oder Aktuator Statusinformationen oder Wartungsanforderungen mit einem Computerized-Maintenance-Management-System (CMMS) austauscht. Diese Art der Kommunikation ist aus Sicht der OT-Security kritisch, weil hier die übliche Abschottung der Ebenen nicht mehr greift. Die für die vertikale Kommunikation verwendeten Protokolle, wie z. B. OPC-UA und MQTT sind hierbei in Bezug auf ihre Security-Eigenschaften zu betrachten. Siehe hierzu auch [STE2019].

Das Bundesamt für Sicherheit in der Informationstechnik gibt in regelmäßigen Abständen eine Liste der Top-10-Bedrohungen für Automatisierungssysteme heraus. Die aktuelle Ausgabe [BSI2022b] nennt die in Tabelle 1 genannten Bedrohungen.

Tabelle 1: Top-10-Bedrohungen [BSI2022b] erweitert um Handlungsfelder

Bedrohung	Handlungsfelder
Einschleusen von Schadsoftware über Wechseldatenträger und mobile Systeme	Mensch, Prozesse
Infektion mit Schadsoftware über Internet und Intranet	Prozesse, Technik
Menschliches Fehlverhalten und Sabotage	Mensch
Kompromittierung von Extranet und Cloud-Komponenten	Prozesse, Netzwerk
Social Engineering und Phishing	Mensch, Prozesse
(D)DoS Angriffe	Netzwerk, Technik
Internet-verbundene Steuerungskomponenten	Technik
Einbruch über Fernwartungszugänge	Netzwerk, Technik
Technisches Fehlverhalten und höhere Gewalt	Netzwerk, Robustheit
Soft- und Hardwareschwachstellen in der Lieferkette	Mensch, Prozesse, Technik

Es ist zu erkennen, dass die genannten Top-10-Bedrohungen verschiedenen Angriffsarten und damit Handlungsfeldern zuzuordnen sind. Angriffe können auf verschiedenem Weg erfolgen: Z. B. über das Netzwerk, über kompromittierte Komponenten (USB-Sticks, Smartphones) aber auch über Social Engineering oder Phishing. Die Überlastung von Komponenten oder Netzwerken durch eine Flut unsinniger Anfragen (Denial of Service, Distributed Denial of Service) stellt ebenfalls eine Angriffsart dar. Basierend auf den beschriebenen Bedrohungen sollen nun im nächsten Abschnitt die Handlungsfelder für die Implementierung eines IT-Sicherheitskonzeptes für Produktionsanlagen abgeleitet werden.

2.3. Handlungsfelder in Bezug auf die OT-Security in der Produktion

Zur Verdeutlichung der Handlungsfelder hat der Autor **Fehler! Verweisquelle konnte n icht gefunden werden.** um die rechte Spalte mit Handlungsfeldern erweitert. Einzelne Themen sind einem oder mehreren Handlungsfeldern zuzuordnen, die im Folgenden kurz beschrieben werden:

- **Mensch:** Der Mensch betreibt und überwacht die Produktionsanlage und soll für deren Sicherheit sorgen. Gleichzeitig stellt der Mensch einen Schwachpunkt in Bezug auf die OT-Security dar. Über Social Engineering und Phishing kann er ungewollt Dritten einen Zugang zur Anlage ermöglichen. Im Falle von Fehlverhalten oder Sabotage kompromittiert der Mensch gewollt oder ungewollt die OT-Security der Anlage.
- **Technik**: Die eingesetzte Technik (Steuerungskomponenten, Netzwerkkomponenten) muss gegen Angriffe geschützt sein. Schwachstellen, die bekannt sind, müssen zeitnah behoben werden. Eine regelmäßige Kommunikation mit dem

Hersteller der Komponenten, z. B. durch Abonnieren von Security Advisories ist sinnvoll.

- **Prozesse**: Nicht alle Aspekte der OT-Security lassen sich über Technik lösen. In vielen Fällen sind neben der Technik entsprechende Prozesse (Regeln, Vorschriften) zu definieren. Die Mitarbeiterinnen und Mitarbeiter sind in diesen Prozessen regelmäßig zu schulen. Die Beachtung der Prozesse ist zu überwachen und ggf. auftretendes Fehlverhalten zu sanktionieren. Dadurch steht dieser Punkt in Beziehung zum Punkt „Mensch“.
- **Netzwerk**: Obwohl das Kommunikationsnetzwerk einer Produktionsanlage der Technik zuzuordnen ist, wird es hier separat genannt. Gerade das Netzwerk stellt in vielen Fällen eines der wesentlichen Einfallstore für Angriffe dar. Hier ist ein besonderes Augenmerk erforderlich, um das Produktionsnetzwerk vom Rest des Firmennetzes und insbesondere vom Internet ausreichend gut abzuschotten.
- **Robustheit:** Denial of Service Angriffe bzw. Distributed Denial of Service Angriffe werden in der Regel über das Internet gegen ein Unternehmen gerichtet und treffen zunächst den äußeren Perimeter des Unternehmens. Auch wenn ein Durchbruch eines solchen Angriffs bis zur Produktionsanlage das Durchdringen weiterer Perimeter erfordert, müssen Automatisierungssysteme dennoch eine gewisse Robustheit gegenüber Überlastsituationen aufweisen.

Die beschriebenen Handlungsfelder zeigen, dass die OT-Security kein ausschließlich technisches Problem ist. Schwachstellen können neben technischen Problemen (Schwachstelle in Software, nicht eingespielter Software-Patch) auch organisatorische Unzulänglichkeiten (Mitarbeiter wissen nicht, dass bestimmte Dinge unzulässig sind, Regelung des Zugangs zu Anlagenkomponenten) sein.

Aus dieser Sachlage kann folgender Handlungsbedarf abgeleitet werden. Das OT-Security-Konzept einer Produktionsanlage muss neben den technischen Aspekten und Aspekten der Netzwerkkommunikation auch organisatorische und soziale Aspekte (Verhalten des Menschen, Fehlverhalten des Menschen) berücksichtigen. Erst ein strukturierter und mehrstufiger Ansatz, der alle Aspekte ganzzeitlich berücksichtigt kann eine optimale Absicherung der Anlage gewährleisten. Zur Organisation der erforderlichen Prozesse ist ein so genanntes Informationssicherheitsmanagementsystem (ISMS) im Unternehmen zu etablieren. Das ISMS betrifft dabei sowohl die IT- als auch die OT. Im ISMS werden die erforderlichen Security-Prozesse definiert, dokumentiert, umgesetzt und überwacht.

Gerade für kleine und mittelständische Unternehmen (KMU) ist die Planung, Implementierung und der dauerhafte Betrieb eines ISMS keine einfache Aufgabe. Das erforderliche Knowhow zum Aufbau ist hoch. Die Ressourcen im Unternehmen hierfür sind in der Regel knapp oder verfügen nicht über die erforderliche Ausbildung auf diesem speziellen Gebiet. Daher sind künftige Konzepte erforderlich, welche auch für KMU wirtschaftliche und trotzdem sichere Lösungen liefern. Ein Beispiel für die Einführung eines ISMS in einem KMU ist in [PUL2024b] beschrieben.

Die [DIN_EN_ISO/IEC_27001] beschreibt den Aufbau eines ISMS für Unternehmen, die [DIN_EN_IEC_62443-2-1] sieht auch für den Produktionsbereich ein ISMS vor. In

[NIE2024b] wird gezeigt, wie die kombinierte Nutzung beider Normen zu einer Vereinfachung der Prozesse und zu einem einheitlichen ISMS führen kann.

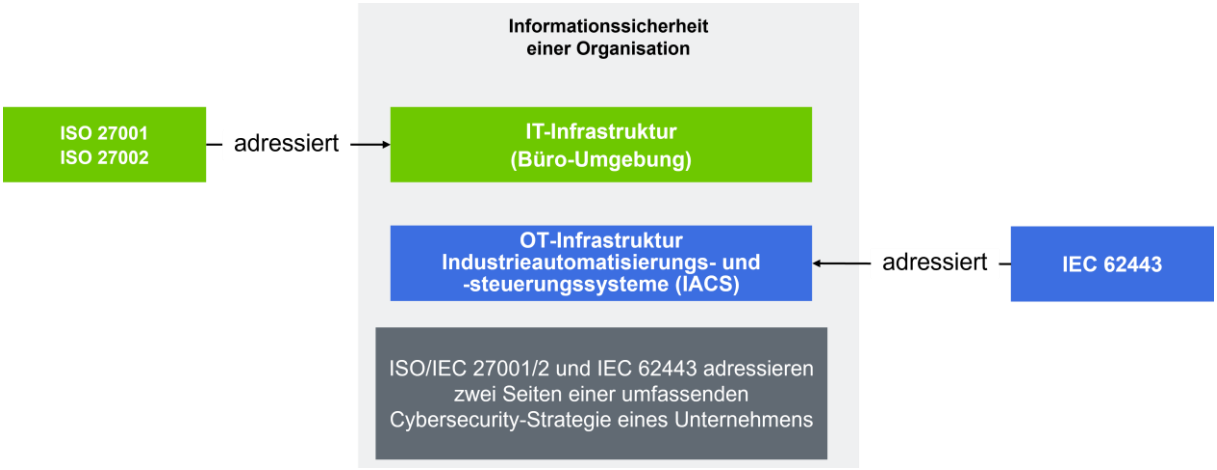

Abbildung 3: ISO 27001/ ISO 27002 und IEC 62443 als Bestandteile einer Cybersecurity-Strategie (In Anlehnung an [NIE2024b])

Abbildung 3 zeigt das Zusammenwirken von ISO 27001 und IEC 62443. Die ISO 27001 adressiert die Informationssicherheit einer Organisation generell. Im Rahmen dieser Norm können die wesentlichen Prozesse für den Aufbau eines ISMS etabliert werden. Dies kann auch den ISMS-Anteil für den Produktionsbereich mit umfassen. Im Rahme der IEC 62443 werden dann zusätzlich, die spezifischen Aspekte für die Automatisierungssysteme abgedeckt, die in der ISO 27001 nicht enthalten sind. Eine detaillierte Betrachtung der kombinierten Nutzung beider Normen finde sich in [NIE2021] [KOB2021]. Die beiden Dokumente sind unabhängig voneinander entstanden, kommen aber weitestgehend zu den gleichen Ergebnissen. Im Nachgang haben sich die beiden Autoren dann entschieden, noch einmal eine gemeinsamen, konsolidierten Beitrag [NIE2024b] zu diesen Thema zu verfassen.

3. Normen, Standards, Richtlinien

Im Bereich der OT-Security stehen Unternehmen eine Reihe von Normen bzw. Normreihen zur Verfügung. Normen basieren auf aktuellem Wissen und auf anerkannten Regeln. Sie ermöglichen so eine standardisierte Vorgehensweise in Bezug auf Auslegung, Implementierung, Betrieb und Zertifizierung von Systemen für die OT-Security.

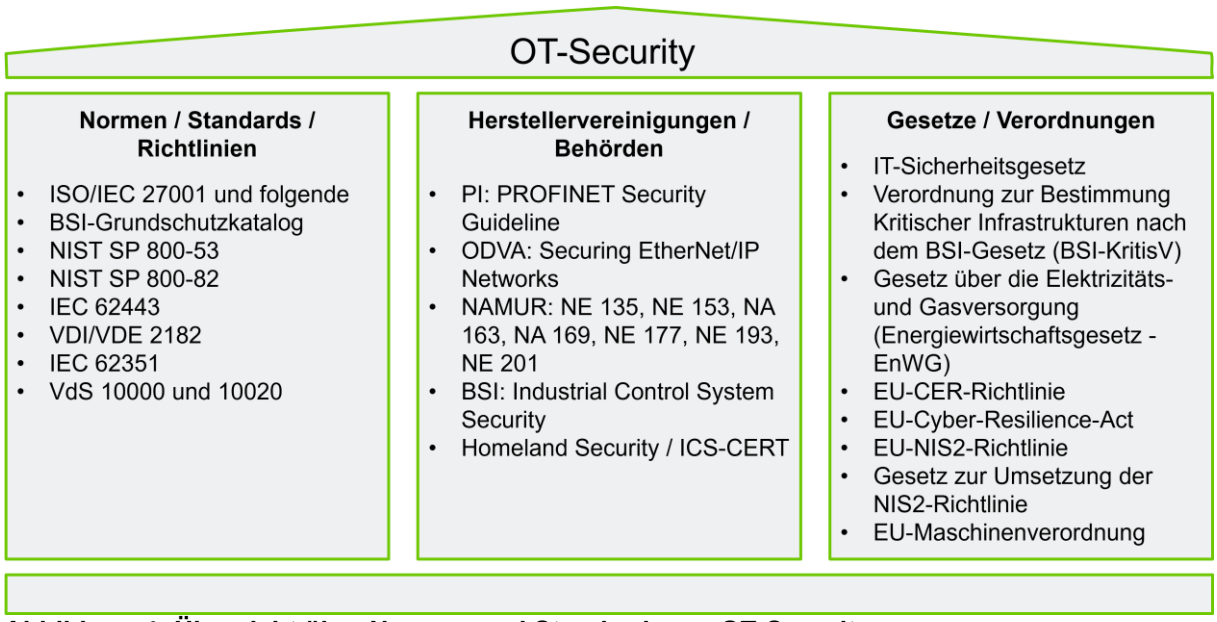

Abbildung 4: Übersicht über Normen und Standards zur OT-Security

Abbildung 4 gibt einen Überblick über Normen und Standards zur OT-Security. Neben Normen und Standards für den Office-Bereich (ISO 27000-Reihe, BSI-Grundschutzkatalog), die für den Aufbau eines ISMS benötigt werden, sind auch Normen aufgeführt, die speziell den Produktionsbereich, also die OT-Security adressieren. Hierzu gehören zum Beispiel die IEC 62443, IEC 62351, NIST SP 800-82, VDI/VDE 2182, VdS 10000 in Verbindung mit der VdS 10020. Die Aufstellung wird ergänzt um eine Reihe von Security-Empfehlungen von Hersteller-/Anwendervereinigungen wie z. B. PROFIBUS & PROFINET International für PROFINET, ODVA für EtherNet/IP und die Interessengemeinschaft Automatisierungstechnik in der Prozessindustrie (NAMUR) sowie Leitfänden von Behörden, wie z. B dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und das ICS-CERT der Homeland Security. Ganz rechts im Bild sind dann die Gesetze und Verordnungen auf EU-Ebene und auf deutscher Ebenen genannt.

Die folgenden Abschnitte liefern einen Überblick über den Stand der verfügbaren Literatur. Dabei werden zunächst die allgemeinen Normen für die IT-Sicherheit (Informationssicherheit / IT-Sicherheit) betrachtet. Im Anschluss folgt ein Überblick über spezielle Normen für die Automatisierungstechnik (OT-Security) und Empfehlungen von Herstellerorganisationen. Danach folgt in Kapitel 4 ein Ausblick auf die gesetzlichen Regelungen auf EU-Ebene und in Deutschland.

3.1. Normen und Standards für den Office Bereich (IT-Security)

Die Normreihe ISO 27000 befasst sich mit der Informationssicherheit und dem Aufbau eines Informationssicherheitsmanagementsystems (ISMS). Eine Einführung findet sich in [BRE2024].. Die ISO 27000-Reihe liefert einen umfassenden Satz an Normen, welche neben den organisatorischen Aspekten auch die zugehörigen Prozesse, die Umsetzung und auch die Zertifizierung beschreiben. Die Normreihe beginnt mit der [DIN_EN_ISO_27000] die eine Einführung gibt und die Terminologie erläutert. Es folgt die [DIN_EN_ISO/IEC_27001]. Hier wird der Aufbau eines ISMS und das risikobasierte Vorgehen beschrieben. Im Anhang werden die erforderlichen Sicherheitsmaßnahmen beschrieben. Die Norm [DIN_EN_ISO_IEC_27002] definiert konkrete Maßnahmen zur Umsetzung. Es gibt noch eine Reihe weiterer Normen. Die Webseite [ISE2025] stellt einen Kurzüberblick über alle Normteile zur Verfügung.

ISO-27000-Managementsyteme lassen sich gemäß den Vorgaben der [DIN_ISO_27006-1] zertifizieren. Die Vorgehensweise bei der Zertifizierung findet sich z. B. in [BRE2024], [HÄU2023]. Die Zertifizierung eines Informationssicherheitsmanagementsystems (ISMS) nach der Normreihe ISO 27000 ist bisher noch wenig verbreitet. Abbildung 5 zeigt den Bestand an gültigen ISO-27001-Zertifikaten in Deutschland.

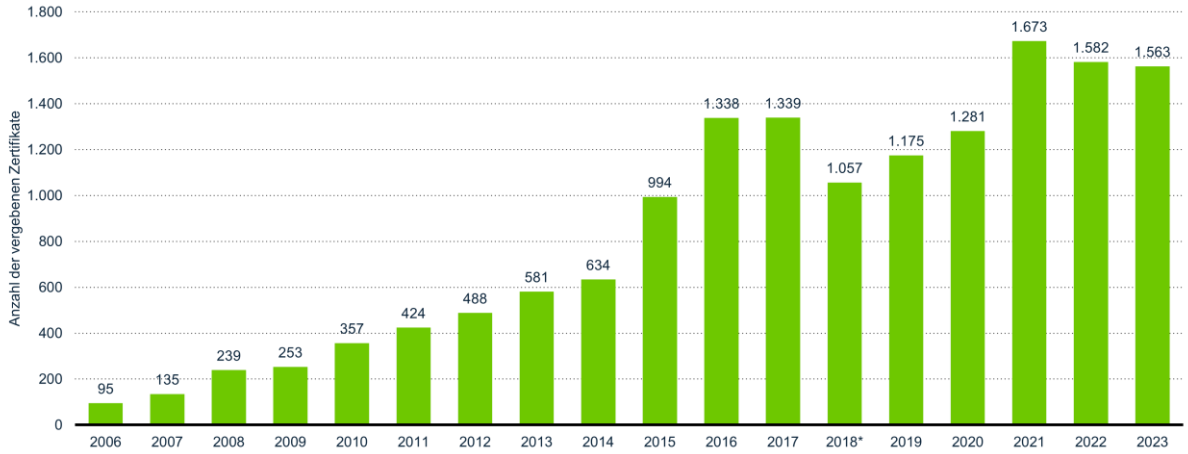

Abbildung 5: Bestand an gültigen ISO-27001-Zertifikaten in Deutschland in den Jahren 2006 bis 2023 [STA2025a]

Die Statistik nennt für das Jahr 2023 eine Zahl von 1 563 gültigen ISO-270001-Zertifikaten [STA2025a]. Dies kann man nun in Relation zu der Anzahl der Unternehmen in Deutschland setzen. Das war im Jahr 2023 eine Anzahl von 3,1 Mio. [STA2025b]. Somit kann man davon auszugehen, dass hauptsächlich Unternehmen zertifiziert sind, die als besonders exponiert gelten (Banken, Zahlungsdienstleister).

Basierend auf der ISO 27000-Normreihe hat das Bundesamt für Sicherheit in der Informationstechnik eine Reihe von Grundschutzkatalogen definiert, welche einen vereinfachten Zugang zur Informationssicherheit ermöglichen. Einen guten Überblick liefert das IT-Grundschutz-Kompendium [BSI2023b]. Darüber hinaus stellt das BSI passende Checklisten und Erhebungsbögen bereit. Das erlaubt KMUs einen einfacheren Zugang zum Thema der IT-Sicherheit.

Der VdS bietet mit den Richtlinien [VDS_10000] eine Leitlinie für die Cyber-Security im Office-Bereich für KMU, welche auf die Bedürfnisse von kleinen und mittleren Unternehmen zugeschnitten ist. Eine Zertifizierung nach diesem Standard ist möglich. Der Aufwand ist auf die Bedürfnisse von KMU zugeschnitten und liegt deutlich unter dem einer Zertifizierung nach der ISO 27000-Normreihe.

3.2. Normen und Standards für den Produktionsbereich (OT-Security)

Die in Kapitel 3.1 beschriebenen Normen adressieren die Informationssicherheit / IT-Security im Office-Bereich. Damit ist die IT eines Unternehmens gemeint, welches über keine Produktionsanlagen verfügt (z. B. Banken) oder der Teil eines Unternehmens, in dem keine Produktionsanalagen angesiedelt sind (z. B. Verwaltung, Vertrieb Personalabteilung, etc.). Die Anforderungen im Office Bereich sind wie folgt priorisiert: Vertraulichkeit, Integrität und Verfügbarkeit. Abbildung 6 zeigt auf der linken Seite die Priorisierung dieser Schutzziele für den Office-Bereich.

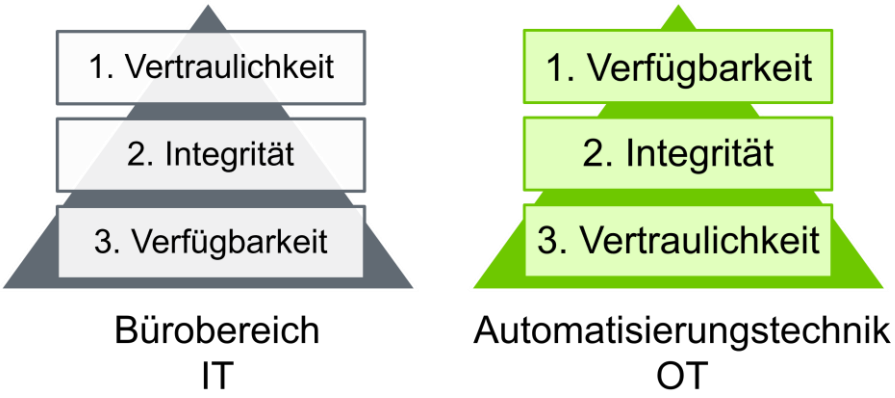

Abbildung 6: Priorisierung der Schutzziele für Bürobereich (IT) und Automatisierungstechnik (OT)

Im Produktionsbereich ist die Priorisierung eine andere. Wie in Abbildung 6 auf der rechten Seite zu sehen ist, hat hier die Verfügbarkeit der Produktionsanlage die höchste Priorität, gefolgt von der Integrität der Anlage. Die Vertraulichkeit folgt erst an dritter Stelle. Der gemäß Abbildung 6 relativ geringe Stellenwert der Vertraulichkeit liegt darin begründet, dass z. B. aus den IO-Daten, die über ein PROFINET kommuniziert werden, nur wenig Information für einen Angreifer enthalten ist. Aus diesem Grund differenziert PROFIBUS & PROFINET International (PI) die Security-Funktion von PROFINET in verschiedene Security Klassen [NIE2023b]. Die Klasse 2 umfasst Integrität und Authentizität, die Klasse 3 zusätzlich die Vertraulichkeit. Abhängig von der Risikoeinschätzung des Anlagenbetreibers kann die Klasse 2 oder Klasse 3 verwendet werden.

Auf Grund dieser Priorisierung und auf Grund des für Produktionsanlagen in vielen Bereichen erforderlichen Echtzeitverhaltens sind die in Kapitel 3.1 beschriebenen Normen nicht oder nur eingeschränkt auf den Produktionsbereich anwendbar. Aus diesem Grund ist eine Reihe von Normen in der Entwicklung, welche die Anforderungen der

Produktion berücksichtigen. Die folgenden Abschnitte stellen die wichtigsten dieser Normen vor.

