Hochschule Wismar
Fakultät für Ingenieurwissenschaften
Bereich Elektrotechnik und Informatik

Master-Thesis

Erstellung eines Umsetzungsleitfadens informationstechnischer Sicherheitsmaßnahmen für Maschinen anhand der IEC-62443

Fassung zur Veröffentlichung

Eingereicht am: 17. September 2024
von: Max-Florian Beck
Betreuer: Prof. Dr. rer. nat. Nils Gruschka
Zweitbetreuerin: Prof. Dr.-Ing. Antje Raab-Düsterhöft

I. Aufgabenstellung

Englischer Titel: Creation of an Implementation Guideline for Cybersecurity Countermeasures for Machines based on IEC-62443

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Lagebericht des Jahres 2023 die Cyber-Sicherheitslage als angespannt bis kritisch eingeschätzt. „Die Bedrohung im Cyberraum ist damit so hoch wie nie zuvor“ [1]. Die Industrie wird dabei besonders häufig Ziel von Double-Extortion, ein Angriff mit Ransomware in Verbindung mit möglichem Daten-Leak. Diese Angriffe fokussieren sich zumeist auf das Büronetzwerk eines Unternehmens, beeinträchtigen aber dennoch auch maßgeblich die Produktion [2].

Vor allem kleine und mittelständische Maschinenbauer stehen vor dem Problem, den zunehmenden Anforderungen von Regulatorien, sowie den Ansprüchen der Kunden gerecht zu werden und sich ausreichend gegen Cyberangriffe zu schützen. Es stehen oftmals nicht genug finanzielle Mittel zur Verfügung eine Vollzeitkraft für das Thema der Cyber Security abzustellen. Des Weiteren verweisen Regulatorien und Normen oftmals auf den „Stand der Technik“, was dies bedeutet oder um welche Sicherheitsmaßnahmen es sich dabei namentlich handelt, wird nicht näher definiert.

Die Master-Thesis soll dabei Abhilfe schaffen und den mittelständischen Maschinenbauern einen Umsetzungsleitfaden bereitstellen, welcher neben Katalogen zur Ausformulierung des Stands der Technik auch Prozesse definiert, welche die Sicherheit der Maschinen erhöht. Darüber hinaus wird ein Einblick in die geltenden Regulatorien gewährt, mit dem Fokus, welche Anforderungen speziell an den deutschen Maschinenbau gestellt werden. Ein Abnahmeprotokoll soll zudem die Sicherheit der Maschine, als auch die Gesetzeskonformität validieren.

II. Kurzreferat

Durch die steigenden rechtlichen Anforderungen in Bezug auf die Informationssicherheit innerhalb der EU, stehen Maschinenbauer vermehrt vor der großen Herausforderung ihre Maschinen sicher zu gestalten und den Kundenanforderungen zukünftig gerecht zu werden. Das Ziel der Arbeit ist es, einen Umsetzungsleitfaden bereit zu stellen, welcher den Maschinenbauern neben der Erarbeitung der konkreten rechtlichen Anforderung durch verschiedene Gesetze, konkrete technische als auch organisatorische Maßnahmen zur Erhöhung der Sicherheit der Maschinen, sowie Tools und Vorgehensweisen für die Validierung dieser Sicherheitsmaßnahmen, zur Hand gibt. Durch die risikobasierte Bewertung der Sicherheit, welche sich an der IEC-62443-3-2 orientiert, erhält der Maschinenbauer zusätzlich zum Umsetzungsleitfaden ein Abnahmeprotokoll, um seinen Kunden die Sicherheit der Maschine zu belegen. Mit der Durchführung des Leitfadens und der abschließenden Dokumentation aller Schritte im Abnahmeprotokoll, erfüllt der Maschinenbauer die kommenden rechtlichen Anforderungen.