3.2.1. IEC 62443 Normreihe

Die Normreihe IEC 62443 wird von der Internationalen elektrotechnischen Kommission (IEC) und der International Society of Automation (ISA) entwickelt. Die ersten Arbeiten an der Norm wurden in der Arbeitsgruppe ISA 99 gestartet und werden zurzeit in einer Kooperation aus IEC und ISA fortgeführt. Daher finden sich in vielen Dokumenten noch Referenzen auf Arbeitsgruppen und Dokumente der ISA.

In der IEC 62443 Normreihe werden die speziellen Anforderungen der OT-Security im Produktionsbereich berücksichtigt. Abbildung 7 zeigt die Struktur der Normreihe. Die grün markierten Teile sind schon erschienen, die grau markierten Teile befinden sich noch in der Erstellung und sind noch nicht allgemein verfügbar. Ein Teil der Normen ist in deutscher Sprache verfügbar. Sofern dies der Fall ist, werden nachfolgend die deutschen Versionen zitiert. Die deutschen Versionen sind daran zu erkennen, dass die Zitationsverweise mit der Buchstabenfolge „DIN_EN_“ beginnen.

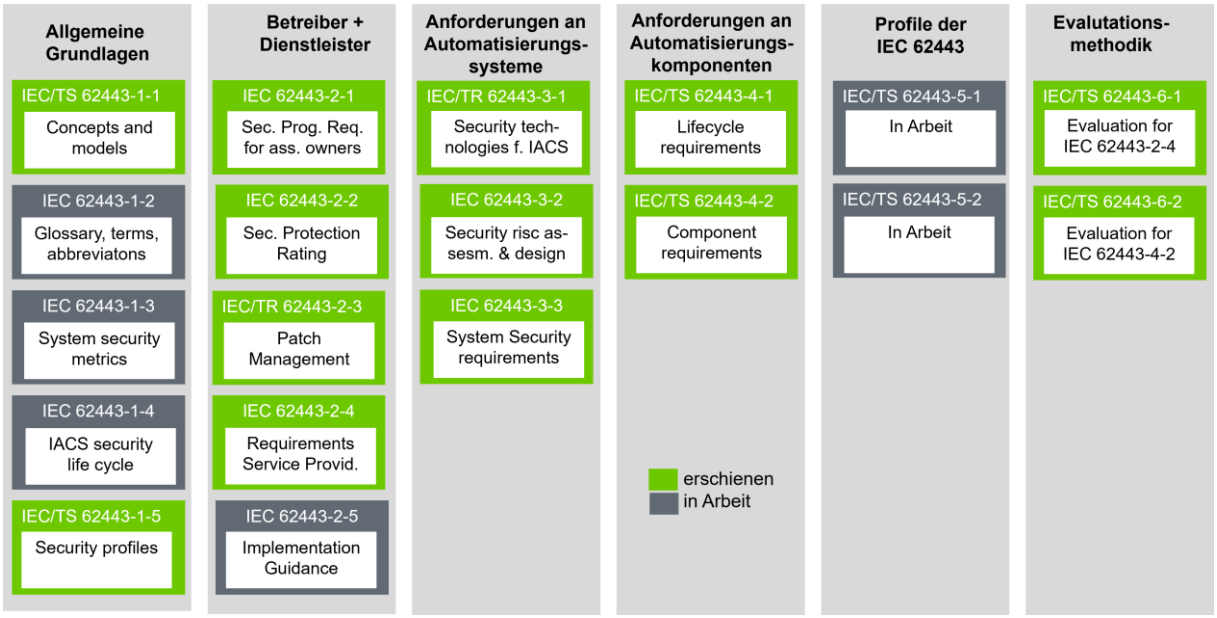

Abbildung 7: Teile der IEC 62443

Die Norm-Reihe IEC 62443 besteht aus sechs Hauptbereichen, die im Folgenden einschließlich der zugeordneten Normen vorgestellt werden:

Im Teil **„Allgemeine Grundlagen“** werden in [IEC_62443-1-1] zunächst Begriffe, Konzepte und Modelle definiert. Der Teil [IEC_62443-1-2] definiert alle Begriffe, die in den Normen verwendet werden. Der Teil [IEC_62443-1-3] definiert Metriken für die Bewertung der OT-Security, im Teil [IEC_62443-1-4] werden der Sicherheitslebenszyklus und Anwendungsfälle beschrieben. Der Normteil [IEC_62443-1-5] beschreibt die Möglichkeit einer Profilbildung durch Selektion ausgewählter Normteile.

Der Teil **„Betreiber und Dienstleister**“ beschreibt das Informationssicherheits-Management-System (ISMS) und definiert damit die Organisation der OT-Security,

gefolgt von Implementierungshilfen. Der Teil [DIN_EN_IEC_62443-2-1] beschreibt Anforderungen an ein Informationssicherheits-Managementsystem (ISMS), z. B die Definition von Security Prozessen. Der Teil [DIN_EN_IEC_62443-2-2] gibt Hinweise, wie und in welchen Bereichen diese Prozesse zu implementieren sind. Das Aktualisieren der Software von Automatisierungssystemen, das Patchen, ist von besonderer Bedeutung, weil es bei unsachgemäßem Vorgehen zu Betriebsstörungen kommen kann. Daher widmet der Standard dem Patch-Management einen eigenen Teil [IEC_62443-2-3]. Der Teil [IEC_62443-2-4] befasst sich mit dem Einsatz von Dienstleistern für Inbetriebnahme und Service aus Sicht der IT-Sicherheit und definiert Anforderungen an diese Dienstleister.

Im Teil **„Anforderungen an Aut0omatisierungssysteme“** werden das Vorgehen bei der Planung einer Anlage sowie die OT-Security-Anforderungen an eine Anlage beschrieben. Der Teil [IEC_62443_3_1] beschreibt zunächst die zu Grunde liegenden Technologien wie z. B. Authentifizierung, Verschlüsselung, Filterung und Logging. Der Teil [DIN_EN_IEC_62443-3-2] beschreibt das Vorgehen für die Security-Planung einer Anlage, das Durchführen einer Risikoanalyse, die Festlegung des erforderlichen Security-Levels (SL-T) sowie die Strukturierung einer Anlage in Zonen (abgeschottete Bereiche) und Conduits (gesicherte Verbindungen zwischen den Bereichen). Damit soll eine automatisierungstechnische Anlage in Teilbereiche unterteilt werden, die wiederum gegeneinander abgeschottet sind. Abbildung 8 zeigt den Ablauf der Risikoanalyse gemäß der [DIN_EN_IEC_62443-3-2]. Die Analyse betrachtet eine Zone oder einen Conduit zunächst in einer initialen Analyse. Übersteigt das initiale Risiko einen vom Unternehmen für die Anlage zu definierenden Grenzwert, werden Maßnahmen zur Risikoreduzierung definiert. Dies erfolgt so lange, bis das vorhandene Risiko das Restrisiko nicht mehr übersteigt.

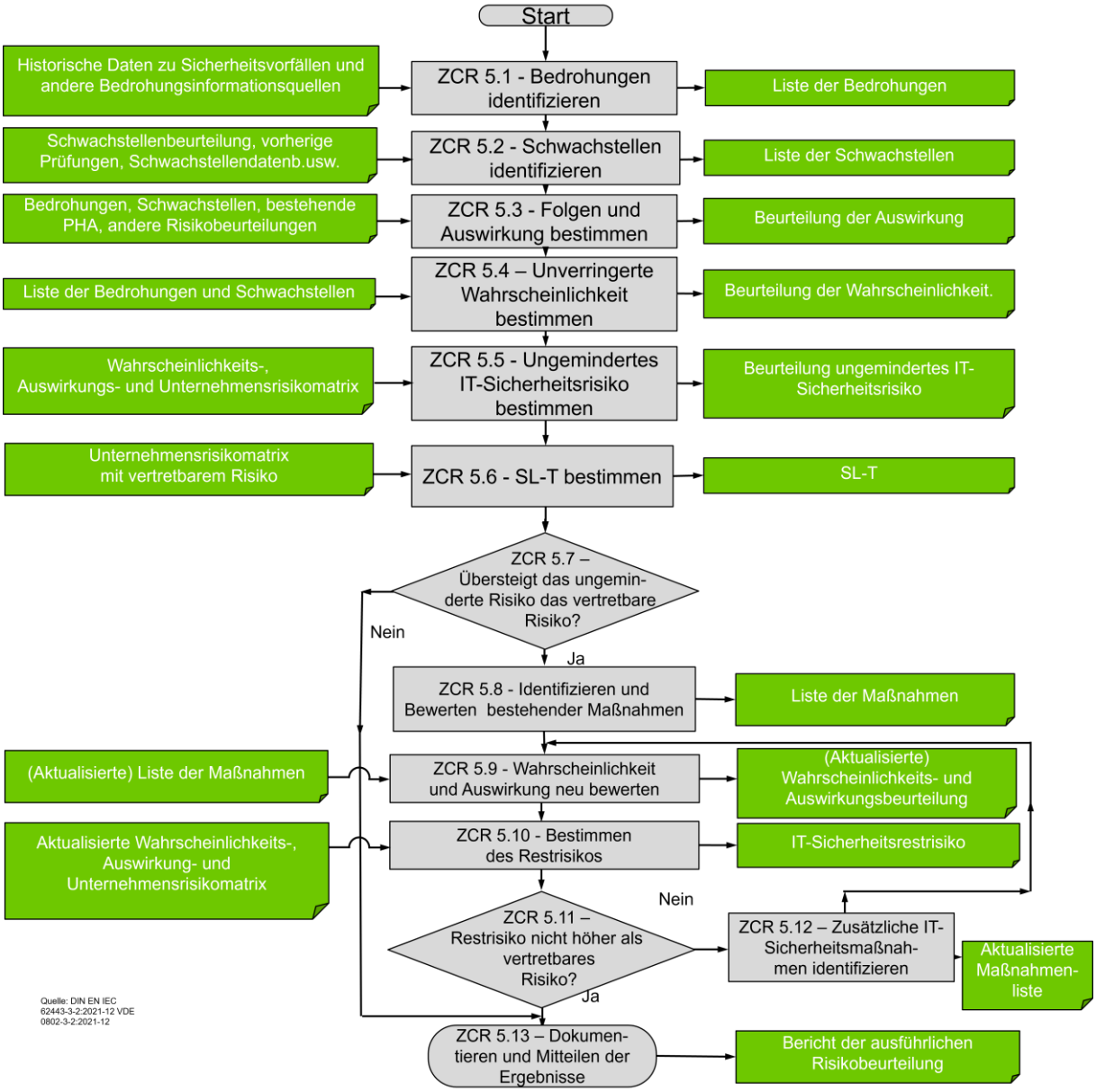

Abbildung 8: Risikoanalyse gemäß der [DIN_EN_IEC_62443-3-2]

Der Teil [DIN_EN_IEC_62443-3-3] definiert die Security-Anforderungen an eine Anlage. Basis hierfür sind die so gennannten „Grundlegenden Anforderungen“ (engl. Foundational Requirements):

- Identifizierungs-/Authentifizierungs-Kontrolle (IAC)
  - Erfassung aller Benutzer (Mensch, Software, Komponente).
- Benutzerverwaltung (UC)
  - Durchsetzen der Zugangsberechtigungen von Benutzern.
  - Erfassen von Ereignisdaten (Logging).
- Systemintegrität (SI)
  - Verhindern von Manipulation des IACS.
- Vertraulichkeit von Daten (DC)
  - Absichern von Daten in Kommunikationskanälen und Speichern.
- Einschränkung des Datenflusses (RDF)

        - Zonenaufteilung und geschützte Kommunikationskanäle.
    - Zeitnahe Reaktion auf Ereignisse (TRE)
        - Schnelle Benachrichtigung von Entitäten über IT-Sicherheitsvorfälle.
        - Event Monitoring und Logging
    - Verfügbarkeit von Ressourcen (RA)
        - Sicherstellung der Verfügbarkeit von Ressourcen.
        - Schutz gegen DoS-Angriff
        - Backup
        - Notstrom

Die Anforderungen werden entsprechend dem Security-Level in einer Stufe zwischen 1 und 4 definiert. Mit zunehmendem Security-Level erhöht sich die Schärfe der Anforderung.

Im Teil **„Anforderungen an Automatisierungskomponenten“** werden die Anforderungen an die Komponenten und den zugehörige sichere Produktentwicklungszyklus (engl. Secure Development Lifecycle – SDL) beschrieben. Dieser Teil richtet sich an die Hersteller von Automatisierungssystemen. Der Teil [DIN_EN_IEC_62443-4-1] definiert den Entwicklungsprozess, der bei der Entwicklung von Komponenten für die Automatisierungstechnik zu beachten ist. Hierbei sind z. B. Themen wie: "Entwicklungsprozess”, “Spezifikation der OT-Security-Anforderungen”, “IT-Sicherheit durch den Entwurf” sowie “Risikoanalyse and Bedrohungsmodell” Bestandteil der Norm. Der Teil [DIN_EN_IEC_62443-4-2] beschreibt die technischen Anforderungen für die Komponenten von Automatisierungssystemen, Applikation und Funktionen. In [NIE2023a] wird am Beispiel eines PROFINET-Gerätes exemplarisch beschrieben, wie die „sichere“ Entwicklung einer Automatisierungskomponente gemäß den beiden hier beschriebenen Normteilen abläuft.

Der Teil **Evaluationsmethodik** ist Anfang 2025 erschienen. In der Norme [IEC_62443-6-1] werden Kriterien zur Evaluierung der Anforderungen der Norm [DIN_EN_IEC_62443-2-4] beschrieben. Der Teil [IEC_62443-6-2] definiert Kriterien zur Evaluierung der Anforderungen der Norm [DIN_EN_IEC_62443-4-2].

Die bisher erschienenen Normen, bzw. Normentwürfe umfassen zurzeit 1 216 Druckseiten (Stand September 2025). Für einen ersten Eintstieg in die Norm wird der „Leitfaden Industrial Security“ [KOB2024] empfohlen. Das Dokument bietet einen Überblick über die Normreihe IEC 62443 und erläutert die Zusammenhänge zwischen den Normteilen.

Die Normreihe IEC 62443 adressiert die Rollen Betreiber (engl. Asset Owner), Planer (engl. System Integrator) und Hersteller (engl. Manufacturer). Jeder dieser Rollen sind Teile der Normreihe zugeordnet. Abbildung 9 zeigt das Zusammenwirken der drei beschriebenen Rollen sowie die Zuordnung der Normteile.

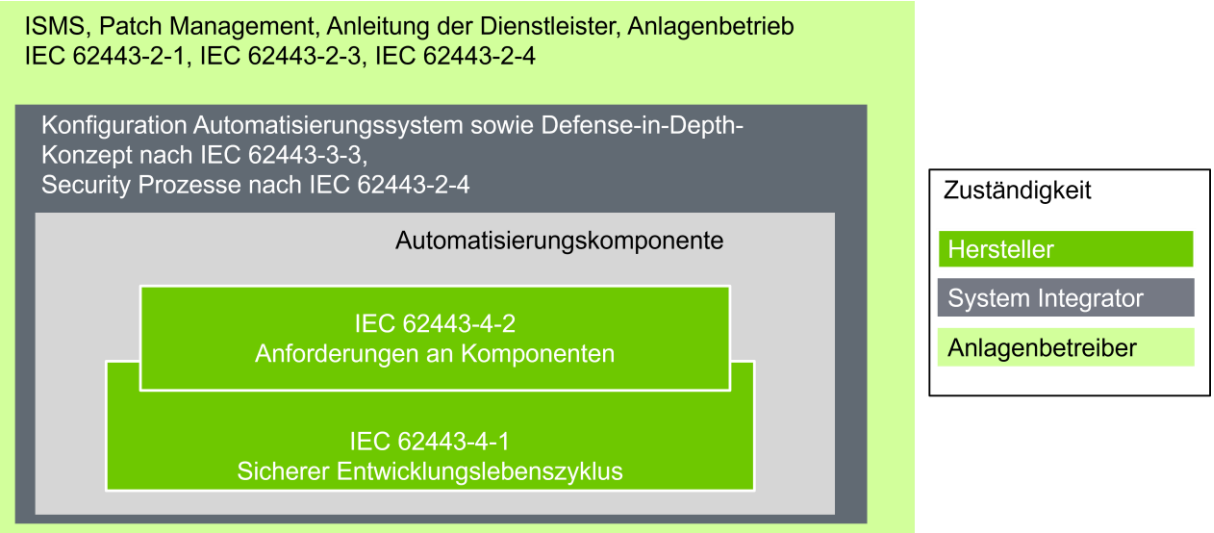

Abbildung 9: Verantwortlichkeiten und zugehörige Normteile im Security Prozess

Es kann festgehalten werden, dass die Normreihe IEC 62443 die wesentliche und wichtigste Norm für die OT-Security ist.

3.2.2. VDI/VDE Normreihe 2182

Mit der Normreihe VDI/VDE 2182 wird das Thema OT-Security anhand von konkreten Beispielen für die Fertigungs- und die Prozessindustrie verdeutlicht. Der Fokus liegt auf der Risikoanalyse im OT-Bereich. Dabei werden die Sichten für Hersteller, Integratoren und Betreiber adressiert. Alternativ zum Vorgehen nach VDI/VDE 2182 kann die Risikoanalyse auch nach der Norm [DIN_EN_IEC_62443-3-2] durchgeführt werden. Diese Norm hat einen vergleichbaren Ansatz und definiert den Ablauf des sicheren Systemdesigns und der Risikoanalyse. Siehe hierzu die Beschreibung in Kapitel 3.2.1.

Der Teil 1 der Norm [VDI_2182_1] definiert zunächst die wesentlichen Begriffe der OT-Security:

- Benutzer
  - Person oder Anwendung, die mit dem Betrachtungsgegenstand interagieren können.
- Asset
  - Alle materiellen und immateriellen Werte von Automatisierungsgeräten, Automatisierungssystemen, Maschinen oder Produktionsanlagen, die bedroht sein können und die schützenswert sind
  - Beispiele: SPS, Rezeptur, Schnittstellenfunktionen, Firmware.
- Bedrohung
  - Ein Umstand oder ein Ereignis, durch den oder das ein Schaden entstehen kann.
- Risiko
  - Kombination von Wahrscheinlichkeit und Ausmaß eines Schadens.
- Risikoreduzierung
  - Senkung der Schadenswahrscheinlichkeit oder der Schadenshöhe durch Anwendung von Schutzmaßnahmen.
- Schwachstelle

    - Mangel, der dazu führt, dass eine Bedrohung für den Betrachtungsgegenstand wirksam werden kann.
- Verursacher
    - Autorisierter oder nicht-autorisierter Benutzer, dessen Aktionen beabsichtigte oder unbeabsichtigte negative Auswirkungen auf Schutzziele eines Betrachtungsgegenstands haben können.

Danach definiert die Norm ein Vorgehensmodell mit zugehörigen Rollen, wie es in Abbildung 10 dargestellt ist.

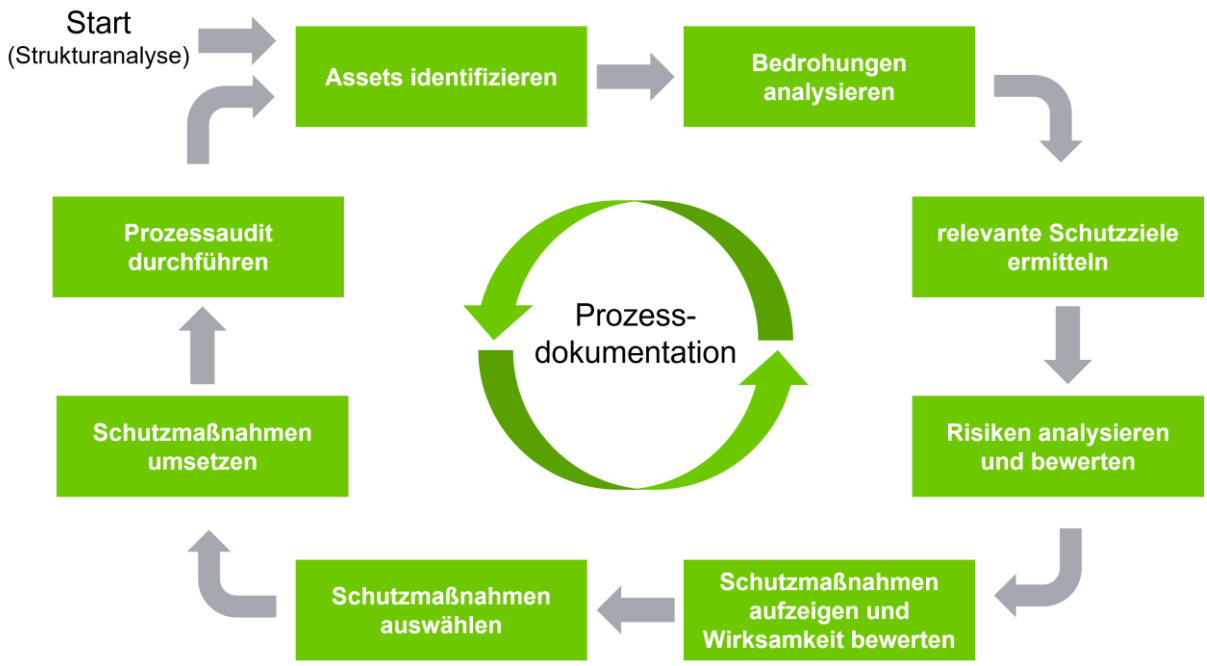

Abbildung 10: Vorgehensmodell nach [VDI_2182_1]

Das Vorgehensmodell der VDI/VDE 2182 orientiert sich an einem so genannten „Plan-Do-Check-Act-Zyklus“ (PDCA).

1. In einem ersten Schritt werden die Assets der Anlage, insbesondere Automatisierungskomponenten, Rechner, Server, etc.) identifiziert und aufgenommen. Das Ergebnis ist eine Liste der identifizierten Assets.
2. Als nächstes sieht der Zyklus vor, die Bedrohungen, welche auf die Assets wirken, zu identifizieren. Dabei werden Bedrohungsszenarien betrachtet und dokumentiert. Die VDI/VDE 2182 gibt dabei entsprechende Templates vor.
3. Im dritten Schritt sieht die Norm die Ermittlung der relevanten Schutzziele vor. Abgeleitet aus den Bedrohungen, werden für jedes Asset die Schutzziele festgelegt und dokumentiert.
4. Der vierte Schritt des Vorgehensmodells sieht nun eine Risikobewertung vor. Basierend auf den Bedrohungen und den identifizierten Schutzzielen werden nun die Wahrscheinlichkeit des Eintretens der identifizierten Bedrohungen und ein zugeordneter potenzieller Schaden beschrieben. Aus der Kombination von Eintrittswahrscheinlichkeit und Schadenshöhe kann ein zugeordnetes Risiko identifiziert werden.

5. Das Ergebnis der Risikobewertung identifiziert Felder, in denen das bestehende Risiko nicht akzeptabel ist. Hier sind Maßnahmen zur Risikoreduzierung, so genannten Schutzmaßnahmen, vorzusehen und in Bezug auf ihre Wirksamkeit und Wirtschaftlichkeit zu bewerten.
6. Basierend auf den Betrachtungen aus Schritt 5 erfolgt nun die Auswahl der Schutzmaßnahmen. Ziel dieser Auswahl ist es, in einem wirtschaftlich vertretbaren Rahmen Schutzmaßnahmen zu implementieren und gleichzeitig die erforderliche Risikoreduzierung zu erreichen.
7. Der nachfolgende Schritt sieht die Umsetzung der ausgewählten Schutzmaßnahmen vor.
8. Auf Basis der vorangehenden Schritte erfolgt abschließend ein Audit des beschriebenen Vorgangs. Hierbei werden die erstellten Dokumente sowie die Wirksamkeit der beschriebenen Schutzmaßnahmen ermittelt. Das Audit sollte von Personen durchgeführt werden, die nicht an den vorangehenden Schritten beteiligt waren.

Da sich die Bedrohungslage für eine Produktionsanlage durch externe Ereignisse ändern kann, sollte dieser Prozess in bestimmten Zeitintervallen wiederholt werden. Das Gleiche gilt auch im Falle von Änderungen oder Erweiterungen der Anlage.

Zur Unterstützung des beschriebenen Prozesses stehen SW-Werkzeuge zur Verfügung, welche die Erfassung und Bewertung der Assets unterstützen. So stellt das Bundesamt für Sicherheit in der Informationstechnik das Werkzeug LARS [BSI2025] zur Verfügung. Die Homeland Security bietet das Werkzeug CSET [ICS2025] an. Beide Werkzeuge fokussieren auf die OT-Security. Aus dem IT-Bereich ist auch das „Microsoft Threat Modelling Tool“ bekannt [MIC2023]. Dieses Tool verwendet zur Analyse den STRIDE-Ansatz. STRIDE beschreibt dabei mögliche Angriffsvektoren, die in Tabelle 2 näher beschrieben sind.

Tabelle 2 : Bedeutung der Abkürzung STRIDE

Buchstabe	Englisch	Deutsch	Beschreibung
S	Spoofing	Vortäuschung	Ein Angreifer gibt sich als jemand anderes aus (Identitätsdiebstahl).
T	Tampering	Manipulation	Unbefugte Veränderung von Daten oder Code.
R	Repudiation	Abstreitbarkeit	Die Möglichkeit, eine Aktion zu leugnen, z. B. eine Transaktion.
I	Information Disclosure	Informationsoffenlegung	Unbefugter Zugriff auf vertrauliche Informationen.
D	Denial of Service	Dienstverweigerung	Angriffe, die die Verfügbarkeit eines Systems einschränken oder verhindern.
E	Elevation of Privilege	Privilegien-Erweiterung	Ein Angreifer verschafft sich höhere Rechte als vorgesehen.

Die VDI/VDE 2182 Normreihe definiert den Prozess in Bezug auf drei Rollen:

- **Hersteller**: Die Hersteller entwickeln und vertreiben die Anlagenkomponenten. Sie sind gleichzeitig für die Wartung und Pflege der gelieferten Komponenten (z. B. SW-Updates zum Beheben von Sicherheitslücken) zuständig.

- **Integrator**: Der Integrator ist ein vom Betreiber beauftragter Dienstleister, der für die Planung und Inbetriebnahme einer Anlage zuständig ist. Betreiber von Anlagen verfügen häufig nicht über ausreichende Ressourcen für die Planung und Inbetriebsetzung von Neuanlagen oder für die Durchführung von Anlagenänderungen. Daher ist der Einsatz von Integratoren eine häufig geübte Praxis.
- **Betreiber**: Der Betreiber ist für den Betrieb und die Instandhaltung der Anlage verantwortlich. Möglicherweise delegiert der Betreiber Instandhaltungsaufgaben an Instandhaltungsdienstleister.

Die Teile 2 und 3 der VDI/VDE 2182 folgen dem beschriebenen Rollenkonzept. Im Teil 2 werden am Beispiel einer Produktionsanlage im Bereich der Fertigungsautomatisierung für die Rollen von Hersteller [VDI_2182_2_1], Integrator [VDI_2182_2_2] und Betreiber [VDI_2182_2_3] die Aufgaben gemäß des in Teil 1 beschriebenen Vorgehensmodells beschrieben. Das gleiche findet sich im Teil 3 für eine Anlage der Prozessautomatisierung in gleicher Weise [VDI_2182_3_1] [VDI_2182_3_2] [VDI_2182_3_3].

Mit der VDI/VDE 2182 Normreihe steht Herstellern, Integratoren und Betreibern eine Basis zur strukturierten Risikoanalyse zur Verfügung. Das Dokument bietet eine auf die jeweiligen Zuständigkeiten fokussierte Sicht auf das beschriebene PDCA-Vorgehensmodell. Die jeweiligen Teile führen anhand eines realen Beispiels durch den Prozess und zeigen durch die Bereitstellung von Checklisten auf, in welcher Form eine Dokumentation der Ergebnisse erfolgen kann.

3.2.3. VdS 10020

Die [VDS_10020] richtet sich an kleine und mittelständische Unternehmen (KMU) und stellt einer Ergänzung zu der bereits bestehenden Richtlinie [VDS_10000] dar. Die VdS 10020 richtet sich an KMU, welche Produktionsanlagen betreiben. In einer knappen und übersichtlichen Form werden die Kriterien beschrieben, welche für die Umsetzung einer OT-Security-Strategie im Produktionsbereich erforderlich sind.

3.2.4. Leitlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Das Bundesamt für Sicherheit in der Informationstechnik bietet eine Reihe von Leitlinien im Bereich der OT-Security. Traditionell bezeichnet das BSI Automatisierungssysteme als ICS (Industrial Control System). Aus diesem Grund findet sich in Dokumenten des BSI häufig der Begriff ICS-Security.

In regelmäßigen Abständen veröffentlicht das BSI die Top-10-Bedrohungen für Automatisierungssysteme und die zugehörigen Gegenmaßnahmen [BSI2022b]. Darüber hinaus bietet das BSI mit dem ICS-Security-Kompendium [BSI2024] einen Einstieg in die OT-Security für Anlagenbetreiber. Das Dokument „Anforderungen an netzwerkfähige Industriekomponenten“ [BSI2018c] richtet sich an die Hersteller von Automatisierungskomponenten und definiert Anforderungen an Komponenten von Automatisierungssystemen. Neben diesen grundlegenden Dokumenten veröffentlicht das BSI in regelmäßigen Abständen Fallbeispiele, in denen spezielle Aspekte aufgegriffen werden. So gibt es z. B. Fallbeispiele für einen möglichen Angriff auf ein Schwimmbad

[BSI2018a] durch die Verwendung fest codierter Passwörter sowie ein Beispiel für den Einsatz eines Servicetechnikers, der über einen verseuchten USB-Stick unwissentlich eine Schadsoftware in eine Anlage eingebracht hat. [BSI2018b].

Das Thema Remote Service und Remote Diagnose ist von besonderer Bedeutung, da hier aus dem Automatisierungsbereich Kommunikationsverbindungen über das Internet zu Dritten betrieben werden. Das BSI widmet diesem Thema ein separates Modul im BSI-Grundschutz [BSI2022a].

3.2.5. Leitlinien von Herstellerorganisationen

Industrielle Kommunikationssysteme wie PROFINET oder EtherNet/IP stellen einen wichtigen Teil einer Automatisierungsinfrastruktur dar. Aus diesem Grund haben die verschiedenen Herstellerorganisationen das Thema OT-Security adressiert und entsprechende Leitlinien herausgebracht.

So bietet die PROFIBUS & PROFINET International (PI) eine Leitlinie für die Planung von PROFINET [PNO2013] unter Berücksichtigung der OT-Security. Diese Leitlinie befindet sich zurzeit in Überarbeitung und wird in absehbarer Zeit neu erscheinen. Darüber hinaus hat PI ein Security-Konzept erarbeitet, welches einen kryptografischen Schutz der PROFINET Kommunikation ermöglicht. Hierzu sind schon verschiedene Richtlinien und Veröffentlichungen erschienen. Zu nennen sind zum Beispiel:

- Security Erweiterungen für PROINET [PNO2019b].
- OT-Security für Produktionsanlagen mit PROFINET. Eine Einordnung der IEC 62443 für Betreiber, Integratoren und Hersteller [PNO2022].
- Security-Event-Logging am Beispiel von PROFINET [NIE2024a].
- Security Class 1 for PROFINET-Security Guideline for PROFINET [PNO2023].
- Wie man ein sicheres PROFINET-Gerät entwickelt. Organisatorische und technische OT-Security-Maßnahmen bei der Entwicklung von PROFINET-Geräten [NIE2023a].
- Security Extensions for PROFINET. Concepts, Status, and Prospects [NIE2023b].

Vergleichbare Dokumente stellt die ODVA unter dem Namen „CIP-Security“ für EtherNet/IP [ODV2023], [VIS2020] zur Verfügung. Des Weiteren liegt für OPC UA ein Security-Modell als Technical Report der IEC [IEC_62451-2] vor. Das Bundesamt für Sicherheit in der Informationstechnik hat dieses Konzept evaluiert und im Wesentlichen positiv bewertet [BSI2022e].

3.2.6. Normen für den maritimen Sektor

International setzt die Internationale Seeschifffahrtsorganisation (engl. International Maritime Organization IMO) den regulatorischen Rahmen für die OT-Security auf Schiffen. Zentral ist die Resolution MSC.428(98) [IMO2017], die fordert, Cyber-Risiken bis spätestens zur ersten jährlichen Überprüfung des Document of Compliance nach dem 1. Januar 2021 systematisch im Safety-Management zu berücksichtigen. Flankierend geben die IMO-Leitlinien zum maritimen Cyber-Risikomanagement MSC-

FAL.1/Circ.3/Rev.3 [IMO2025] eine Unterstützung zu Risikobeurteilung, Schutzmaßnahmen, Erkennung, Reaktion und Wiederanlauf.

Für Schiffe wurden von der International Association of Classification Societies (IACS) mit den IACS Unified Requirements E26 (Cyber Resilience of Ships) [UR_E26] und E27 (Cyber Resilience of On-Board Systems and equipment) [UR_E27] verbindliche Mindestanforderungen für Neubauten geschaffen. Sie adressieren u. a. die Segmentierung und Härtung von Bordnetzwerken, das Management privilegierter Zugänge und Fernwartung, Patch- und Schwachstellenmanagement, Logging und Ereigniserkennung sowie Lebenszyklusanforderungen an Zulieferer und Integratoren.

Klassifikationsgesellschaften haben auf Basis der oben genannten Standards eigene Notationen und Leitfäden etabliert (z. B. DNV Cyber Secure Class Notation [DNV2025], ABS CyberSafety [ABS2025], Lloyd's Register ShipRight Cyber [LLO2024]), die teilweise über die UR hinausgehen und Prüf- und Abnahmekriterien definieren.

3.2.7. Sonstige branchenspezifische Normen

Neben den Herstellervereinigungen befassen sich auch Anwendervereinigungen mit dem Thema OT-Security. Die Interessengemeinschaft Automatisierungstechnik in der Prozessindustrie (NAMUR) hat bereits im Jahr 2006 eine erste Empfehlung zur OT-Security herausgegeben. Im Laufe der Jahre sind weitere Dokumente erschienen. Die wesentlichen Dokumente sind:

- IT-Sicherheit für Systeme der Automatisierungstechnik [NA_115].
- Fernwartung bei Systemen der Automatisierungstechnik in der Prozessindustrie [NE_135].
- Automation Security 2020 – Design, Implementierung und Betrieb industrieller Automatisierungssysteme [NE_153].
- Automation Security Management in der Prozessindustrie [NA_169].
- NAMUR Open Architecture – NOA-Security-Zonen und NOA-Security-Gateway [NE_177].
- Ein Informationsmodell für das Automation Security Engineering [NE_193].
- IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen [NA_163]
- Identity and Access Management on Automation Devices [NE_201].

An dieser Stelle kann lediglich ein begrenzter Ausblick auf branchenspezifische Normen gegeben werden, die keinen Anspruch auf Vollständigkeit hat.

3.2.8. Zusammenfassung Normen und Standards

Vielen zuvor beschriebenen Dokumenten liegt der „Plan-Do-Check-Act-Zyklus" (PDCA-Zyklus) zu Grunde. In einem strukturierten Vorgehen werden, wie in Kapitel 3.2.2 beschrieben, die Assets erfasst, die Bedrohungen identifiziert, die Risiken bewertet und die notwendigen Maßnahmen abgeleitet, implementiert und verifiziert. Ein weiteres gemeinsames Kriterium ist die Etablierung einer IT-Sicherheitsstrategie im Unternehmen, die eine ganzheitliche und übergreifende Betrachtung einfordert. Neben technischen Aspekten sind insbesondere auch organisatorische und personelle Aspekte zu berücksichtigen.

In Bezug auf die technische Implementierung gehen die bestehenden Standards von einer Defense in Depth Strategie aus. Durch eine Reihe sich ergänzender Maßnahmen werden die Assets gegen Bedrohungen von außen abgeschottet und so geschützt.

Mit der zunehmenden horizontalen und vertikalen Integration im Kontext von Industrie 4.0 werden die bestehenden Konzepte erweitert und verbessert werden müssen. In [NIE2014] [NIE2014_1] wurden bereits im Jahr 2014 eine Reihe von zusätzlichen Herausforderungen definiert, welche in Bezug auf die OT-Security zu adressieren sind. Dies sind insbesondere:

- Schutz gegen Innentäter
- Kommunikation auch über Unternehmensgrenzen hinweg
- Zugangskontrolle zum Netzwerk
- Absicherung der Kommunikation mit kryptografischen Mitteln.

Diese Herausforderungen gelten heute – 11 Jahre später – durchaus weiter. Kapitel 6 wird diese Aspekte noch einmal aufgreifen und diskutieren.

4. Rechtliche Vorgaben

Das Thema der IT-Security und der OT-Security hat sowohl auf EU-Ebene als auch auf nationaler, deutscher Ebene an Bedeutung gewonnen. Daher wird diesem Thema hier ein eigenes Hauptkapitel gewidmet. Die Begriffe CER-Richtlinie, NIS2-Richtlinie, Cyber-Resilience-Act (CRA) und IT-Sicherheitsgesetz sind vielen Lesern inzwischen sicher ein Begriff. Aus diesem Grund werden in Kapitel 4.1 die rechtlichen Vorgaben auf EU-Ebene behandelt, in Kapitel 4.1.1 folgen dann die nationalen deutschen Vorgaben.

!	Die in den folgenden Kapiteln beschriebenen Sachverhalte bezüglich der rechtlichen Vorgaben ändern sich momentan noch stark. Viele Informationen zur Umsetzung sind noch im Entstehen begriffen. Die hier gemachten Angaben beziehen sich auf den Monat September 2025 und sind als vorläufig anzusehen. Die Sachverhalte werden sich danach auch weiter ändern.

4.1. Vorgaben auf EU-Ebene

Die Europäische Union hat in den letzten Jahren des Thema IT-Security, OT-Security und Resilienz in Form verschiedener Richtlinien adressiert. Hier sind z. B. zu nennen: Cyber-Resilience-Act (CRA), CER-Richtlinie, NIS-Richtlinie, NIS 2 Richtlinie, Cyber-Security-Act, Maschinenverordnung. Die folgenden Kapitel beschreiben übersichtsartig die für die OT-Security relevanten Teile. Es ist zu beachten, dass einige der Vorgaben (z. B. CRA, Maschinenverordnung) direkt rechtskräftig sind. Andere sind von den Mitgliedstaaten noch in nationales Recht umzusetzen (z. B. CER-Richtlinie, NIS-2-Richtlinie).

4.1.1. CER-Richtlinie

Die CER-Richtlinie der EU (Critical Entities Resilience Directive, EU 2022/2557) [CER2022] wurde eingeführt, um die physische Widerstandsfähigkeit kritischer Infrastrukturen gegenüber Bedrohungen wie Naturkatastrophen, Sabotage oder Terroranschlägen zu stärken. Die Abkürzung CER steht dabei für „Critical Entities Resilience“. Sie ersetzt die bisherige Richtlinie 2008/114/EG über kritische Infrastrukturen aus dem Jahr 2008 und verpflichtet die Mitgliedstaaten dazu, Betreiber sogenannter „kritischer Einrichtungen“ zu identifizieren und deren Resilienz durch konkrete Maßnahmen zu verbessern. Dazu gehören unter anderem Risikoanalysen, Schutzkonzepte, Krisenreaktionspläne und Meldepflichten bei Störungen. Die Richtlinie deckt elf zentrale Sektoren ab, darunter Energie, Verkehr, Gesundheit, Trinkwasser, digitale Infrastruktur und öffentliche Verwaltung. Ziel ist es, die Versorgungssicherheit und das Funktionieren der Gesellschaft auch in Krisensituationen zu gewährleisten.

Die Mitgliedstaaten müssen die Richtlinie bis Oktober 2024 in nationales Recht überführen, in Deutschland erfolgt dies über das „Gesetz zur Umsetzung der Richtlinie (EU)

2022/2557 und zur Stärkung der Resilienz kritischer Anlagen“ [BMI2024] dem sogenannte KRITIS-Dachgesetz. Die Umsetzung der CER-Richtlinie in das KRITIS-Dachgesetz ist bislang (Stand September 2025) noch nicht abgeschlossen. Seit November 2024 liegt ein Regierungsentwurf vor und wurde bereits im Bundestag beraten, doch durch den Bruch der Ampelkoalition sind die Gesetzesvorhaben vor der Neuwahl nicht abgeschlossen worden. Das bedeutet, dass der Entwurf erneut in den Bundestag eingebracht und beraten werden muss. Mit Datum 27.08.2025 wurde nun ein aktualisierter Referentenentwurf veröffentlicht [BMI2025] und am 10. September 2025 im Bundeskabinett beschlossen.

4.1.2. NIS-Richtlinie

Die NIS-Richtlinie 2016/1148 [EUR2016] des Europäischen Parlaments und des Rates wurde geschaffen, um ein „hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der EU“ zu gewährleisten. Sie war die erste europaweite Regelung zur Cybersicherheit und legte den Grundstein für eine koordinierte Sicherheitsstrategie der Mitgliedstaaten. Ziel war es, die Widerstandsfähigkeit kritischer digitaler Infrastrukturen zu stärken und die Zusammenarbeit zwischen den EU-Staaten zu verbessern. Die Richtlinie verpflichtete die Mitgliedstaaten dazu, nationale Strategien zur Cybersicherheit zu entwickeln, zentrale Anlaufstellen und Computer-Notfallteams (CSIRTs) einzurichten und Betreiber wesentlicher Dienste sowie bestimmte Anbieter digitaler Dienste zu identifizieren. Diese Unternehmen mussten Sicherheitsmaßnahmen ergreifen und erhebliche Sicherheitsvorfälle melden. Die NIS-Richtlinie 2016/1148 wurde in Deutschland durch das „Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148“ [BUN2017] vom 23. Juni 2017 in nationales Recht überführt. Dieses Gesetz (umgangssprachlich NIS-UG) passte insbesondere das BSI-Gesetz (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) an und ergänzte es um Regelungen für Betreiber kritischer Infrastrukturen sowie Anbieter digitaler Dienste.

Die NIS-Richtline wurde im Jahr 2022 durch die NIS-2-Richtlinie abgelöst. Siehe hierzu das folgende Kapitel 4.1.3.

4.1.3. NIS2-Richtlinie

Die Richtline NIS2 (EU 2022/2555) [NIS-2_de] ist seit Anfang 2023 in der EU in Kraft. Sie ist der europäische Rahmen für Betreiber Kritischer Infrastrukturen und legt Cyber-Security Mindeststandards in der EU fest. NIS2 erweitert Betroffenheit und Pflichten für die Unternehmen deutlich. Im Wesentlichen sind folgende Änderungen relevant:

Sektoren: Die kritischen Essential Entities erhöhen sich auf elf Sektoren, die Important Entities wachsen auf sieben Sektoren — auf insgesamt achtzehn NIS2 Sektoren.

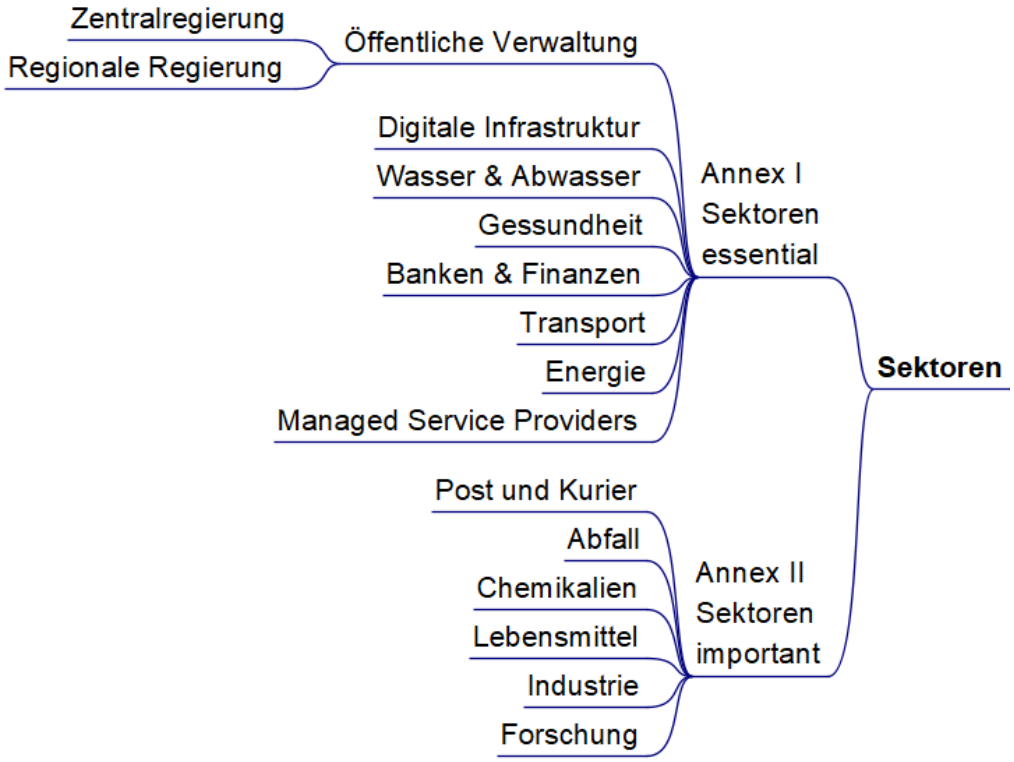

Abbildung 11: NIS2-Sektoren

Abbildung 11 zeigt die Sektoren der wesentlichen (essential) und wichtigen (important) Unterhemen. Wichtig ist, dass im Sektor „Industrie“ auch die chemische Industrie und die Automobilherstellung enthalten sind.