III. Abstract

Due to the increasing legal requirements regarding cyber security within the EU, machine manufacturers are increasingly faced with major challenges in designing their machines securely and meeting customers' requirements in the future. The aim of this paper is to provide an implementation guide which, in addition to the development of the specific legal requirements through various laws, also provides concrete technical and organizational countermeasures to increase the security of the machines, as well as tools and procedures for validating these countermeasures. Through the risk-based cyber security assessment, which is based on IEC-62443-3-2, the machine manufacturer receives an acceptance report in addition to the implementation guide to prove the cyber security of the machine to its customers. By carrying out the implementation guide and finally documenting all steps in the acceptance protocol, the machine manufacturer meets the upcoming legal requirements.

IV. Inhalt

1 Einleitung

1.1 Problemstellung

Der Lagebericht aus dem Jahr 2023 des Bundesamts für Sicherheit in der Informationstechnik beschreibt die Cyber-Sicherheitslage als angespannt bis kritisch. Die Industrie wird besonders häufig Ziel von Cyberangriffen mit Ransomware, es werden häufiger Schwachstellen gefunden und auch künstliche Intelligenzen erhalten Einzug in kriminelle Machenschaften [1].

Zu der steigenden Cyber-Bedrohung kommt eine wachsende Regulatorien-Landschaft hinzu. Mit der neuen EU-Cybersicherheitsstrategie hat die EU allein in den letzten 5 Jahren vier Gesetze zur Stärkung der Cybersicherheit vorgelegt, darunter der Rechtsakt zur Cybersicherheit, Cyber-Solidaritätsgesetz, Cyber Resilience Act und die NIS2. Weitere Regulatorien wie die Maschinenverordnung erschweren die Übersicht über geltende Bestimmungen zusätzlich.

Auch die Normenlandschaft sieht weniger übersichtlich aus. So existieren verschiedene Normen zur Umsetzung von Cyber-Sicherheitsstrategien, wie beispielsweise die ISO-27000-Reihe, BSI-200-Reihe, IEC-62443 oder die VDI/VDE 2182, um nur einige zu nennen.

Die in Regulatorien oft verwendete Klausel „Stand der Technik“ wird weder in Regulatorien, noch in Normen näher definiert und beschrieben. Es ist also nicht ersichtlich, welche technischen und organisatorischen Maßnahmen hierbei tatsächlich eingesetzt werden sollten, um die entsprechenden Anforderungen zu erfüllen.

1.2 Zielsetzung

Das Ziel der Arbeit ist die Erstellung eines Umsetzungsleitfadens informationstechnischer Sicherheitsmaßnahmen für Maschinen anhand der IEC-62443. Dieser Umsetzungsleitfaden soll als Unterstützung für Maschinenbauer dienen, um den rechtlichen Anforderungen auch zukünftig gerecht werden zu können und die Konformität leichter zu erreichen.

Aus dieser Zielsetzung ergeben sich folgende Teilziele:

- Erarbeitung der rechtlichen Anforderungen an Maschinenbauer
- Prüfung der gesetzlichen Konformität der IEC-62443
- Ausformulierung des Stands der Technik in technische und organisatorische Maßnahmen in Form von Katalogen
- Bereitstellung von Methoden und Tools zur Bewertung und Prüfung der eingesetzten Maßnahmen
- Detaillierte Erklärung des IEC-62443-3-2 – Cyber Security Risikobewertungsprozesses
- Erstellung von Begleitmaterialien für den Cyber Security Risikobewertungsprozess
- Bereitstellung eines Abnahmeprotokolls für Maschinenbauer

1.3 Abgrenzung

Der Schwerpunkt dieser Arbeit liegt im Bereich des Maschinen- und Anlagenbaus und richtet sich damit unmittelbar an Systeme der Produktion (OT = Operational Technology). Prozesse und Entwicklungen im IT-Bereich werden dabei nicht beachtet, sind aber zum Verständnis vieler Inhalte von Vorteil.

Die Zielgruppe dieser Arbeit sind hauptsächlich Integratoren, also Maschinen- und Anlagenbauer aus Deutschland. Die Zielgruppe ist aber nicht ausschließlich darauf limitiert. Auch Betreiber können von den Inhalten dieser Arbeit profitieren.