Betreiber: Medium und Large Enterprises ab 50 Mitarbeiter/10 Mio. EUR Umsatz sind betroffen, ohne Anlagen-Schwellenwerte.

Cyber Security: Die Anforderungen an Betreiber und Mitgliedstaaten steigen, Cyber Security muss auch in Lieferketten betrachtet werden. Betreiber in der EU müssen mindestens folgende Cyber Security Maßnahmen umsetzen, um die IT und Netzwerke ihrer kritischen Dienstleistungen zu schützen: Art. 21.

- Policies: Richtlinien für Risiken und Informationssicherheit.
- Incident Management: Prävention, Detektion und Bewältigung von Cyber Incidents.
- Business Continuity Management: BCM mit Backup Management, Krisen-Management.
- Supply Chain: Sicherheit in der Lieferkette — bis zur sicheren Entwicklung bei Zulieferern.
- Einkauf: Sicherheit in der Beschaffung von IT und Netzwerk-Systemen.
- Effektivität: Vorgaben zur Messung von Cyber und Risiko Maßnahmen.
- Training: Cyber Security Hygiene.
- Kryptographie: Vorgaben für Kryptographie und wo möglich Verschlüsselung.
- Personal: Human Resources Security.
- Zugangskontrolle.
- Asset Management.

- Authentication: Einsatz von Multi-Faktor-Authentisierung und SSO.
- Kommunikation: Einsatz sicherer Sprach-, Video- und Text-Kommunikation.
- Notfall-Kommunikation: Einsatz gesicherter Notfall-Kommunikations-Systeme.

Kooperation: Die Aufsicht und Zusammenarbeit in der EU zwischen Behörden und Betreibern werden vertieft, europäische Jurisdiktion geschärft.

Sanktionen: Strafen und Enforcement-Actions werden deutlich ausgeweitet – auf Maximalstrafen von mind. 7 oder 10 Mio. EUR, je nach Sektor.

Die EU-Mitgliedsstaaten müssen den Mindeststandard von NIS2 durch nationale Gesetze umsetzen. Weitere Informationen hierzu finden sich in Kapitel 4.2.3.

4.1.4. Cyber-Resilience-Act

Der Cyber-Resilience-Act (CRA) [CRA2024] wurde am 20.11.2024 veröffentlicht und ist am 11.12.2024 in Kraft getreten. Er betrifft Hersteller von Geräten mit digitalen Elementen, die über eine Kommunikationsverbindung (direkt oder indirekt) verfügen.

Der Anwendungsbeginn des CRA ist 36 Monate nach dem Termin des Inkrafttretens. Das bedeutet:

- Ab dem 11. September 2026 sind aktiv ausgenutzte Schwachstellen an nationale Behörden und die ENISA zu melden. Siehe Artikel 14.
- Ab dem 11. Dezember 2027 gelten alle Anforderungen des CRA. Das CE-Kennzeichen dokumentiert dann, dass ein Produkt mit digitalen Elementen die Anforderungen des CRA erfüllt.

Abbildung 12 fasst die Zeitschiene des CRA zusammen.

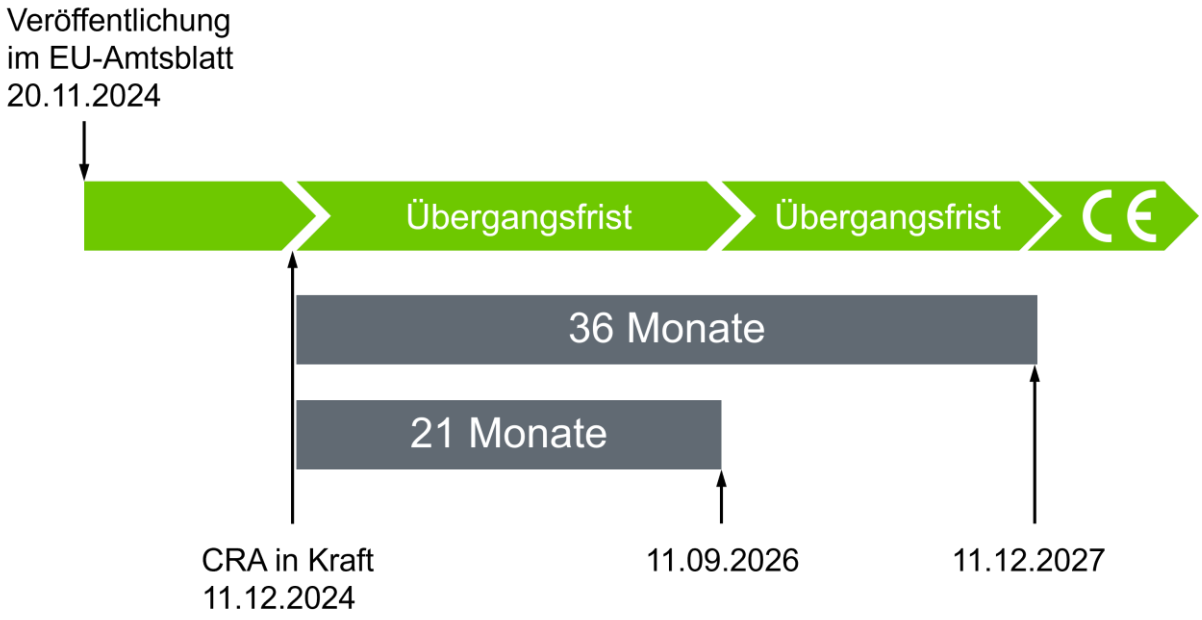

Abbildung 12: Zeitschiene des CRA

Die wesentlichen Aspekte des CRA betreffen laut [KIR2022] die Definition von Cybersicherheitsvorschriften für das Inverkehrbringen von Hardware und Software in der EU. Hierbei werden Verpflichtungen für Hersteller, Vertreiber und Importeure definiert. Dies sind im Wesentlichen Anforderungen an die Cybersicherheit während des gesamten Lebenszyklus (mindestens 5 Jahre). Die zu befolgende harmonisierte Normen befinden sich zurzeit in der Erstellung. Ziel dieser Normen ist das Ermöglichen einer nach Risikoniveau differenzierten Konformitätsbewertung. Es ist davon auszugehen, dass die Normen im Wesentlichen auf der Normreihe IEC 62443 basieren werden.

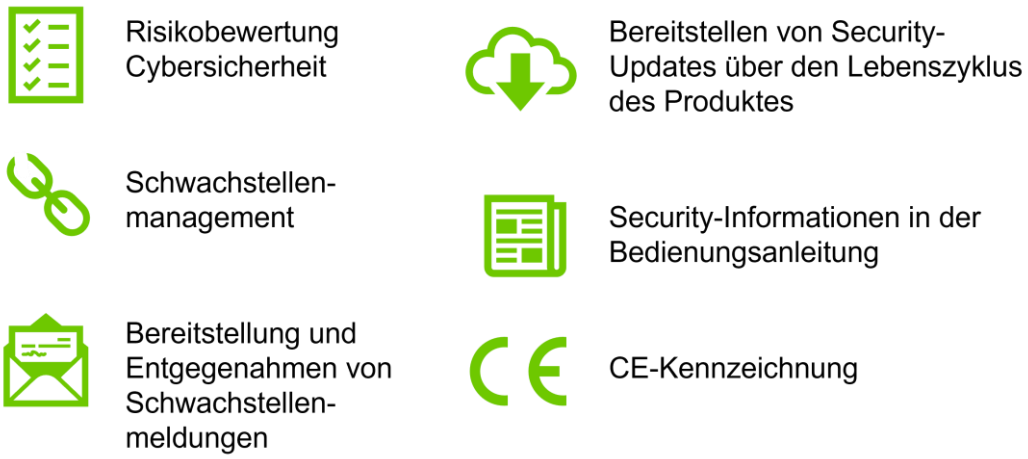

Abbildung 13: Pflichten der Hersteller gemäß CRA

Abbildung 13 zeigt die wesentlichen Pflichten der Hersteller gemäß CRA. Für die Betreiber und Planer von Produktionsanlagen ist der CRA insofern relevant, als man seitens der Hersteller ab dem Stichtag 11.12.2027 mit der Erfüllung definierter OT-Security-Anforderungen rechnen kann. Dies unterstützt auch die in der NIS2-Richtlinie geforderte Security entlang der Lieferkette.

4.1.5. Maschinenverordnung

Die EU-Maschinenverordnung [EUR2023] befasst sich im Wesentlichen mit den Aspekten der Funktionalen Sicherheit (Safety). Sie wird dennoch an dieser Stelle genannt, weil sie in Anhang III Abschnitte 1.1.9 und 1.2.1 den Schutz vor Korrumpierung und die Sicherheit und Zuverlässigkeit von Steuerungssystemen adressiert. Somit ist auch die Maschinenverordnung in Bezug auf die OT-Security relevant.
Die EU-Maschinenverordnung ist verabschiedet. Es ist keine Umsetzung in nationales Recht erforderlich. Es läuft zurzeit eine 42-monatige Übergangsfrist, die Verordnung ist spätestens ab dem 20.01.2027 anzuwenden. Die Maschinenverordnung löst die bisherige Maschinenrichtlinie 2006/42 ab [EUR2006]. Zur Vertiefung wird das Buch [HÜN2024] empfohlen.

4.2. Nationale deutsche Vorgaben

Die nationale deutsche Gesetzgebung hat mit dem IT-Sicherheitsgesetz [ITSichG2015] erste Regelungen zur OT-Security in kritischen Infrastrukturen erlassen. Durch die

europäische Gesetzgebung kommt nun noch der Bedarf hinzu die CER-Richtlinie (siehe Kapitel 4.1.1) und die NIS2-Richlinie (siehe Kapitel 4.1.3) in nationales Recht umzusetzen. Die folgenden Kapitel geben einen kurzen Überblick über die nationale, deutsche Gesetzgebung.

4.2.1. IT-Sicherheitsgesetz und BSI Kritisverordnung

Mit dem IT-Sicherheitsgesetz [ITSichG2015] aus dem Jahr 2015 definierte der Gesetzgeber Vorgaben in Bezug auf die IT-Sicherheit kritischer Infrastrukturen (KRITIS). Die Definition der kritischen Infrastrukturen war seinerzeit durch eine gesonderte Rechtsverordnung [BSI-KritisV_2016] geregelt. In der damaligen Ausgabe fielen die folgenden Infrastrukturen unter die Verordnung: Stromversorgung, Gasversorgung, Kraftstoff und Heizölversorgung, Fernwärmeversorgung, Abwasserbeseitigung, Trinkwasserversorgung. Die Verordnung definierte Schwellenwerte für die Versorgungseinrichtungen. So fielen z. B. Kläranlagen ab 500 000 Einwohnerwerten oder Kraftwerke ab 420 MW Nennleistung unter die Verordnung.

Im Rahmen des IT-Sicherheitsgesetzes wird beim Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Meldestelle für Vorfälle eingerichtet und eine Meldepflicht für kritische Vorfälle definiert.

Weiterhin legt das Gesetz fest:

> *„Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtverordnung nach §10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind.“* [ITSichG2015]

Die Betreiber Kritischer Infrastrukturen wurden zudem verpflichtet eine Kontaktstelle einzurichten und mussten die Erfüllung der Anforderungen nachweisen. Darüber hinaus sind im [ITSichG2015] eine Reihe weiterer Änderungen an anderen Gesetzen zusammengefasst, welche einen Bezug zum Thema kritische Infrastrukturen und IT-Sicherheit haben.

Im Jahr 2021 wurde das IT-Sicherheitsgesetz 2.0 [IT_SIG_2.0] veröffentlicht, welches das Gesetz aus dem Jahr 2015 aktualisierte. Der Kreis der betroffenen Unternehmen wurde erweitert, die Siedlungsabfallentsorgung wurde als kritische Infrastruktur aufgenommen. Systeme zur Angriffserkennung wurden vorgeschrieben. Die zugehörige Verordnung wurde inzwischen durch die „Dritte Verordnung zur Änderung der BSI-Kritisverordnung“ [BUN2023] abgelöst. Hier wurden z. B. auch Entladeterminals für Flüssiggas als kritische Infrastruktur definiert.

In Anbetracht der zu erwartenden Umsetzungsgesetze zur CER- und NIS2-Richtlinie ist zu erwarten, dass auch das IT-Sicherheitsgesetz angepasst werden muss, damit durch die drei Gesetze keine Widersprüche oder Mehrfachregelungen entstehen.

4.2.2. KRITIS-Dachgesetz

Gesetz zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen“ [BMI2024] das sogenannte KRITIS-Dachgesetz wurde in Kapitel 4.1.1 beschrieben.

4.2.3. NIS2-Umsetzungsgesetz

Das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz [NIS2UmsuCG] wurde Ende 2024 vom Bundeskabinett verabschiedet und sollte anschließend im Bundestag verabschiedet werden. Durch die Regierungsumbildung Ende 2024 konnte das Gesetzesvorhaben nicht abgeschlossen werden. Ein aktualisierter Referentenentwurf mit leicht geändertem Namen befand sich seit 23. Juni 2025 in der Verbändeabstimmung. Am 11.09.2025 hat der Deutsche Bundestag das NIS2-Umsetzungsgesetz [NIS2_DE_2025] in der Version vom 08.09.2025 in erster Lesung beraten.

5. Maßnahmen zur Umsetzung der OT-Security in der Produktion

In Kapitel 3 wurde eine Übersicht über die für die OT-Security relevanten Normen und Standards gegeben, in Kapitel 4 folgte eine Zusammenfassung der rechtlichen Rahmenbedingungen. Betreiber und Planer von Produktionsanlagen stehen nun vor der Aufgabe, hieraus ein entsprechendes Vorgehen abzuleiten. Das Problem für KMU ist jedoch, dass diese Normen- und Gesetzeswerke sehr umfangreich und teilweise noch unvollständig sind. Daher fällt es den Mitarbeitenden in KMU häufig schwer, zu einer Beurteilung in Bezug auf das eigene Unternehmen zu kommen.

Ein sinnvolles Vorgehen ist daher zunächst eine Bestandsaufnahme vorzunehme, mit die Ist-Situation beschreiben zu können. Eine erste Einschätzung kann ein Quick-Check liefern (z. B. www.vds-quick-check.de), der eine erste Einstufung des Unternehmens in Bezug auf die IT-Sicherheit liefert. Es stehen auf dieser Webseite je ein Check für den Office- und den Produktionsbereich zur Verfügung. Vergleichbare Checks zur Bestandsaufnehme im OT-Bereich gibt es auch von der ISACA [ENN2021] oder das Tool SiToM [MIT2025a] von Mittelstand Digital.

Um KMU einen einfachen Einstieg in die IT-Sicherheit im Produktionsbereich zu ermöglichen, wird im Folgenden ein Zehn-Punkte-Plan für die Etablierung der IT-Sicherheit im Produktionsbereich als eine initiale Maßnahme vorgeschlagen. Diese zehn Punkte sind:

1. Management Commitment
2. Organisation der Zuständigkeiten und Prozesse
3. Erstellung einer Richtlinie
4. Personal
5. Beschaffung und Bereitstellung von Wissen
6. Identifizierung, Bewertung und Schutz der Assets
7. Regelung des externen Zugriffs auf Produktionsanlagen
8. Datensicherung
9. Behandlung von Störungen und Ausfällen
10. IT-Sicherheitsvorfälle erkennen

Die folgenden Kapitel werden sich mit diesen zehn Punkten befassen und notwendige Maßnahmen für die Etablierung eines IT-Sicherheitsprozesses im Produktionsbereich beschreiben. In der Regel fokussiert sich die Literatur stark auf die Punkte 6 und 7. Es ist jedoch festzuhalten, dass die IT-Sicherheit als gesamtheitlicher Prozess unter Einbeziehung aller Punkte anzusehen ist.

5.1. Management Commitment

Die IT-Sicherheit muss als Top-Down Prozess im Unternehmen etabliert werden. Nur durch ein entsprechendes Commitment des Managements ist eine Durchsetzung im

Unternehmen sinnvoll. Hierfür sollte das Management eine IT-Sicherheitsstrategie für das Unternehmen verfassen (lassen), welche den Office- und den Produktionsbereich umfasst. Die Strategie sollte klare Ziele und entsprechende Verantwortlichkeiten definieren.
Für dieses Vorgehen werden die folgenden Punkte als erster Schritt empfohlen:

- Etablierung eines Top-Down-Prozesses zur Etablierung der OT-Security im Unternehmen.
- Nutzung von Synergien zwischen IT- und OT-Security
- Erstellung einer OT-Security-Strategie.
  - Definition von Zielen.
  - Definition von Verantwortlichkeiten.

- Anstoß eines Projektes für die Bearbeitung der Aufgaben.
- Definition von Zuständigkeiten.
- Bereitstellung von Ressourcen:
  - Intern.
  - Gegebenenfalls extern.
  - Personell und finanziell

Es wird empfohlen für die Initiierung des Prozesses ein Projekt zu definieren und es mit den erforderlichen internen und ggf. auch externen Ressourcen auszustatten. Das hier beschriebene Vorgehen ist vergleichbar zur Einführung eines Qualitätsmanagementprozesses.

5.2. Organisation der Zuständigkeiten und Prozesse

Nach dem Projektstart sind durch das Management entsprechende Verantwortlichkeiten zu definieren. Da die OT-Security als übergreifender Prozess zu sehen ist, sollte eine Gesamtverantwortung in Form eines IT-Sicherheitsbeauftragten (engl. Chief Information Security Officer – CISO) definiert werden der IT- und OT-Security verantwortet. Es ist sicherzustellen, dass die Person über das erforderliche Wissen im Office- und im Produktionsbereich verfügt. Ggf. kann der IT-Sicherheitsbeauftragte Aufgaben delegieren. Der IT-Sicherheitsbeauftragte sollte gemeinsam mit weiteren Mitarbeitern und einem Vertreter des Managements das Informationssicherheitsteam bilden. Dieses Team ist für die Umsetzung der IT-Sicherheitsstrategie und für die Behandlung von Störungen, Ausfällen und IT-Sicherheitsvorfällen verantwortlich.

Basis für die Organisation von IT- und OT-Security ist ein so genanntes Informationssicherheitsmanagementsystem (ISMS). Das BSI schreibt dazu im Grundschutzmodul IND.1: Prozessleit- und Automatisierungstechnik im Teil A1 und folgende [BSI2021c]:

- „Ein Informationssicherheits-Managementsystem (ISMS) für den Betrieb der OT-Infrastruktur MUSS entweder als selbständiges ISMS oder als Teil eines Gesamt-ISMS existieren und MUSS in seinem Geltungsbereich die Definition von Zielen und Werten, Prozessen, Rollen, Verantwortlichkeiten und Vorgaben für die OT explizit umfassen.

- Die Leitungsebene der Institution MUSS den Sicherheitsprozess initiieren, steuern und kontrollieren. Die Institution MUSS eine Sicherheitsorganisation aufbauen, welche die Rollen und Verantwortlichkeiten für die Informationssicherheit der OT-Infrastruktur und -Komponenten regelt.
- Es MUSS ein Gesamtverantwortlicher für die Informationssicherheit im OT-Bereich bestimmt und innerhalb der Institution bekannt gegeben werden.
- Es MUSS ein Prozess existieren, wie konkrete Vorgaben (Richtlinien) für bestimmte Themenbereiche im Prozessbereich verfasst, kommuniziert, zur Umsetzung gebracht, fortgeschrieben, bewertet und verbessert werden."

Zur Sicherstellung einer kontinuierlichen Arbeit ist dem Thema /dem Projekt entsprechendes Personal zuzuordnen. Die Berichtswege sind zu definieren. Die Delegation von Aufgaben und die Einbindung des Top-Managements müssen ebenfalls geregelt sein. Sowohl die NIS2-Richtlinie [NIS-2_de] als auch die [DIN_EN_ISO/IEC_27001] definieren die Verantwortung des Top-Managements in Bezug auf die IT- und OT-Security. Es ist zu beachten, dass auch Lieferanten und Systemintegratoren in die Prozesse mit einzubeziehen sind.

5.3. Erstellung von Richtlinien

Das Thema OT-Security ist vom Unternehmen in einer oder mehreren entsprechenden Richtlinien, die dem Personal grundlegende Verhaltensregeln aufgeben, zu beschreiben. Nur wenn das Personal weiß, was von ihm in Bezug auf die IT-Sicherheit erwartet wird, kann es sich entsprechend verhalten. Beispiele für Themen der Richtlinie(n) könnten sein:

- Grundlegende Verhaltensregeln im Produktionsbereich:
  - Privatnutzung.
  - Einbringen von Softwareaktualisierungen in die Produktionsanlage.
  - Vorherige Prüfung von SW-Aktualisierungen.
- Umgang mit Schutzeinrichtungen.
- Weitergabe Zugangskennungen.
- Informationsfluss bei Abwesenheit.
- Missbrauchskontrolle.
- Regelungen für Lieferanten/ Integratoren

Die Richtlinie sollte auch klarstellen, dass eine Missbrauchskontrolle erfolgt und dass bei Fehlverhalten mit Sanktionen zu rechnen ist. Entsprechende Abstimmungen mit dem Betriebsrat sind in der Regel erforderlich.

5.4. Personal

Das Personal ist für die OT-Security ein entscheidender Faktor. Durch ein adäquates Knowhow und eine Ausbildung des Personals kann ein entscheidender Beitrag zur OT-Security im Unternehmen erfolgen.

Das BSI schreibt im Grundschutzmodul IND.1 im Teil A2 Sensibilisierung und Schulung des Personals [BSI2021c] dazu:

- „Betriebspersonal MUSS regelmäßig zu relevanten IT-Sicherheitsbedrohungen im OT-Bereich informiert und sensibilisiert werden. OT-Verantwortliche MÜSSEN regelmäßig zur Bedrohungslage und Handlungsbedarfen informiert oder geschult werden."

Es sei and dieser Stelle auch auf die Schulungspflicht für Geschäftsleitungen gemäß der NIS2-Richtlinie [ATU2025] hingewiesen.

Bei Eintritt in das Unternehmen ist eine Vertraulichkeitserklärung durch den Mitarbeiter bzw. die Mitarbeiterin zu unterzeichnen. In der Einarbeitungsphase sind neue Mitarbeiter in die Richtlinien zur OT-Security und evtl. weitere Richtlinien einzuweisen.

Bei dem Ausscheiden von Mitarbeitern sind entsprechende Maßnahmen zu treffen. VPN-Zugänge dieser Mitarbeiter sind zu sperren, Passworte sind zu ändern. Das gilt auch für Schichtzugänge.

5.5. Beschaffung und Bereitstellung von Wissen

In einer Befragung zur Auswertung von Security-Advisories im Produktionsumfeld durch KMI [WUL2022] zeigte sich, dass nur 50% der befragten Unternehmen Security-Advisories der Automatisierungstechnik-Hersteller überwacht und auswertet. Aus diesem Grund ist im Unternehmen ein Prozess zu etablieren, der die Beschaffung entsprechender, aktueller Informationen für das Unternehmen gewährleistet. Mögliche Quellen für die Beschaffung von Informationen über Schwachstellen können sein:

- Informationen der Hersteller der Automatisierungssysteme. Zum Beispiel:
  - z. B. ABB [ABB2025]
  - z. B. Siemens [SIE2025]
  - z. B. Wago über CERT@VDE: [WAG2025]

- Konsolidierte Informationen über Schwachstellen (IT und OT)
  - Informationen von ICS-CERT (Homeland Security der U.S.A) bezüglich bekannter Schwachstellen von Automatisierungssystemen [DHS2025]
  - CVE Common Vulnerabilities and Exposures [MIT2025b]
  - European Union Vulnerability Database [ENI2025]

Die Aktualität des Wissens ist sicherzustellen. In einigen Fällen besteht die Möglichkeit Alerts (Meldungen über vom Hersteller erkannte Schwachstellen) für bestimmte Systeme über einen E-Mail-Verteiler zu abonnieren. Im Unternehmen sind Personen zu benennen, welche diese Meldungen auswerten und Maßnahmen für das Unternehmen daraus ableiten.

Die Überwachung und Auswertung von Schwachstellenmeldungen ist zeitaufwändig. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) propagiert daher seit einiger Zeit die Bereitstellung von Schwachstellenmeldungen in maschinenlesbarer Form über das Common Security Advisory Framework (CSAF) [BSI2025a]. Dies würde in Verbindung mit einer Asset-Datenbank des Betreibers eine automatisierte Auswertung und Zuordnung der Schwachstellenmeldungen ermöglichen.

Neben dem spezifischen Wissen in Bezug auf bekannte Schwachstellen ist das allgemeine Wissen der Mitarbeiterinnen und Mitarbeiter durch Sensibilisierung, Aus- und Weiterbildung zu etablieren und auf einem aktuellen Stand zu halten.

5.6. Identifizierung, Bewertung und Schutz der Assets

Dieser Abschnitt beschreibt wie die Assets einer Produktionsanlage systematisch erfasst, in Bezug auf Ihr Risiko bewertet und bei Bedarf geschützt werden. Hierbei wird gemäß der Normreihe VDI 2182 vorgegangen. Die Normreihe IEC 62443 gibt ein vergleichbares Vorgehen wieder. Für die Analyse des Automatisierungssystems wird in den in Abbildung 10 dargestellten Schritten vorgegangen. Kapitel 3.2.2 beschreibt den „Plan-Do-Check-Act-Zyklus“ (PDCA) und die notwendigen Schritte.

Das Ergebnis dieser Analyse ist:

- Liste aller Assets
- Aufstellung der Bedrohungen, welche auf die Assets wirken in Form einer Bedrohungsmatrix.
- Liste aller relevanten Schutzziele in Form einer Bedrohungsmatrix mit relevanten Schutzzielen.
- Liste der bewerteten Risiken, welche auf die Assets wirken.
    - Die Normreihe VDI 2182 macht Vorschläge für den Aufbau derartiger Listen.
- Liste von möglichen Schutzmaßnahmen und Bewertung von deren Wirksamkeit und deren Kosten.
- Liste der ausgewählten und zu realisierenden Schutzmaßnahmen.
- Bericht über die Umsetzung der Schutzmaßnahmen
- Ergebnisse des Prozessaudits zur Beurteilung der Wirksamkeit der gewählten Maßnahmen.

Typische Schutzmaßnahmen, die das Ergebnis des beschriebenen Prozesses sind, resultieren in der Regel in einem so genannten Defense in Depth Konzept [DHS2016], [KUI2006]. Die folgenden Abbildungen zeigen exemplarisch ausgewählte Bestandteile eines Defense in Depth Konzeptes.

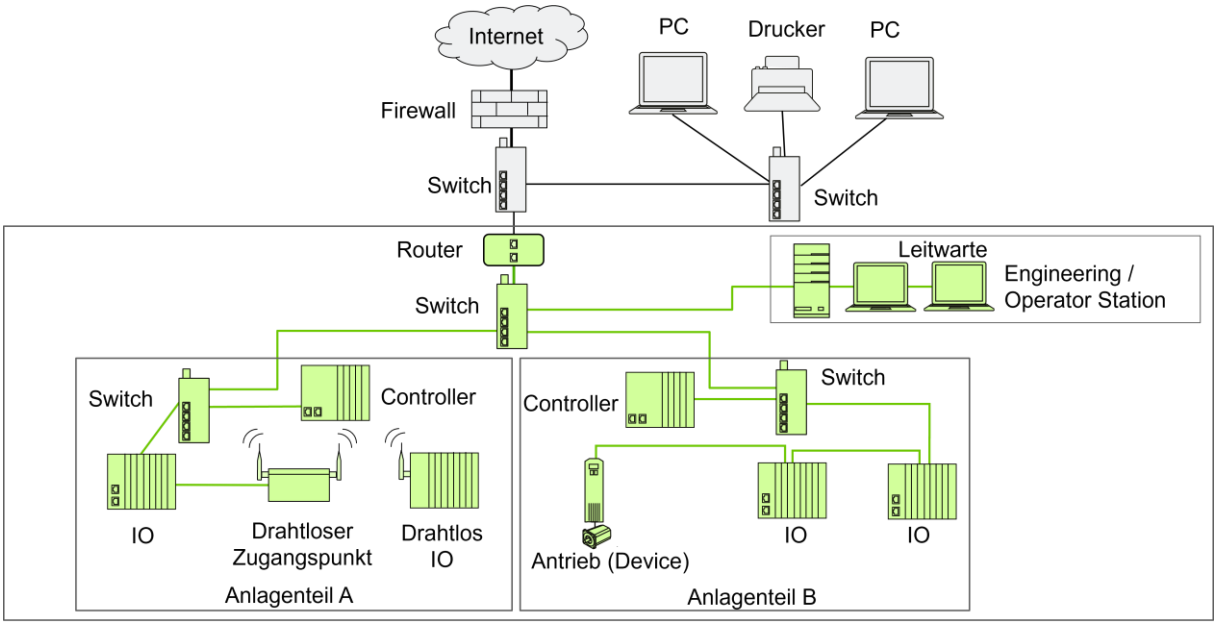

Abbildung 14: Beispielanlage mit Office und Produktionsbereich

Abbildung 14 zeigt eine aus den zwei Anlagenteilen A und B bestehende Produktionsanlage. Oberhalb der Produktionsanlage ist der Bereich der Leitwarte (engl. Control Room) angesiedelt. Darüber ist der Office-Bereich dargestellt. Es wird davon ausgegangen, dass das Unternehmen durch eine Firewall vom Internet getrennt ist. Eine Verbindung zum Internet wird z. B. für den Bezug von Software-Updates oder für die Speicherung von Daten in der Cloud benötigt.

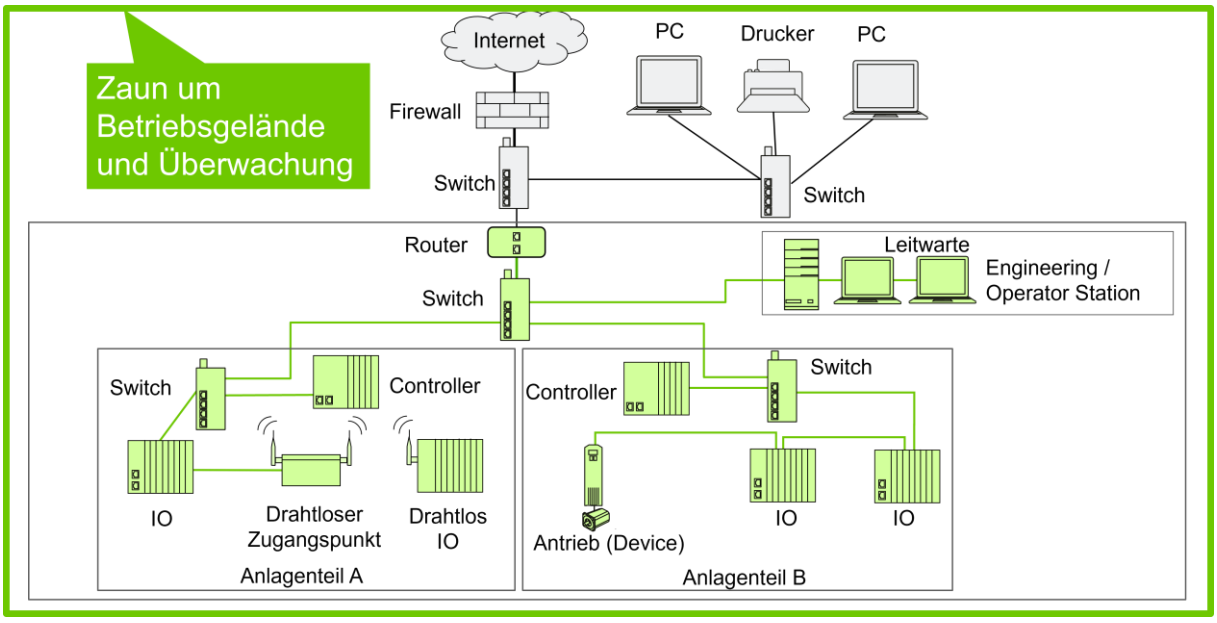

Abbildung 15: Perimeterschutz

Als erste Maßnahme kann, wie in Abbildung 15 dargestellt, die gesamte Liegenschaft gegen Eindringen von außen, z. B. durch einen Zaun geschützt werden. Diese Maßnahme verhindert den Zugang unautorisierter Personen zum Werksgelände und stellt die erste Barriere für Angreifer dar. Es ist zu berücksichtigen, dass eine Überwachung des Zauns, z. B. durch eine KI-gestützte Videoüberwachung, so wie in [SEC2024]

beschrieben, sinnvoll ist. Der Perimeterschutz ist auch Bestandteil der CER-Richtlinie [CER2022]. Unternehmen, welche unter diese Richtlinie fallen, sollten daher die CER-Richtlinie bei der Auswahl des Perimeterschutzes berücksichtigen.

Seit dem Jahr 2008 ist ein Vorfall bekannt, bei dem ein Cyber-Angreifer einen doppelten Zaun überwinden und durch einen Cyber-Angriff ein Kraftwerk stilllegen konnte [PAN2008]. Das bedeutet, dass der Zaun nur eine von mehreren ineinandergreifenden Maßnahmen sein kann. Für Funkwellen stellt ein Zaun kein Hindernis dar. Bei Verwendung von drahtloser Kommunikation in der Produktionsanlage ist eine entsprechende Risikobetrachtung erforderlich. Dies gilt insbesondere, wenn die Funkstrecke in der Nähe der Einzäunung liegt.

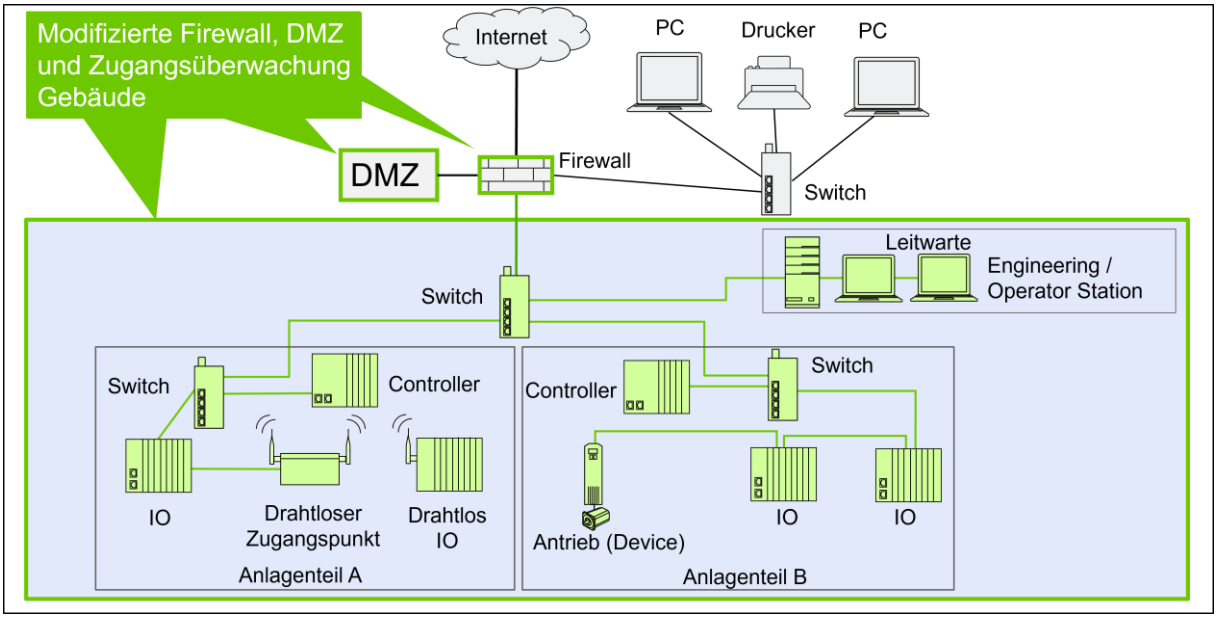

Abbildung 16: Modifizierte Firewall, DMZ und Zugangsüberwachung Gebäude

Abbildung 16 zeigt als nächste Schutzmaßnahme eine geänderte Konfiguration der Firewall. Diese wird nun so konfiguriert, dass ein Zugang zum Automatisierungssystem (blauer Hintergrund) von außerhalb der Firma nicht zulässig ist. Gleichzeitig werden für den Betrieb der Anlage notwendige Verbindungen in den Office-Bereich zugelassen. Diese Trennung ist in der [DIN_EN_IEC_62443-3-3] unter dem Stichwort „Schutz der Zonengrenze“ vorgegeben. Die Funktion des Routers kann von der Firewall ebenfalls übernommen werden. Der Router entfällt daher.

An dieser Stelle kann auch eine demilitarisierte Zone (DMZ) an die Firewall angebunden werden. Diese dient der Trennung von IT- und OT-Netzwerk. Sie bilden eine isolierte Netzwerkzone zwischen dem „unsicheren“ externen Netzwerk – etwa dem Internet oder dem Unternehmensnetz – und dem besonders schützenswerten Produktionsnetzwerk. In dieser Zwischenzone werden typischerweise Dienste wie Remote-Zugänge, Datenablagen oder Update-Server betrieben, die sowohl mit der Außenwelt als auch mit der Produktionsumgebung kommunizieren müssen. Durch diese Trennung wird verhindert, dass ein erfolgreicher Angriff auf öffentlich erreichbare Systeme direkten Zugriff auf die Produktionsanlagen ermöglicht. Die DMZ fungiert dabei als Puffer.

Als weitere Maßnahme wird gemäß Abbildung 16 eine Zugangsüberwachung für das Gebäude installiert, in dem sich die Produktionsanlage befindet. Durch diese Maßnahmen wird der Produktionsbereich vom Office-Bereich und vom Internet datenmäßig getrennt. Zusätzlich zum Zaun um das Werksgelände ist ein zweiter, enger gefasster Zugangsschutz realisiert worden.

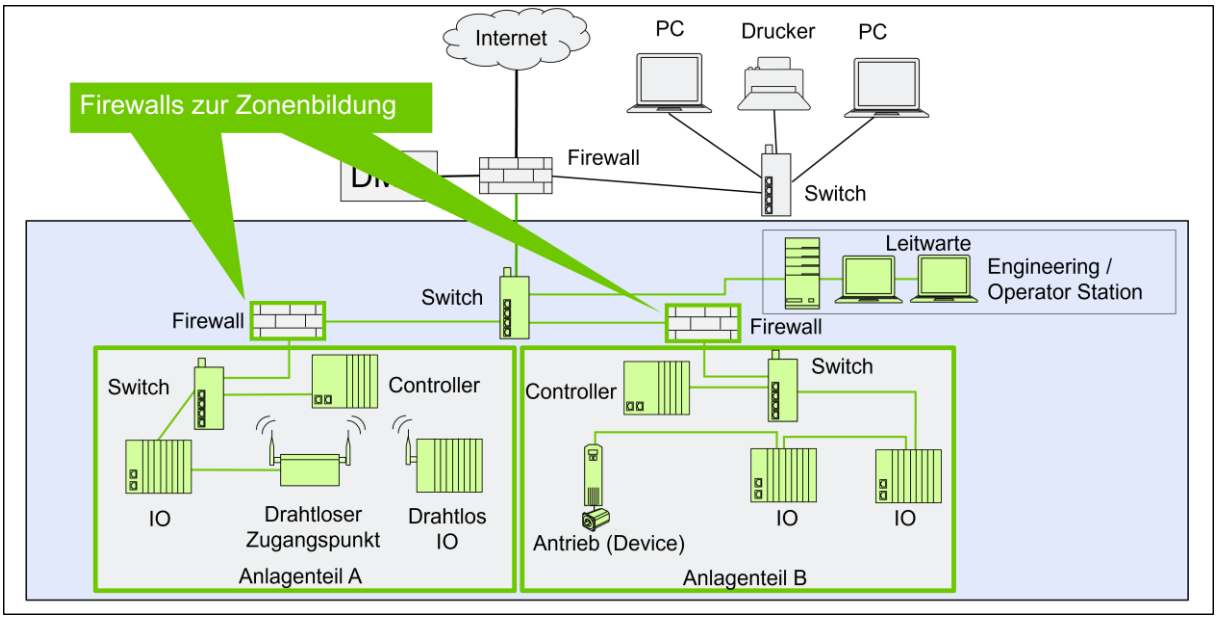

Abbildung 17: Einteilung des Produktionsbereichs in Zonen

Abbildung 17 zeigt eine weitere Untergliederung der Produktionsanlage. Die Produktionsanlage wird in zwei Teilbereiche unterteilt (grauer Hintergrund). Jeder dieser Bereiche wird wiederum über eine Firewall vom Leitwartenbereich getrennt. Zusätzlich könnten die Komponenten in den Teilbereichen z. B. durch Einbau in einen verschlossenen Schaltschrank weiter geschützt werden.

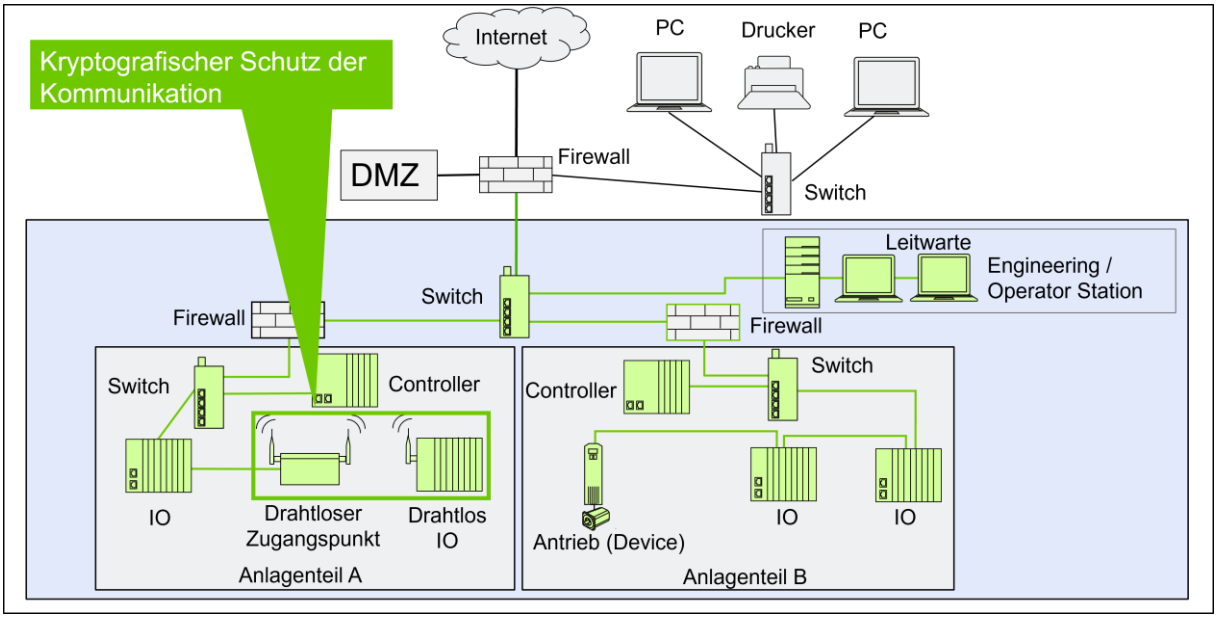

Abbildung 18: Kryptographischer Schutz der Kommunikation

Abbildung 18 zeigt die Schutzmaßnahme für einen drahtlosen Zugangspunkt durch Verschlüsselung. Auch wenn marktgängige WLAN-Access-Points standardmäßig eine Verschlüsselung bieten, ist auf die Wahl eines ausreichend sicheren Verfahrens und auf ausreichend starke Passworte zu achten.

Neben dem standardmäßig vorhandenen Schutz der WLAN-Kommunikation wird künftig auch die Möglichkeit bestehen, die drahtgebundene Kommunikation kryptografisch zu sichern. PROFIBUS & PROFINET International (PI) haben für das Kommunikationsprotokoll PROFINET ein Security-Konzept entwickelt, welches Integrität und Authentizität und bei Bedarf auch die Vertraulichkeit der PROFINET-Kommunikation schützt. Nähere Informationen zu PROFINET siehe [NIE2023b], [PNO2019a], [WAL2023].

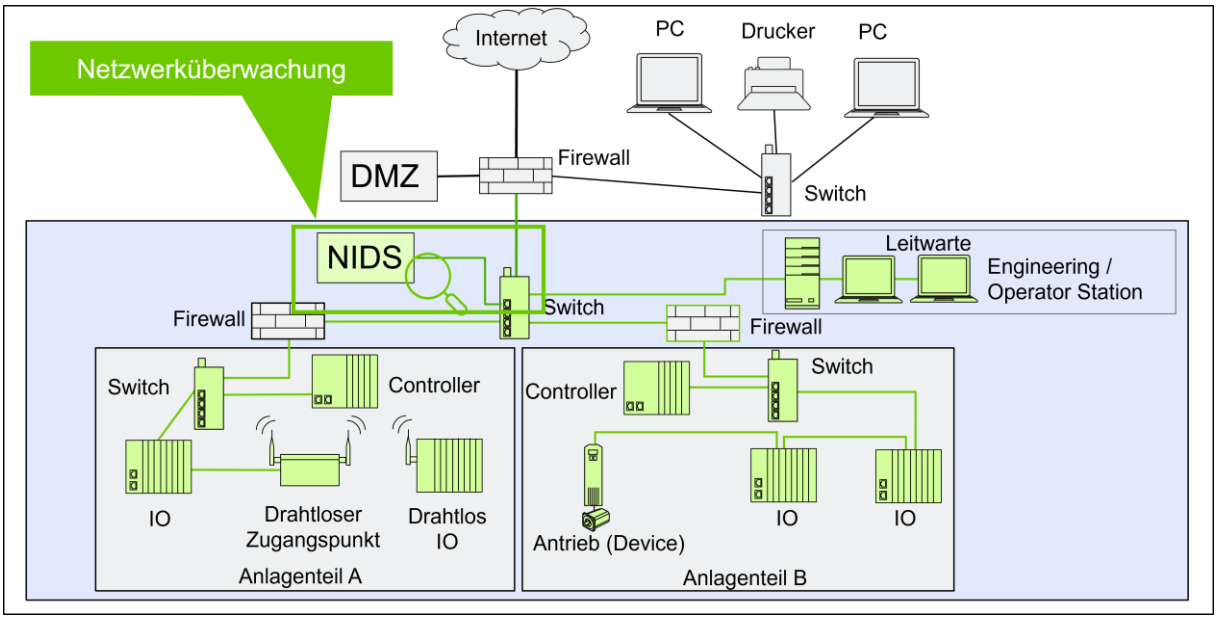

Abbildung 19: Netzwerküberwachung

Abbildung 19 zeigt als letzte Maßnahme die Überwachung z. B. über ein Netzwerküberwachungssystem. Ein Netzwerküberwachungssystem (Network Intrusion Detection System-NIDS bzw. Intrusion Detection System-IDS) überwacht an bestimmten Stellen den Netzwerkverkehr auf Anomalien. Die kontinuierliche Überwachung des Automatisierungssystems ist in der Anforderung SR6.2 der [DIN_EN_IEC_62443-3-3] enthalten. Dabei ist ein NIDS eine von mehreren Möglichkeiten.