Der Begriff der „Cyber Security“ wird hier als Synonym für die Cyber-Sicherheit als auch Informationssicherheit verwendet und bezieht sich dabei auf den Schutz der Integrität, Verfügbarkeit und Vertraulichkeit von Systemen.

1.4 Vorgehensweise

Zu Beginn werden im Grundlagenteil die verschiedenen geltenden und zukünftig geltenden Gesetze begutachtet und grundlegend erläutert. Dazu gehört neben dem Europäischen Rechtsakt zur Cybersicherheit und dem NIS2 Umsetzungs- und Cybersicherheitsstärkungsgesetz auch der Cyber Resilience Act, sowie die

Maschinenverordnung. Im normativen Grundlagenteil wird die IEC-62443 als zentrale Norm der OT-Security vorgestellt. Dabei werden vor allem die verschiedenen Kernaspekte der Norm dargestellt.

Anschließend werden zwei Anforderungsanalysen durchgeführt. Zum einen wird analysiert, welche rechtlichen Anforderungen es aus den zuvor eingeführten Gesetzen für Maschinen und Anlagenbauer zu beachten gilt, zum anderen muss anhand der rechtlichen Anforderungen analysiert werden, inwieweit die IEC-62443 diese Anforderungen erfüllt.

Darauffolgend, wird der Umsetzungsleitfaden vorgestellt und erklärt, wie mit diesem gearbeitet werden soll, um ein aussagekräftiges Ergebnis zu erzielen.

Ein weiterer Schritt ist die Erstellung der Kataloge, in denen sowohl technische, als auch organisatorische Maßnahmen ausformuliert werden und damit den Stand der Technik als reale Maßnahmen definieren. Ebenso werden in einem Katalog Prüftools und Prüfverfahren berücksichtigt und erklärt, welche die Sicherheitsmaßnahmen validieren. Sowohl zu den Maßnahmen, als auch zu den Prüftools und -Verfahren, sollen ausführliche Beschreibungen zur leichten Implementierung erstellt werden. Ein Bedrohungskatalog als Vorlage für verschiedene Risikobeurteilungen wird ebenfalls erstellt.

Mit der Beschreibung des Cyber Security Risikobewertungsprozess wird danach ein zentraler Punkt des Leitfadens inhaltlich erläutert. Zur Erleichterung der Umsetzung, werden zusätzliche Begleitmaterialien erstellt.

Abschließend wird ein Abnahmeprotokoll erstellt, welches alles beinhalten soll, was zur Erreichung der gesetzlichen Konformität nötig ist, und als Bestätigung der Sicherheit der Maschine dient.

2 Grundlagen

In diesem Kapitel werden die grundlegenden Informationen zum Verständnis der vorliegenden Arbeit gegeben. Informationstechnische Grundlagen werden dabei jedoch vorausgesetzt, da eine Erklärung dieser den Umfang der Arbeit deutlich überschreiten würde. Zu Beginn wird eine Übersicht über die zum Zeitraum der Arbeit aktuellen Bedrohungslager der Cyber Security gegeben, ehe rechtliche Grundlagen, darunter die geltenden und zukünftig geltenden Gesetze im Anwendungsbereich der Arbeit, beschrieben werden. Abschließend zu den rechtlichen Grundlagen führen die normativen Grundlagen in die aktuell als Stand der Technik geltenden Norm, IEC-62443, ein.

2.1 Aktuelle Bedrohungslage

Der BSI-Lagebericht 2023, zur Lage der IT-Sicherheit in Deutschland, beschreibt die Lage als angespannt bis kritisch. „Die Bedrohung im Cyberraum ist damit so hoch wie nie zuvor. […] Kleine und mittlere Unternehmen […] wurden überproportional häufig angegriffen“ [1]. Auch der Cybercrime Bundeslagebericht des Bundeskriminalamts von 2023 bewertet das verarbeitende Gewerbe als die am stärksten von Ransomware- bzw. Double Extortion-Angriffen betroffene Branche [3].