Die hier vorgestellten Maßnahmen stellen einige exemplarische Beispiele dar. Es existieren weitere Maßnahmen, auf die an dieser Stelle aus Platzgründen nicht weiter eingegangen wird. Beispiele hierfür sind z. B:

- Virenschutz /Anti-Malware / Endpoint-Protection.
- Applikations-Whitelisting.
- Zugangsbeschränkung für transportable Medien.
- Authentifizierung von Personal und Netzwerketeilnehmern.
- Begrenzung des Zugangs zum Netz durch Abschalten unbenutzter Netzwerk-Ports (Härtung).

Obwohl dieser Teil des Zehn-Punkte-Programms der aufwendigste ist, sollten die anderen Punkte nicht gegenüber diesem Teil vernachlässigt werden.

5.7. Regelung des externen Zugriffs auf Produktionsanlagen

Der externe Zugriff auf Produktionsanlagen für Remote-Diagnose- und Remote-Wartungs-Zwecke ist aus Sicht der OT-Security ein besonders kritischer Vorgang. Aus diesem Grund wird dieses Thema in einem separaten Abschnitt beschrieben.

Bekannte Vorfälle dieser Art gehen auf die Nutzung von Remote-Zugängen zurück [TOF2009] [SAN2016] [PIT2023]. In [CLA2024a] werden weitere Angriffe über Remote-Zugänge dokumentiert. Aus diesem Grund gelten für diese Zugänge besondere Sicherheitsmaßnahmen. Eine gute Orientierung kann des BSI-Grundschutzmodul IND.3.2 Fernwartung im industriellen Umfeld [BSI2022a] geben. Hier beschreibt das BSI die grundlegenden Vorgehensweisen für die Errichtung von Remote-Zugängen. Die wesentlichen Vorgaben des BSI sind:

- Einheitliche Lösung errichten. Dies standardisiert die verwendete Hardware und die genutzten Prozesse und reduziert so den Verwaltungsaufwand.
- Anordnung der Fernwartungskomponenten in einer vorgelagerten Zone (DMZ)
- Kein pauschaler Zugriff auf ein ganzes (Sub-) Netz sondern nur auf dedizierte Endpunkte.
- Aufbau der Verbindung aus dem Unternehmen heraus nach außen.
- Einsatz dedizierter Systeme, die nur für diesen Zweck verwendet werden.
- Es werden ausschließlich etablierte Protokolle wie IPsec, SSH oder SSL/TLS in aktuellen Versionen eingesetzt, um einen Tunnel zwischen zwei Endpunkten bzw. Netzen herzustellen.
- Die Verbindung zwischen Unternehmen und Diagnosestelle ist zu verschlüsseln. Es werden hinreichend starke kryptographische Verfahren zur Verschlüsselung verwendet.
- Es sollte nur ein Benutzer pro Account vorgesehen werden. Gruppen-Accounts sind unbedingt zu vermeiden.
- Verwendung von Multi-Faktor-Authentifizierungsverfahren.
- Bei Einsatz von Passworten sind entsprechende Vorgaben zu erstellen und zu beachten.
- Mechanismen zur Detektion von Angriffen auf Passwort-basierte Authentisierungsverfahren sind zu verwenden.
- Erstellen einer Risikoanalyse.
- Beachten des Minimalitätsprinzips (So wenige Verbindungen, wie möglich).
- Etablierung von Prozessen zur Freigabe und Sperrung von Zugängen.
- Vorgaben für das Personal, welches die Fernwartung durchführt. Z. B. Verbot die Fernwartung über Mobiltelefone durchzuführen.
- Begrenzung des Zugangs auf ein definiertes Zeitfenster. Automatische Trennung der Verbindung nach Ablauf einer bestimmten Zeitspanne.
- Einschalten und Auswerten von Protokollfunktionen.

Das referenzierte Dokument enthält noch weitere Informationen. In diesem Dokument werden lediglich die wesentlichen Punkte wiedergegeben.

Die Firma Claroty hat in einer Studie untersucht, wie viele verschiedene Remote-Access-Lösungen parallel in Produktionsanlagen betrieben werden. [CLA2024b].

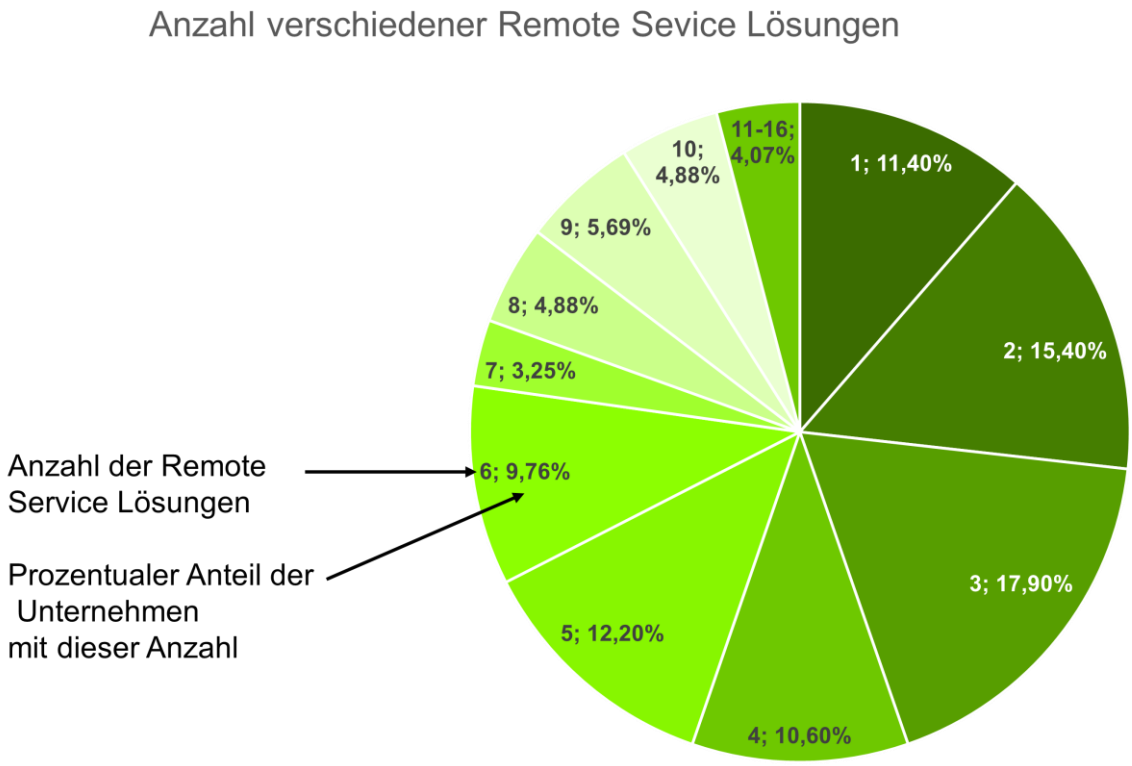

Abbildung 20: Anzahl unterschiedlicher Fernwartungslösungen in einem Unternehmen (Abgeleitet aus [CLA2024b])

Abbildung 20 zeigt die Anzahl unterschiedlicher Fernwartungslösungen der befragten Unternehmen. Die Autoren der Studie sagen dazu:

> *„Fast 22 % haben acht oder mehr, einige verwalten sogar 15 oder 16 Fernzugriffstools.“*

Hieraus kann man schließen, dass eine rechtzeitige Standardisierung auf eines oder wenige Fernzugriffstools den Wartungsaufwand und das Risiko deutlich verringern.

Weitere Informationen zur Fernwartung finden sich z. B. in der NAMUR-Empfehlung „Fernzugriff (Remote Access) - Anforderungen an die IT-Sicherheit von Fernzugriffen“ [NE_135]. Eine Zusammenfassung viele Richtlinien zur Fernwartung und ein Überblick über die verschiedenen technischen Ansätze findet sich in [LAN2022].

5.8. Datensicherung

In [ZET2016] und [SAN2016] wird der Angriff auf das ukrainische Energieversorgungsnetz im Jahr 2015 beschrieben. Unter anderem wurden bei diesem Angriff die Festplatten von Steuersystemen mit Hilfe der Software „KillDisk“ unbrauchbar gemacht. Das Auslösen eines totalen Datenverlustes ist eine bekannte Angriffsmethode. Auch sind Ransomware-Angriffe auf Produktionsanlagen bekannt. So wurde im Jahr 2020 eine Pipeline an der Ostküste der U.S.A durch eine Ransomware inoperabel [CYB2020]. Ziel eines Ransomware-Angriffs ist die Verschlüsselung von Daten und das Einfordern eines Lösegeldes zur Wiederherstellung der Daten. Aus diesem Grund kommt der Datensicherung im Produktionsbereich eine besondere Bedeutung bei.

Es ist daher ein Konzept für die Beherrschung eines katastrophalen Datenverlustes (Löschung aller Datenbestände einschließlich Betriebssystem) für den OT-Bereich zu entwickeln. Bestandteil eines Datensicherungskonzeptes ist die regelmäßige und vollständige Sicherung aller Datenbestände des Automatisierungssystems. Die Wiederherstellungsroutinen sind zu dokumentieren und zu testen.

In Anbetracht der sich weiter ausbreitenden Verschlüsselungstrojaner /Ransomware sollten die Backupsysteme und das Backupkonzept dieser Bedrohung Rechnung tragen. Das BSI formuliert in seinem Maßnahmenkatalog Ransomware [BSI2022d] folgende allgemeine Anforderungen, die auch auf den OT-Bereich übertragbar sind:

- „Ein Backup ist die wichtigste Schutzmaßnahme, mit der im Falle eines Ransomware-Vorfalls die Verfügbarkeit der Daten gewährleistet ist. Jede Institution sollte über ein Datensicherungskonzept (IT-Grundschutz: B 1.4 Datensicherungskonzept) verfügen und dieses auch umsetzen.
- Daher sollte zumindest je eine Kopie offline gesichert werden. Diese Kopien werden nach dem Backup von den anderen Systemen der Einrichtung getrennt und sind daher vor Remote-Angriffen geschützt.
- Offline-Backups können etwa mit getrennten Tapes, in einem getrennten Archiv mit nötigem physischem Zugriff oder auch in einem komplett vom eigenen Netz getrennten Cloud-Speicher erfolgen.
- Zu einem Backup gehört auch immer die Planung und Vorbereitung des Wiederanlaufs und der Rücksicherung der Daten.“

Das Mittelstand Digitalzentrum Hannover hat einen Best Practice Leitfaden zu Verschlüsselungstrojaner-resilienten Datensicherungen im OT-Bereich erarbeitet [PUL2024a]. Personen, die für das Backup im OT-Bereich verantwortlich sind, können sich an folgenden Leitfragen orientieren:

- Ist das Backupkonzept dokumentiert und den Mitarbeitenden bekannt?
- Gibt es einen Backup-Plan (3-2-1-Strategie)?
    - Sind **3** Kopien vorhanden (eine davon ist das Original+2 Backups).
    - **2** unterschiedliche Medien (interne Festplatte /externe Festplatte).
    - **1** Auslagerungsort.
- Wird das Einhalten des Backup-Plans überwacht und/oder das Durchführen der Backups dokumentiert?

- Ist das Backup physisch gesichert (Feuer / Wasser / Diebstahl)?
- Ist das Backup ein Offline-Backup oder anderweitig gegen Trojaner gesichert?
- Wurde das Rückspielen von Backups getestet?
- Kann das Backup bei Ausfall der Hardware auf eine Ersatzhardware aufgespielt werden?
- Gibt es einen Notfallplan für die Wiederherstellung von Systemen aus dem Backup.

Weitere Vorgaben zum Thema Backup finden sich auch in [DIN_EN_ISO_IEC_27002] unter dem Stichwort „Datensicherungen“.

5.9. Behandlung von Störungen und Ausfällen

Eine schnelle und effiziente Behandlung von Störungen und Ausfällen ist erforderlich, um nach einem solchen Vorfall den Betrieb schnell wieder aufnehmen zu können. Hierfür ist es maßgebend, dass der Begriff eindeutig definiert ist. Die Meldeart und die Meldewege sind festzulegen und zu dokumentieren. Es ist festzulegen, welche Art von Vorfällen in diese Kategorie fällt. Weiterhin ist ein Plan für eine Kommunikation nach außen zu erstellen. Die Reaktionen auf Störungen und Ausfälle sind zu definieren und Vorgehensmodelle (Wiederanlaufpläne) zur Beherrschung derartiger Störfälle sind erforderlich.

Bei Auftreten hat zunächst die Wiederherstellung des ordnungsgemäßen Betriebs die höchste Priorität. Danach erfolgen eine Ursachenuntersuchung, eine Dokumentation des Schadens sowie die Nachbereitung zur Abwendung künftiger Vorfälle.

Der BSI-Standard 100-4 Notfallmanagement [BSI100-4] liefert eine gute Basis für die Erstellung eines Notfallplans. Der „BSI Leitfaden Reaktion auf Sicherheitsvorfälle“ [BSI2022c] fasst die erforderlichen Schritte im Falle eines Notfalls wie folgt zusammen:

- Meldepflichten.
- Digitale Rettungskette.
- Einbindung von Fachpersonal.
- Standardvorgehen.
- Angriffsszenarien und Gegenmaßnahmen.
- Forensisches Vorgehen.
- Datensammlung.
- Datenanalyse.
- Remote Unterstützung.
- Notbetrieb.
- Nachbereitung.

5.10. OT-Security-Vorfälle erkennen

Die in Kapitel 5.9 beschriebenen Störungen können zunächst allgemeiner Art sein. Die IT-Sicherheitsvorfälle bilden eine Unterkategorie dieser Vorfälle, die einer besonderen Behandlung bedürfen. Grundsätzlich gilt für IT-Sicherheitsvorfälle zunächst das in Kapitel 5.9 beschriebene Vorgehen. Zusätzlich sind zum Erkennen und Abwenden von IT-Sicherheitsvorfällen präventive Maßnahmen sinnvoll. Eine Befragung des SANS-Institute [SAN2015] ergab, dass 15% der befragten Unternehmen angaben, mehr als einen Monat für das Erkennen eines Befalls benötigt zu haben. Das Ponemon Insitute [PON2017] nennt eine Dauer von 170 Tagen zwischen Befall und Entdeckung eines Security-Vorfalls

Aus diesem Grund ist die Erfassung, Speicherung und Auswertung Security-relevanter Ereignisse (engl. Security-Logging) ein wesentlicher Erfolgsfaktur zur frühzeitigen Erkennung von Cyber-Vorfällen. In der Regel werden die Ereignisse aus dem OT-Bereich an ein übergeordnetes Security-Information-and-Event-Management-System (SIEM) weitergeleitet. Ein SIEM dient der zentralen Erfassung, Analyse und Korrelation sicherheitsrelevanter Daten innerhalb einer IT- und OT-Infrastruktur. Es sammelt kontinuierlich Ereignisse aus verschiedenen Quellen wie Steuerungskomponenten, Firewalls, Servern, Endgeräten und Cloud-Diensten, und wertet sie in Echtzeit aus, um potenzielle Bedrohungen frühzeitig zu erkennen. Durch die intelligente Verknüpfung scheinbar isolierter Vorfälle kann ein SIEM-Muster identifizieren, die auf Angriffe oder Sicherheitsverletzungen hindeuten.

Das Thema Security-Logging kann anhand folgender Quellen weiter vertieft werden:

- Monitoring and Anomaly Detection in Production Networks [BSI2019]
- BSI Grundschutz: OPS.1.1.5: Protokollierung [BSI2021a]
- BSI Grundschutzkatalog - DER.1 Detektion von sicherheitsrelevanten Ereignissen [BSI2021b]
- Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen nach § 8 Abs. 1 Satz 1 BSIG [BSI2023a]
- Logging and log management – The authoritative guide to understanding the concepts surrounding logging and log management [CHU2013]

6. Ausblick

Der in Kapitel 5 vorgestellte 10-Punkte-Maßnahmenplan bietet einen ersten Ansatz zur Umsetzung der OT-Security im Produktionsbereich für KMU. Obwohl er geeignet ist einen ausreichenden Schutz für eine Produktionsanlage zu realisieren, bestehen dennoch einige Herausforderungen, welche künftig zu adressieren sind:

Die bisherigen Konzepte fokussieren stark auf die Abwehr von „Außen“. In [BER2023] wird dargestellt, dass vorsätzlich und unabsichtlich handelnde Beschäftigte einen signifikanten Anteil an Cyber-Angriffen verursachen. Siehe Abbildung 21. Daher reicht ein nach außen gerichteter Schutz nicht mehr aus.

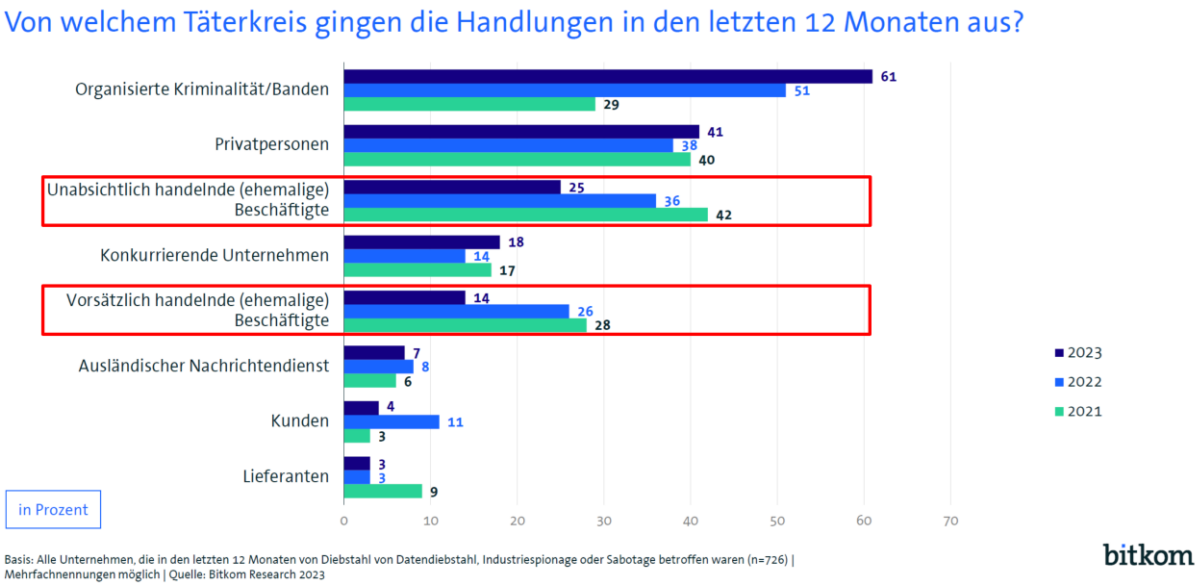

Abbildung 21: Anteil von Innentätern [BER2023]

Künftige Konzepte müssen sich also stärker als bisher auf einen Schutz gegen Innentäter konzentrieren. Hierzu gehört z. B. auch der Einbau von Automatisierungskomponenten in verschlossene Schaltschränke und eine Netzwerkszugangsüberwachung und das Einführen von Nutzeraccounts für Automatisierungssysteme.

Die zunehmende horizontale und vertikale Integration im Kontext von Industrie 4.0 wird dazu führen, dass die klassischen Schutzmechanismen nur noch eingeschränkt wirksam sein werden. Die Anzahl der Netzwerkknoten wird zunehmen, der Aufwand für die Sicherstellung der OT-Security wird steigen. In diesem Sinne ist bei der Security die IT-/OT-Konvergenz verstärkt zu betrachten. Die Konvergenz von IT und OT stellt Unternehmen vor die Herausforderung, zwei bislang nur lose gekoppelte Welten sicher miteinander zu verknüpfen. Bei der engeren Kopplung von IT und OT entstehen neue Angriffsflächen. OT-Komponenten, die früher isoliert betrieben wurden, werden durch die Vernetzung plötzlich leichter erreichbar. Zur weiteren Vertiefung hier eine Forschungsarbeit [AMI2024] und ein Erfahrungsbericht [GAN2023].

Die NAMUR hat bereits im Jahr 2015 in der [NE_153] Anforderungen an künftige Automatisierungssysteme beschrieben. Der wesentliche Grundgedanke ist der „Secure

by Design“ Ansatz. Statt einer Abschottung der Geräte werden künftig Sicherheitsfunktionen in die Geräte integriert, welche eine sichere Kommunikation auch unter Echtzeitbedingungen erlauben werden. Das Vorgehen für die Entwicklung von Automatisierungskomponenten nach diesem Ansatz ist am Beispiel eines Ethernet-APL-Messumformers in [NIE2023a] beschrieben. Weitere Überlegungen zum Thema „Secure by Design“ finden sich in [FLU2022].

Eine weitere große Herausforderung liegt sicher in der zeitgerechten Erfüllung der Anforderungen aus der Gesetzgebung. NIS2-Richtlinie und Cyber-Resilience-Act (CRA) werden Betreiber, Planer und Hersteller in der nächsten Zeit stark beschäftigen.

Für die Umsetzung der OT-Security sollten jedoch die gängigen Maßnahmen realisiert werden und insbesondere die „low hanging fruits“, die mit beschränktem Aufwand erreichbaren Ziele, geerntet werden. Hier kann mit geringem Aufwand ein großer Gewinn an Sicherheit erzielt werden.

7. Abbildungsverzeichnis

Abbildung 1: Cyber-Vorfälle aus dem Bereich der Gebäudeautomation [LI2023] 9
Abbildung 2: Horizontale und vertikale Integration 10
Abbildung 3: ISO 27001/ ISO 27002 und IEC 62443 als Bestandteile einer Cybersecurity-Strategie (In Anlehnung an [NIE2024b]) 13
Abbildung 4: Übersicht über Normen und Standards zur OT-Security 14
Abbildung 5: Bestand an gültigen ISO-27001-Zertifikaten in Deutschland in den Jahren 2006 bis 2023 [STA2025a] 15
Abbildung 6: Priorisierung der Schutzziele für Bürobereich (IT) und Automatisierungstechnik (OT) 16
Abbildung 7: Teile der IEC 62443 17
Abbildung 8: Risikoanalyse gemäß der [DIN_EN_IEC_62443-3-2] 19
Abbildung 9: Verantwortlichkeiten und zugehörige Normteile im Security Prozess 21
Abbildung 10: Vorgehensmodell nach [VDI_2182_1] 22
Abbildung 11: NIS2-Sektoren 30
Abbildung 12: Zeitschiene des CRA 31
Abbildung 13: Pflichten der Hersteller gemäß CRA 32
Abbildung 14: Beispielanlage mit Office und Produktionsbereich 40
Abbildung 15: Perimeterschutz 40
Abbildung 16: Modifizierte Firewall, DMZ und Zugangsüberwachung Gebäude 41
Abbildung 17: Einteilung des Produktionsbereichs in Zonen 42
Abbildung 18: Kryptographischer Schutz der Kommunikation 42
Abbildung 19: Netzwerküberwachung 43
Abbildung 20: Anzahl unterschiedlicher Fernwartungslösungen in einem Unternehmen (Abgeleitet aus [CLA2024b]) 45
Abbildung 21: Anteil von Innentätern [BER2023] 49

8. Tabellenverzeichnis

Tabelle 1: Top-10-Bedrohungen [BSI2022b] erweitert um Handlungsfelder 11
Tabelle 2 : Bedeutung der Abkürzung STRIDE 23

9. Index

Anforderungen 20
Angriffserkennung 33
Anomaly Detection 48
Anti-Malware 43
Asset 21
Asset Management 30
Asset Owner 20
Ausfälle 47
Authentication 31
Authentifizierung 19, 43
Backup 46
Bedrohung 21
Benutzer 21
Benutzerverwaltung 19
Betreiber 17, 20, 24
BSI 14, 24
BSI-Grundschutz 25
BSI-Grundschutzkatalog 14
Bundesamt für Sicherheit in der Informationstechnik 24
Business Continuity 30
CER-Richtlinie 28
CERT@VDE 38
CIP-Security 25
Cloud 40
CMMS 10
Conduits 18
CRA 31
CSAF 39
CSET 23
CVE 38
Cyber-Angriff 7
Cyber-Resilience-Act 31
Cyber-Resilience-Act (CRA) 28
Datenfluss 19
Datenhoheit 10
Datensicherung 46
demilitarisierte Zone 41
Denial of Service 12
Dienstleister 17
DMZ 41
EtherNet/IP 14, 25
EU-Maschinenverordnung 32
Evaluationsmethodik 20
Event-Logging 25
Fernwartung 8, 26, 44, 45
Firewall 40
Foundational Requirements 19
Gebäudeautomation 8, 9
Gebäudeautomatisierung 9
Grundlegenden Anforderungen 19
Grundschutz 38
Härtung 43
Hersteller 23
horizontale Integration 10
IACS 26
ICS 24
ICS-CERT 14
ICS-Security 6, 24
ICS-Security-Kompendium 24
IEC 60870-5-101 7
IEC 60870-5-104 7
IEC 61850 7
IEC 62351 14
IEC 62443 17
Incident Management 30
Industroyer 7
Informationssicherheitsmanagementsystem 12
Innentäter 27
Integrator 24
International Maritime Organization IMO 25
Internet 40
Intrusion Detection System-IDS 43
ISMS 12, 14, 15, 36
ISO 27000 15
ISO 27001 13
IT-Grundschutz-Kompendium 15
IT-Sicherheit 6
IT-Sicherheitsgesetz 33
IT-Sicherheitsgesetz 2.0 33
IT-Sicherheitsvorfälle 7
KMU 3, 6, 12, 16, 24, 35, 49, 64, 66
Kontaktstelle 33
KRITIS 33
KRITIS-Dachgesetz 34
Kryptographie 30
Lieferkette 8
Lieferketten 10, 30
Logging 18, 19, 20, 26, 48, 58, 63
Management Commitment 35
Manufacturer 20
maritimer Sektor 9

Maritimer Sektor 25
Maschinenverordnung 32
Microsoft Threat Modelling Tool 23
Minimalitätsprinzip 44
MQTT 10
NAMUR 14, 26
Network Intrusion Detection System-NIDS 43
NIS2-Richtlinie 28, 29
NIS2-Umsetzungsgesetz 34
NIS-Richtlinie 29
NIST SP 800-82 14
Normen 14
Notfall-Kommunikation 31
Notfallmanagement 47
ODVA 14, 25
Office-Bereich 42
OPC 7
OPC-UA 10
Operational Technology 6
OT 6
OT-Security 1, 3, 6, 7, 9, 10, 11, 12, 14, 16, 17, 18, 20, 21, 23, 24, 25, 26, 27, 28, 32, 35, 36, 37, 38, 44, 48, 49, 50
Passworte 43
PDCA 22, 26
Personal 30, 37
Petya/NotPetya 8
Phishing 11
Plan-Do-Check-Act 22
Planer 20
PROFINET 14, 16, 20, 25, 43
Protokollierung 48
Quick-Check 35
Ransomware 8
Reaktion 20
Remote Service 25
Remote-Diagnose 44
Remote-Zugänge 41
Richtlinien 14, 37
Risiko 21
Risikoanalyse 18
Risikoreduzierung 21
Sanktionen 31
Schutz der Zonengrenze 41
Schwachstelle 21
Security in der Lieferkette 8
Security-Level 18
Sektoren 29
Sicherheitslebenszyklus 17
SiToM 35
Social Engineering 11
SolarWinds 8
Standards 14
Störungen 47
STRIDE 23
Sunburst 8
Supply Chain 30
Supply-Chain-Security 8
System Integrator 20
Systemintegrität 19
Top-10-Bedrohungen 11, 24
Training 30
Update-Server 41
VDI/VDE 2182 ..... 14, 21
VdS 16
VdS 10000 14
VdS 10020 ..... 14, 24
Verfügbarkeit 20
vertikale Integration 10
Vertraulichkeit 19
Verursacher 22
Virenschutz 43
Vorfälle 48
WannaCry 8
Whitelisting 43
Wiederanlaufpläne 47
Wissen 38
Zonen 18
Zugangsbeschränkung 43
Zugangskontrolle 27, 30
Zugangsüberwachung 42
Zuständigkeiten 36

10. Literaturverzeichnis

[ABB2025] ABB Asea Brown Boveri Ltd: Cyber security alerts and notifications. URL: http://new.abb.com/about/technology/cyber-security/alerts-and-notifications, 29.11.2016.

[ABS2025] American Bureau of Shipping: ABS CyberSafety Program. URL: https://ww2.eagle.org/en/Products-and-Services/cyber/abs-cybersafety.html.

[ALK2021] Alkhadra, Rahaf; Abuzaid, Joud; AlShammari, Mariam; Mohammad, Nazeeruddin: Solar Winds Hack: In-Depth Analysis and Countermeasures: 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT). IEEE, Piscataway, NJ, 2021; S. 1–7.

[AMI2024] Amiri, Amirali; Steindl, Gernot; Gorton, Ian; Hollerer, Siegfried; Kastner, Wolfgang; Sauter, Thilo: Integrated Safety and Security by Design in the IT/OT Convergence of Industrial Systems: A Graph-Based Approach. In (Chang, R. N. Hrsg.): 2024 IEEE International Conference on Software Services Engineering. IEEE SSE 2024 Shenzhen, China, 7-13 July 2024 proceedings. IEEE, Piscataway, NJ, 2024; S. 123–129.

[ATU2025] Atug, Manuel: NIS2: Schulungspflicht für Geschäftsleitungen. In ix - Magazin für professionelle Informationstechnik, 4, 2025; S. 92–95. URL: https://www.wiso-net.de/browse/Alle%20Quellen/Fachzeitschriften/Elektroindustrie/iX%20-%20Magazin%20f%C3%BCr%20professionelle%20Informationstechnik?preview=IX__2025-4.

[BER2023] Berg, Achim: Wirtschaftsschutz 2023. URL: https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf.

[BMI2024] Bundesministerium des Innern: Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen. URL: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/KM4/regentwurf-kritisDachG.pdf?__blob=publicationFile&v=3.

[BMI2025] Bundesministerium des Innern: Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen. Referentenentwurf, Bearbeitungsstand: 27.08.2025 16:26. URL: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/KM4/Kritis-Dachgesetz.pdf?__blob=publicationFile&v=1.

[BRE2024] Brenner, Michael; gentschen Felde, Nils; Hommel, Wolfgang; Metzger, Stefan; Reiser, Helmut; Schaaf, Thomas: Praxisbuch ISO/IEC 27001. Management der Informationssicherheit und Vorbereitung auf die Zertifizierung. 5. Auflage. Hanser, München, 2024.

[BRO2011] Broad, William J.; Markoff, John, Sander, David E.: Israeli Test on Worm Called Crucial in Iran Nuclear Delay. URL: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=3&sq=stux.

[BSI_INF.13] Bundesamt für Sicherheit in der Informationstechnik (BSI): INF.13 Technisches Gebäudemanagement. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/10_INF_Infrastruktur/INF_13_Technisches_Gebaeudemanagement_Edition_2023.pdf?__blob=publicationFile&v=3.

[BSI_INF.13U] Bundesamt für Sicherheit in der Informationstechnik (BSI): Umsetzungshinweise zum Baustein INF.13 Technisches Gebäudemanagement. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise_2021/Umsetzungshinweis_zum_Baustein_INF_13_Technisches_Gebaeudemanagement.pdf?__blob=publicationFile&v=2.

[BSI_INF.14] Bundesamt für Sicherheit in der Informationstechnik (BSI): INF.14 Gebäudeautomation. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-

GS-Kompendium_Einzel_PDFs_2023/10_INF_Infrastruktur/INF_14_Gebaeudeautomation_Edition_2023.pdf?__blob=publicationFile&v=3.

[BSI_INF.14U] Bundesamt für Sicherheit in der Informationstechnik (BSI): Umsetzungshinweise zum Baustein INF.14 Gebäudeautomation. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise_2021/Umsetzungshinweis_zum_Baustein_INF_14_Gebaeudeautomation.pdf?__blob=publicationFile&v=2.

[BSI100-4] Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI Standard 100-4 Notfallmanagement, 2008. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf?__blob=publicationFile&v=2.

[BSI2014] Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2014. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile, 12.01.2015.

[BSI2018a] Bundesamt für Sicherheit in der Informationstechnik: Empfehlung IT in der Produktion. Fallbeispiel Schwimmbad. URL: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_095a.pdf?__blob=publicationFile&v=1, 23.07.2025.

[BSI2018b] Bundesamt für Sicherheit in der Informationstechnik: Fallbeispiel Servicetechniker. URL: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_095c.pdf?__blob=publicationFile&v=1, 25.07.2025.

[BSI2018c] Bundesamt für Sicherheit in der Informationstechnik: Anforderungen an netzwerkfähige Industriekomponenten. BSI-CS 067. URL: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_067.pdf?__blob=publicationFile&v=1, 26.04.2025.

[BSI2019] Bundesamt für Sicherheit in der Informationstechnik (BSI): Monitoring and Anomaly Detection in Production Networks. URL: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_134E.pdf?__blob=publicationFile&v=1.

[BSI2021a] Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI Grundschutz: OPS.1.1.5: Protokollierung. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_1_1_5_Protokollierung_Edition_2021.pdf?__blob=publicationFile&v=2.

[BSI2021b] Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI Grundschutzkatalog - DER.1 Detektion von sicherheitsrelevanten Ereignissen. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/05_DER_Detektion_und_Reaktion/DER_1_Detektion_von_sicherheitsrelevanten_Ereignissen_Edition_2022.pdf?__blob=publicationFile&v=3#download=1.

[BSI2021c] Bundesamt für Sicherheit in der Informationstechnik (BSI): IND.1: Prozessleit- und Automatisierungstechnik. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/08_IND_Industrielle_IT/IND_1_Prozessleit_und_Automatisierungstechnik_Edition_2021.pdf?__blob=publicationFile&v=2.

[BSI2022a] Bundesamt für Sicherheit in der Informationstechnik (BSI): IND.3.2 Fernwartung im industriellen Umfeld. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/08_IND_Industrielle_IT/IND_3_2_Fernwartung_im_industriellen_Umfeld_Edition_2022.pdf?__blob=publicationFile&v=3.

[BSI2022b] Bundesamt für Sicherheit in der Informationstechnik (BSI): Industrial Control System Security - Top 10 Bedrohungen und Gegenmaßnahmen 2022. BSI-CS 005. URL:

https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005.html;jsessionid=EEC337374A53B4720636D8C64B94EF99.internet081.

[BSI2022c] Bundesamt für Sicherheit in der Informationstechnik (BSI): Leitfaden zur Reaktion auf IT- Sicherheitsvorfälle für Vorfall-Praktiker und Vorfall-Experten. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CSN/Leitfaden_VP_VE.pdf?__blob=publicationFile&v=21.

[BSI2022d] Bundesamt für Sicherheit in der Informationstechnik (BSI): Maßnahmenkatalog Ransomware. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Massnahmenkatalog.pdf?__blob=publicationFile&v=2.

[BSI2022e] Bundesamt für Sicherheit in der Informationstechnik (BSI): Sicherheitsanalyse OPC UA. URL: https://cdn.weka-fachmedien.de/media_uploads/documents/1648647762-236-opcua-2022.pdf.

[BSI2023a] Bundesamt für Sicherheit in der Informationstechnik (BSI): Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen nach § 8 Abs. 1 Satz 1 BSIG. Version 2.0 vom 29.06.2023. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_Protokollierung_und_Detektion_Version_2_0.pdf?__blob=publicationFile&v=3.

[BSI2023b] Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kompendium. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1.

[BSI2024] Bundesamt für Sicherheit in der Informationstechnik: ICS-Security-Kompendium. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile&v=6, 05.06.2014.

[BSI2025a] Bundesamt für Sicherheit in der Informationstechnik (BSI): Common Security Advisory Framework CSAF. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/CSAF/CSAF_node.html.

[BSI2025] Allianz für Cyber-Sicherheit: LARS ICS. Ein Werkzeug für den leichtgewichtigen Einstieg in industrielle Cyber-Security. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/Tools/LarsICS/LarsICS_node.html, 23.07.2025.

[BSI-KritisV_2016]: Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung). BSI-KritisV, 2016.

[BUN2017]: Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union. NIS-UG: Bundesgesetzblatt, 2017.

[BUN2023]: Dritte Verordnung zur Änderung der BSI-Kritisverordnung. KritisV 2.0, 2023.

[BUN2025]: Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung. Gesetzentwurf der Bundesregierung. Stand 25.07.2025. NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, 2025.

[CER2022]: Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates. CER Richtlinie, 2022.

[CERT2016] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT): Cyber-Attack Against Ukrainian Critical Infrastructure. URL: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[CERT2018] The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT): Alert (ICS-ALERT-14-176-02A). ICS Focused Malware (Update A). URL: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A, 20.07.2025.

[CHE2017] Cherepanow, Anton: Win32/Industroyer. A new threat for industrial control systems. URL: https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.

[CHU2013] Chuvakin, A. Hrsg.: Logging and log management. The authoritative guide to understanding the concepts surrounding logging and log management. Syngress, Waltham, MA, 2013.

[CLA2024a] Claroty Ltd.: An Open Door. URL: https://web-assets.claroty.com/team82-secure-access-report.pdf.

[CLA2024b] Claroty Ltd.: Remote Access Tool Sprawl. URL: https://web-assets.claroty.com/resource-downloads/claroty-team82-report_secure-access-tool-sprawl.pdf.

[CRA2024]: Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung) (Text von Bedeutung für den EWR). CRA: Amtsblatt der Europäischen Union, 2024; S. 1–81.

[CYB2020] Cybersecurity & Infrastructure Security Agency: Ransomware Impacting Pipeline Operations Alert (AA20-049A). URL: https://www.us-cert.gov/ncas/alerts/aa20-049a.

[DHS2016] Department of Homeland Security: Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. URL: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

[DHS2025] Department of Homeland Security: Cybersecurity Alerts & Advisories. URL: https://www.cisa.gov/news-events/cybersecurity-advisories, 25.07.2025.

[DIN_EN_IEC_62443-2-1] DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, DIN EN IEC 62443-2-1:2020-10 - Entwurf VDE 0802-2-1:2020-10: IT-Sicherheit für industrielle Automatisierungssysteme - Teil 2-1: Anforderungen an ein IT-Sicherheitsprogramm für IACS-Betreiber (IEC 65/756/CDV:2019); Deutsche und Englische Fassung prEN IEC 62443-2-1:2019, 2020. URL: https://www.dinmedia.de/de/norm-entwurf/din-en-iec-62443-2-1/327919389.

[DIN_EN_IEC_62443-2-2] DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, DIN EN IEC 62443-2-2 (VDE 0802-2-2): 2021-05: IT-Sicherheit für industrielle Automatisierungssysteme Teil 2-2 IACS-Sicherheitsprogramm-Einstufungen (IEC 65/797/CD:2020); Text Deutsch und Englisch Ausgabedatum: 2021-05, 2021.

[DIN_EN_IEC_62443-2-4] DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, DIN EN IEC 62443-2-4:2024-11 VDE 0802-2-4:2024-11: IT-Sicherheit für industrielle Automatisierungssysteme - Teil 2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme (IEC 62443-2-4:2023); Deutsche Fassung EN IEC 62443-2-4:2024, 2024. URL: https://www.dinmedia.de/de/norm/din-en-iec-62443-2-4/380674327.

[DIN_EN_IEC_62443-3-2] DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, DIN EN IEC 62443-3-2:2021-12 VDE 0802-3-2:2021-12: IT-Sicherheit für industrielle Automatisierungssysteme - Teil 3-2: Sicherheitsrisikobeurteilung und Systemgestaltung (IEC 62443-3-2:2020); Deutsche Fassung EN IEC 62443-3-2:2020, 2021. URL: https://www.dinmedia.de/de/norm/din-en-iec-62443-3-2/344299957.

[DIN_EN_IEC_62443-3-3] DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, DIN EN IEC 62443-3-3:2020-01 VDE 0802-3-3:2020-01: Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme - Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level (IEC 62443-3-3:2013 +

COR1:2014); Deutsche Fassung EN IEC 62443-3-3:2019 + AC:2019, 2020. URL: https://www.dinmedia.de/de/norm/din-en-iec-62443-3-3/311519620.

[DIN_EN_IEC_62443-4-1] DKE-Deutsche Kommission Elektrotechnik, Elektronik Informationstechnik DIN und VDE, DIN Deutsches Institut für Normung e. V, DIN EN IEC 62443-4-1 (VDE 0802-4-1): IT -Sicherheit für industrielle Automatisierungssysteme - Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung (IEC 62443-4-1 2018); Deutsche Fassung EN IEC 62443-4-1 2018. Beuth Verlag, Berlin, 2018. URL: https://www.dinmedia.de/de/norm/din-en-iec-62443-4-1/292194568.

[DIN_EN_IEC_62443-4-2] DKE-Deutsche Kommission Elektrotechnik, Elektronik Informationstechnik DIN und VDE, DIN EN IEC 62443-4-2 (VDE 0802-4-2): IT-Sicherheit für industrielle Automatisierungssysteme - Teil 4-2: Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme (IACS) (IEC 62443-4-2:2019); Deutsche Fassung EN IEC 62443-4-2:2019, 2019. URL: https://www.dinmedia.de/de/norm/din-en-iec-62443-4-2/312858287.

[DIN_EN_ISO/IEC_27001] DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), DIN EN ISO/IEC 27001:2024: Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagementsysteme – Anforderungen (ISO/IEC 27001:2022); Deutsche Fassung EN ISO/IEC 27001:2023, 2024. URL: https://www.dinmedia.de/de/norm/din-en-iso-iec-27001/370680635.

[DIN_EN_ISO_27000] DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), DIN EN ISO/IEC 27000:2020: Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Überblick und Terminologie (ISO/IEC 27000:2018); Deutsche Fassung EN ISO/IEC 27000:2020, 2020. URL: https://www.iso27001security.com/html/27000.html.

[DIN_EN_ISO_IEC_27002] DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), DIN ISO/IEC 27002:2024: Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022); Deutsche und Englische Fassung prEN ISO/IEC 27002:2022 - Entwurf, 2024.

[DIN_ISO_27006-1] DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), DIN EN ISO/IEC 27006-1: Informationssicherheit, Cybersicherheit und Datenschutz – Anforderungen an Stellen, die Informationssicherheitsmanagementsysteme auditieren und zertifizieren – Teil 1: Allgemeines (ISO/IEC 27006-1:2024); Deutsche Fassung EN ISO/IEC 27006-1:2024.

[DIR2015] DiRenzo, Joseph; Goward, Dana A.; Fred S. Roberts: The Little-known Challenge of Maritime Cyber Security: 6th International Conference on Information, Intelligence, Systems and Applications (IISA), 2015.

[DNV2025] DNV AS: Cyber Secure class notation. URL: https://www.dnv.com/services/cyber-secure-class-notation-124600/.

[EIK2013] Eikenberg, Ronald: Vaillant-Heizungen mit Sicherheits-Leck. URL: http://www.heise.de/security/meldung/Vaillant-Heizungen-mit-Sicherheits-Leck-1840919.html, 12.02.2016.

[ENI2025] ENISA European Union Agency for Network and Information Security: EU Vulnerability Database. URL: https://euvd.enisa.europa.eu/search.

[ENN2021] Ennenbach, Martin et al.: Leitfaden Cyber-Sicherheits-Check OT. Ein Leitfaden zur Durchführung von Cyber-Sicherheits-Checks der operativen Technologie (CSC-OT) in der Industrie und Automatisierungstechnik. URL: https://www.isaca.de/sites/default/files/isaca_leitfaden_cyber-sicherheits-check_ot.pdf.

[EUR2006]: Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (Neufassung). Maschinenrichtlinie, 2006.

[EUR2016]: Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, 2016.

[EUR2023]: Verordnung (EU) 2023/1230 des Europäischen Parlaments und Rates vom 14. Juni 2023 über Maschinen und zur Aufhebung der Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates und der Richtlinie 73/361/EWG des Rates. Maschinenverordnung, 2023.

[FAL2011] Falliere, Nicolas; Murchu, Liam O.; Chien, Eric: W32.Stuxnet Dossier. URL: https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en, 21.08.2014.

[FLU2022] Fluchs, Sarah; Tasten, Emre; Mertens, Martin; Horch, Alexander; Drath, Rainer; Fay, Alexander: Security by Design Integration Mechanisms for Industrial Control Systems: IECON 2022 – 48th Annual Conference of the IEEE Industrial Electronics Society. IEEE, 2022; S. 1–6.

[FOR2025] Fortinet Inc.: Solar-Winds Cyber Angriff. URL: https://www.fortinet.com/de/resources/cyberglossary/solarwinds-cyber-attack.

[GAN2023] Ganschowr, Sebastian: Stolperfallen vermeiden, Sicherheit erhöhen. IT- und OT-Integration. In Industrie 4.0 Magazin, 7, 2023; S. 11–12.

[GRA2024] Graham, Mark; Ahlers; Carolyn; o‘ Meara, Kyle: Impact of FrostyGoop ICS Malware on Connected OT Systems. URL: https://hub.dragos.com/hubfs/Reports/Dragos-FrostyGoop-ICS-Malware-Intel-Brief-0724_.pdf.

[HÄU2023] Häußler, Alexander: ISO/IEC 27001 Information security management system and the road to certification. URL: https://www.tuvsud.com/en/resource-centre/white-papers/iso-iec-27001-information-security-management.

[HÜN2024] Hüning, Alois; Reusch, Philipp; Gast, Torsten: Die neue EU-Maschinenverordnung. Übersicht über die Änderungen, Lösungen und Antworten für die Praxis. Vogel Communications Group, Würzburg, 2024.

[ICS2025] ICS-CERT: Downloading and Installing CSET. URL: https://www.cisa.gov/downloading-and-installing-cset, 23.07.2025.

[IEC_62443_3_1] IEC- International Electrotechnical Commission, ISA 62443-3-1: Technical Report Security Technologies for Industrial Automation and Control Systems, Rev. 2, 2007. URL: http://isa99.isa.org/Public/Documents/ISA-62443-3-1-EX.pdf.

[IEC_62443-1-1] IEC- International Electrotechnical Commission, IEC/TS 62443-1-1-alt: Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models- alt, 2009.

[IEC_62443-1-2] IEC- International Electrotechnical Commission, ISA-TR62443-1-2: Security for industrial automation and control systems - Master Glossary. URL: http://isa99.isa.org/Public/Documents/ISA-62443-1-2-WD.pdf.

[IEC_62443-1-3] IEC- International Electrotechnical Commission, IEC/TS 62443-1-3: Security for industrial process measurement and control – Network and system security – Part 1-3: System security compliance metrics, 2014. URL: http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx.

[IEC_62443-1-4] IEC- International Electrotechnical Commission, ISA-62443-1-4: Security for industrial automation and control systems Life Cycle and Use Cases, 2013. URL: http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx.

[IEC_62443-1-5] IEC- International Electrotechnical Commission, IEC TS 62443-1-5: Security for industrial automation and control systems - Part 1-5: Scheme for IEC 62443 security profiles, 2023. URL: https://webstore.iec.ch/publication/67461.

[IEC_62443-2-3] IEC- International Electrotechnical Commission, IEC TR 62443-2-3:2015: Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment, 2015. URL: https://webstore.iec.ch/preview/info_iec62443-2-3%7Bed1.0%7Den.pdf.

[IEC_62443-2-4] IEC- International Electrotechnical Commission, IEC 62443-2-4:2015+AMD1:2017 CSV consolidated version: Security for industrial automation and

control systems - Part 2-4: Security program requirements for IACS service providers, 2017.

[IEC_62443-6-1] IEC- International Electrotechnical Commission, IEC TS 62443-6-1:2024: Security for industrial automation and control systems - Part 6-1: Security evaluation methodology for IEC 62443-2-4, 2024. URL: https://www.vde-verlag.de/iec-normen/252700/iec-ts-62443-6-1-2024.html.

[IEC_62443-6-2] IEC- International Electrotechnical Commission, IEC TS 62443-6-2:2025: Security for industrial automation and control systems - Part 6-2: Security evaluation methodology for IEC 62443-4-2, 2025. URL: https://www.vde-verlag.de/iec-normen/254715/iec-ts-62443-6-2-2025.html.

[IEC_62451-2] IEC- International Electrotechnical Commission, IEC TR 62541-2:2020 RLV: OPC unified architecture - Part 2: Security Model, 2020. URL: https://webstore.iec.ch/publication/68036.

[IMO2017] International Maritime Organization (IMO): Resolution MSC.428(98) (adopted on 16 June 2017) Maritime Cyber Risk Management in Safety Management Systems. URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf.

[IMO2025] International Maritime Organization (IMO): Guidelines on Maritime Cyber Risk Management. MSC-FAL.1/Circ.3/Rev.3. URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.3.pdf.

[ISE2025] IsecT Ltd: Overwiew on ISO 27000 standard series. URL: https://www.iso27001security.com/html/iso27000.html.

[IT_SIG_2.0]: Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0). IT-SiG 2.0: Bundesgesetzblatt, 2021; S. 1122–1138.

[ITSichG2015]: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), 2015.

[JEN2015] Jensen, Lars: Challenges in Maritime Cyber-Resilience. In Technology Innovation Management Review, 04, 2015; S. 35–39. URL: http://timreview.ca/sites/default/files/article_PDF/Jensen_TIMReview_April2015.pdf.

[KAL2024] Kallisch, Jonas; Niemann, Karl-Heinz; Wunck, Christoph: Bridging the Data Borders – Connecting Supply-Chain Shop-Floors. In (Witte, P.; Niemann, Karl-Heinz Hrsg.): Sensorik und Automation: Schriften des Forschungsinstituts ISA 2024. HsH Applied Academics, 2024; S. 50–61. https://doi.org/10.25968/opus-3245.

[KAL2025] Kallisch, Jonas; Voss, Marvin; Runge, Maxim; Wunck, Christoph; Niemann, Karl-Heinz: Cyber-Sicherheit in vernetzten Lieferketten. 441 KB, 2025. URL: https://doi.org/10.25968/opus-3594.

[KIR2022] Kirketerp de Viron, Christiane; Stefanuc, Raluca; Boegel, Benjamin; Fohrenbach, Maika: Cyber Resilience Act: new EU cybersecurity rules ensure safer hardware and software, Connect University Online Session, 2022.

[KOB2021] Kobes, Pierre: Applying ISO/IEC 27001/2 and the ISA/IEC 62443 Series for Operational Technology Environments. URL: https://gca.isa.org/blog/white-paper-excerpt-applying-iso/iec-27001/2-and-the-isa/iec-62443-series-for-operational-technology-environments.

[KOB2024] Kobes, Pierre: Leitfaden Industrial Security. IEC 62443 einfach erklärt. VDE Verlag, Berlin, 2024.

[KUI2006] Kuipers, David; Fabro, Mark: Control Systems Cyber Security:Defense in Depth Strategies. URL: https://www.osti.gov/biblio/911553.

[LAN2013] Langner, Ralph: To kill a centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve. URL: http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf, 13.11.2014.

[LAN2022] Langreder, Philipp; Schmidt, Frank; Niemann, Karl-Heinz: Fernwartung und OT-Security. In atp magazin, 9, 2022; S. 64–73. URL: https://doi.org/10.25968/opus-2366.

[LEL2021] Lella, Ifigeneia; Theocharidou, Marianthi; Tsekmezoglou, Eleni; Malatras, Apostolos: ENISA Threat Landscape for Supply Chain Attacks. URL: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

[LI2023] Li, Guowen; Ren, Lingyu; Fu, Yangyang; Yang, Zhiyao; Adetola, Veronica; Wen, Jin; Zhu, Qi; Wu, Teresa; Candan, K.Selcuk; O'Neill, Zheng: A critical review of cyber-physical security for building automation systems. In Annual Reviews in Control, 2023, Jahrgang 55; S. 237–254.

[LLO2024] Lloyd's Register: Digital Ships Procedures. URL: https://www.lr.org/en/knowledge/lloyds-register-rules/shipright/digital-ships/.

[MIC2023] Microsoft: Microsoft Threat Modeling Tool. URL: https://learn.microsoft.com/de-de/azure/security/develop/threat-modeling-tool, 23.07.2025.

[MIT2025a] Mittelstand Digital: SiToM - Sicherheitstool Mittelstand. URL: https://www.sitom.de/home.

[MIT2025b] Mitre Corporation: Common Vulnerabilities and Exposures. URL: https://www.cve.org/, 25.07.2025.

[NA_115] NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V: NA115: IT-Sicherheit für Systeme der Automatisierungstechnik: Randbedingungen für Maßnahmen beim Einsatz in der Prozessindustrie, 17.11.2016.

[NA_163] NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V, NA 163: IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen, 2024.

[NA_169] NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V, NA 169: Automation Security Management in der Prozessindustrie, Leverkusen, 2019.

[NE_135] NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V, NE 135: Fernzugriff (Remote Access) - Anforderungen an die IT-Sicherheit von Fernzugriffen, Leverkusen, Version: 2023. URL: https://www.namur.net/de/empfehlungen-und-arbeitsblaetter/aktuelle-nena.html.

[NE_153] NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V, NE 153: Automation Security 2020 – Design, Implementierung und Betrieb industrieller Automatisierungssysteme, Leverkusen, 2015.

[NE_177] NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V, NE 177: NAMUR Open Architecture - NOA Security Zonen und NOA Security Gateway, 2021. URL: https://www.namur.net/de/empfehlungen-und-arbeitsblaetter/aktuelle-nena.html.

[NE_193] NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V, NE 193: Ein Informationsmodell für das Automation Security Engineering, 2024.

[NE_201] NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V, NE 201: Identity and Access Management on Automation Devices, 2025. URL: https://www.namur.net/de/empfehlungen-und-arbeitsblaetter/aktuelle-nena.html.

[NHL2025] NHL Stenden - University of Applied Sciences: MCAD Maritime Cyber Attack Database. URL: https://maritimecybersecurity.nl/.

[NIE2014] Niemann, Karl-Heinz: IT-Security-Konzepte für die Prozessindustrie. Anforderungen im Kontext von Industrie 4.0. In atp-edition, 7-8/2014, 2014, Jahrgang 56; S. 62–69. URL: http://media.di-verlag.de/atp/atp_07-08_2014_Niemann.pdf.

[NIE2014_1] Niemann, Karl Heinz: IT Security Konzepte. Anforderungen im Kontext von Industrie 4.0. In (VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik Hrsg.): Automation 2014. Smart X - Powered by Automation. VDI-Verlag GmbH, Düsseldorf, 2014; S. 489–506.

[NIE2017] Niemann, Karl-Heinz: IT-Sicherheit in Produktionsanlagen. Eine Einführung für kleine und mittlere Unternehmen. URL: https://doi.org/10.25968/opus-1135.

[NIE2021] Niemann, Karl-Heinz: Abgrenzung der IT-Sicherheitsnormenreihen ISO 27000 und IEC 62443 - Eine Sicht auf automatisierungstechnische Anlagen der Fertigungs- und Prozessindustrie. URL: https://doi.org/10.25968/opus-1973.

[NIE2023a] Niemann, Karl-Heinz; Walz, Andreas; Merklin, Simon; Ziegler, Andreas; Waldeck, Boris: Wie man ein sicheres PROFINET-Gerät entwickelt. Organisatorische und technische OT-Security-Maßnahmen bei der Entwicklung von PROFINET-Geräten. In atp Magazin, 2023; S. 62–70. URL: https://doi.org/10.25968/opus-2961.

[NIE2023b] Niemann, Karl-Heinz; Walz, Andreas; Sikora, Axel: Security Extensions for PROFINET. Concepts, Status, and Prospects. In (Sikora, A. Hrsg.): Embedded World Conference 2023 Proceedings. WEKA Fachmedien GmbH, 2023; S. 99–104.

[NIE2024a] Niemann, Karl-Heinz; Göppert, Julian; Walz, Andreas; Ziegler, Dominik: Security-Event-Logging am Beispiel von PROFINET. In (Technische Hochschule Ostwestfalen-Lippe; Jasperneite, Jürgen; Jumar, Ulrich Hrsg.): Kommunikation in der Automation Beiträge des Jahreskolloquiums KommA 2024. Institut für industrielle Informationstechnik - inIT der Technischen Hochschule Ostwestfalen-Lippe, 2024; S. 48–60. https://doi.org/10.25644/jnac-vp34.

[NIE2024b] Niemann, Karl-Heinz; Kobes, Pierre: ISO 27000 oder IEC 62443? Wie man beide Normreihen sinnvoll für die OT-Security kombiniert. In atp Magazin, 03, 2024; S. 60–67. URL: https://doi.org/10.25968/opus-3072.

[NIS-2_de]: Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie). NIS-2-Richtlinie: Amtsblatt der Europäischen Union, 2022.

[NIS2_DE_2025]: Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung. Drucksache 21/1501, 2025.

[NIS2UmsuCG]: Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz), 2024.

[ODV2023] ODVA Inc.: Overview of CIP Security. URL: https://www.odva.org/wp-content/uploads/2023/07/PUB00319R2_CIP-Security-At-a-Glance.pdf.

[OTO2022] OTORIO Ltd.: 2022 OT Cybersecurity Survey Report. URL: https://go.otorio.com/hubfs/Whitepapers%20and%20Reports/OTORIO_2022%20OT%20Cybersecurity%20Survey%20Report.pdf.

[PAK2005] Pakalski, Ingo: Computerwurm befällt CNN, DaimlerChrysler und Walt Disney. URL: http://www.golem.de/0508/39902.html.

[PAN2008] Pany, Thomas: Saboteur schaltet Turbine des britischen Kohlekraftwerks Kingsnorth aus. URL: https://www.heise.de/newsticker/meldung/Saboteur-schaltet-Turbine-des-britischen-Kohlekraftwerks-Kingsnorth-aus-188799.html?view=print.

[PIT2023] Pittler, Jens: Sabotageaufklärung in Logistikunternehmen. URL: https://rhebo.com/de/download/file/case-study-sabotageaufklaerung-im-logistikunternehmen/.

[PNO2013] PROFIBUS Nutzerorganisation e.V.: PROFINET Security Guideline. URL: https://www.profibus.com/index.php?eID=dumpFile&t=f&f=47893&token=f543743e30d8aa3b51b883d00cdc304926678fe8.

[PNO2019a] PROFIBUS Nutzerorganisation e.V.: Security Extensions for PROFINET. PI White Paper for PROFINET. URL: https://www.profibus.com/download/pi-white-paper-security-extensions-for-profinet/.

[PNO2019b] PROFIBUS Nutzerorganisation e.V.: Security Erweiterungen für PROFINET. PI White Paper für PROFINET. URL: https://www.profibus.com/download/pi-white-paper-security-extensions-for-profinet/, 07.09.2019.

[PNO2022] PROFIBUS Nutzerorganisation e.V.: OT-Security für Produktionsanlagen mit PROFINET. Eine Einordnung der IEC 62443 für Betreiber, Integratoren und Hersteller. URL: https://www.profibus.com/download/white-paper-ot-security-classification-of-iec62443.

[PNO2023] PROFIBUS Nutzerorganisation e.V.: Security Class 1 for PROFINET-Security Guideline for PROFINET. URL: https://www.profibus.com/download/profinet-security-guideline.

[PON2017] Ponemon Institute LLC: 2017 Cost of Data Breach Study. URL: https://www.ponemon.org/news-updates/blog/security/2017-cost-of-data-breach-study-united-states.html.

[PUL2024a] Puls, Jan-Niklas; Niemann, Karl-Heinz; Meyer, Sebastian: Best Practice zu Verschlüsselungstrojaner-resilienten Datensicherungen. URL: https://doi.org/10.25968/opus-3095.

[PUL2024b] Puls, Jan-Niklas; Niemann, Karl-Heinz: Einführen eines Informationssicherheitsmanagementsystems in einem KMU. In Zukunft.Digital, 02, 2024; S. 26–29. URL: https://digitalzentrum-hannover.de/wp-content/uploads/2024/12/MDZH_Magazin_24-02_web.pdf.

[SAN2015] SANS Institute: The State of Security in Control Systems Today. URL: http://www.sans.org/reading-room/whitepapers/analyst/state-security-control-systems-today-36042, 19.07.2016.

[SAN2016] SANS Institute: Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case. URL: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf.

[SCH2018] Schmidt, Jürgen: Erpressung macht sich breit. Ransomware mit neuen Tricks und Techniken. In c't Magazin für Computertechnik, 2, 2018; S. 22–23. URL: http://eaper.heise.de/download/archiv/b7e6194fa397/ct.18.02.022-023.pdf.

[SEC2024] Securiton Deutschland: Das KRITIS-Dachgesetz und seine Umsetzung. Höchste Sicherheit für kritische Infrastrukturen. URL: https://www.securiton.de/anwendungen/kritische-infrastrukturen-kritis/unser-whitepaper-fuer-sie.html.

[SIE2025] Siemens Aktiengesellschaft: ProductCERT Security Advisories. URL: http://www.siemens.com/cert/de/cert-security-advisories.htm, 29.11.2016.

[STA2013] Stahl, Louis-F.; Eikenberg, Ronald: Fünf nach zwölf. Die „Gefahr im Kraftwerk" ist noch nicht gebannt. In c't Magazin für Computertechnik, 15, 2013; S. 16–17.

[STA2015] Stahl, Louis-F.; Benz, Benjamin; Eikenberg, Ronald: Risiko verdrängt und vergessen. Industriesteuerungen nach über zwei Jahren noch verwundbar. In c't Magazin für Computertechnik, 21, 2015; S. 86–87.

[STA2025a] Statista GmbH: Bestand an gültigen ISO-27001-Zertifikaten in Deutschland in den Jahren 2006 bis 2023. URL: https://de.statista.com/statistik/daten/studie/829353/umfrage/bestand-an-vergebenen-iso-27001-zertifikaten-in-deutschland/.

[STA2025b] Statista GmbH: Anzahl der umsatzsteuerpflichtigen Unternehmen[1] in Deutschland von 2004 bis 2023. URL: https://de.statista.com/statistik/daten/studie/246358/umfrage/anzahl-der-unternehmen-in-deutschland/.

[STE2019] Steinke, Kai; Tebbje, Sebastian; Niemann, Karl-Heinz: Änderung von IT-Security-Anforderungen durch den Wandel der Automatisierungsstrukturen im Kontext von Industrie 4.0. In (Bauer, B.; Wittenberg, Carsten Hrsg.): Tagungsband AALE 2019. 16. Fachkonferenz, Autonome und intelligente Systeme in der Automatisierungstechnik, 2019; S. 97–104.

[TOF2009] Tofino Security: Daimler Chrysler Cyber Security Incident case Profile. Virus shuts down 13 plants; loss estimated at $14 million. URL: https://www.tofino-security.com/sites/default/files/CP-104-Case_Profile-Daimler_Chrysler-rev1.pdf.

[TÜV2025] TÜV-Verband: TÜV Cybersecurity Studie 2025 - Cybersicherheit in deutschen Unternehmen. Neue Bedrohungslage – besserer Schutz. URL: https://www.tuev-verband.de/fileadmin/user_upload/Content_local/Studien_local/2025_TUEV-Verband_Cybersecurity-Studie_Studienbericht.pdf.

[UR_E26] International Association of Classification Societies (IACS), UR E26 REV1 CR: Cyber resilience of ships, 2023. URL: https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/02/04140503/UR-E26-Rev.1-Nov-2023-CR.pdf.

[UR_E27] International Association of Classification Societies (IACS), UR E27 Rev. 1: Cyber resilience of on-board systems and equipment, 2023. URL: https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/29103853/UR-E27-Rev.1-Sep-2023-CLN.pdf.

[VDI_2182_1] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA), VDI/VDE 2182 Blatt 1: Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell. Beuth Verlag, Berlin, 2020. URL: https://www.dinmedia.de/de/technische-regel/vdi-vde-2182-blatt-1/314114388.

[VDI_2182_2_1] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA), VDI/VDE 2182 Blatt 2.1: Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Hersteller Speicherprogrammierbare Steuerung (SPS). Beuth Verlag, Berlin, 2013. URL: http://www.beuth.de/de/technische-regel/vdi-vde-2182-blatt-21/170847294?SearchID=889635358.

[VDI_2182_2_2] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA), VDI/VDE 2182 Blatt 2.2: Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Maschinen- und Anlagenbauer Umformpresse. Beuth Verlag, Berlin, 2013. URL: http://www.beuth.de/de/technische-regel/vdi-vde-2182-blatt-22/173513663?SearchID=889639460.

[VDI_2182_2_3] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA), VDI/VDE 2182, Blatt 2.3: Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Maschinen- und Anlagenbauer für Betreiber Presswerk. Beuth Verlag, Berlin, 2017.

[VDI_2182_3_1] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA), VDI/VDE 2182 Blatt 3.1: Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Hersteller Prozessleitsystem einer LDPE-Anlage. Beuth Verlag, Berlin, 2013. URL: http://www.beuth.de/de/technische-regel/vdi-vde-2182-blatt-31/187310424?SearchID=890274896.

[VDI_2182_3_2] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA), VDI/VDE 2182 Blatt 3.2: Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Integratoren LDPE-Reaktor. Beuth Verlag, Berlin, 2013. URL: http://www.beuth.de/de/technische-regel/vdi-vde-2182-blatt-32/167996669?SearchID=890279216.

[VDI_2182_3_3] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA), VDI/VDE 2182 Blatt 3.3: Informationssicherheit in der industriellen Automatisierung Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Betreiber LDPE-Anlage. Beuth Verlag, Berlin, 2013. URL: http://www.beuth.de/de/technische-regel/vdi-vde-2182-blatt-33/170881034.

[VDM2023] VDMA - Verband der Maschinen und Anlagenbauer e. V.: VDMA Lastenheft Supply Chain Security. Betreiber - Integrator. URL: https://www.vdma.org/documents/34570/14530044/SuD_2023-01+VDMA+Supply+Chain+Security+Lastenheft_Datei.pdf.

[VDS_10000] VdS Schadenverhütung GmbH, VdS 10000:2025-01(03): Informationssicherheitsmanagementsystem für kleine und mittlere Unternehmen (KMU), 2025. URL: https://shop.vds.de/publikation/vds-10000.

[VDS_10020] VdS Schadenverhütung GmbH, VdS 10020:2020-04(02): Cyber Security für kleine und mittlere Unternehmen (KMU) - Leitfaden zur Interpretation und Umsetzung der VdS 10000 für Industrielle Automatisierungssysteme, Köln, 2018. URL: https://shop.vds.de/publikation/vds-10020.

[VIS2020] Visoky, Jack; Wiberg, Joakim: CIP Security and IEC 62443-4-2. URL: https://www.odva.org/wp-content/uploads/2020/05/2020-ODVA-Conference_CIP_Security_and_IEC_62443_Visoky_Wiberg_Final.pdf.

[VOß2024] Voß, Marvin; Kallisch, Jonas; Runge, Maxim; Theus, Tobias; Niemann, Karl-Heinz; Wunck, Christoph: IT-Security Risk Based Approach for Secure Operation of Distributed Data Platforms in Supply Chains: 2024 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM). IEEE, 2024; S. 952–958.

[WAG2025] WAGO Kontakttechnik GmbH & Co. KG: Wago Security-Hinweise Automatisierungskomponenten über VDE-CERT. URL: https://www.wago.com/de/automatisierungstechnik/security, 31.07.2018.

[WAL2023] Walz, Andreas; Niemann, Karl-Heinz; Göppert, Julian; Fischer, Kai; Merklin, Simon; Ziegler, Dominik; Sikora, Axel: PROFINET Security: A Look on Selected Concepts for Secure Communication in the Automation Domain: 2023 IEEE 21st International Conference on Industrial Informatics (INDIN). IEEE, 2023 - 2023; S. 1–6.

[WUL2022] Wulfmeier, Kirsten; Niemann, Karl-Heinz: Befragung zur Auswertung von Security Advisories im Produktionsumfeld durch KMU. URL: https://doi.org/10.25968/opus-2303.

[ZET2016] Zetter, Kim: Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. URL: http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/, 05.03.2016.