„Pro Jahr entstehen der deutschen Wirtschaft 206 Milliarden Euro Schaden durch Diebstahl von IT-Ausrüstung und Daten sowie digitale und analoge Industriespionage“, erklärt der Bitkom-Präsident Dr. Ralf Wintergerst. Weiter sagt er: „Inzwischen entfallen davon 148 Milliarden Euro, also 72 Prozent, auf reine Cyberangriffe, 2021 lag der Anteil noch bei 59 Prozent“ [4]. In zwei Jahren stieg der Anteil der Schäden durch reine Cyberangriffe auf die deutsche Wirtschaft um 13 Prozentpunkte an.

Auch nahmen die Schwachstellen in Softwareprodukten im Berichtszeitraum des BSI-Lagerberichts 2023 um 24 Prozent, auf mehr als 2000 Schwachstellen pro Monat, zu [1]. Ein Faktor ist dabei, dass die Software-Qualität der Betriebssysteme und Anwendungen für die heutige Bedrohungslage nicht mehr

ausreicht. Hier ist die Fehlerdichte, also die Anzahl der Softwarefehler pro 1000 Zeilen Code, bei qualitativ hochwertiger Software im Schnitt 0,3. Bei ca. 10 Millionen Zeilen bei heutigen gängigen Betriebssystemen wären dies im Schnitt 3000 Software-Fehler und damit potenzielle Schwachstellen [5].

Zusätzlich wurden im Berichtszeitraum des BSI-Lageberichts 2023 rund eine Viertelmillionen neue Schadprogamm-Varianten durchschnittlich pro Tag gefunden [1]. Dies ist eine beunruhigende Zahl, vor Allem bei dem Hintergrund, dass die Anti-Malware-Lösungen bei Massen-Angriffen mit 75 Prozent bis 95 Prozent eine zu schwache Erkennungsrate haben. „Bei gezielten und direkten Angriffen auf IT-Systeme liegt die Erkennungsrate im Schnitt sogar nur bei 27 Prozent“ schreibt Prof. Dr. Norbert Pohlmann, Professor für Informationssicherheit an der Westfälischen Hochschule, in seinem Buch „Cyber-Sicherheit“ [5].

Ein weiterer Negativtrend, welcher die aktuelle Bedrohungslage weiter verschärft, ist der Einzug generativer KI in kriminelle Machenschaften. Neben KI-Modellen zur Entwicklung von Deep-Fakes und gefälschten Audio-Dateien [1], ist die rasante Zunahme verschiedener krimineller Chat-Bots wie FraudGPT, WormGPT oder DarkBart, um nur ein paar zu nennen, kritisch einzuordnen. Diese Chat-Bots sind in der Lage Phishing-Mails täuschend echt und schnell zu generieren oder dabei zu unterstützen Schadsoftware zu schreiben, wie Dipl.-Ing. (FH) Stefan Luber in Artikeln von Security Insider berichtet [6], [7], [8].

2.2 Rechtliche Grundlagen

Sowohl auf nationaler, als auch internationaler Ebene, steigen die Anforderungen an die Cyber Security enorm. In den letzten fünf Jahren wurden von der EU vier Gesetze zur Stärkung der Cybersicherheit vorgelegt [9]. Auf nationaler Ebene ist Deutschland von diesen Gesetzen als Mitgliedsstaat direkt betroffen, weshalb diese Gesetze auch die Richtung für Maschinenbauer weisen. Auf EU-Ebene muss man bei der Gesetzgebung zwischen einer Verordnung (englisch: Act) und einer Richtlinie (englisch: Directive) unterscheiden. Während eine Verordnung unmittelbar nach einer Übergangsfrist für alle Mitgliedsstaaten verbindlich gilt,

somit auch in jedem EU-Mitgliedsland gleich ist, muss eine Richtlinie erst in nationales Recht umgewandelt werden. Die Richtlinie gibt den einzelnen Mitgliedsstaaten nur Rahmenbedingungen, welche erzielt werden müssen. Wie genau jedes Land diese Rahmenbedingungen erfüllt, ist ihnen selbst überlassen.

Nachfolgend werden die wichtigsten und aktuellen Gesetze, welche in Deutschland gelten oder zukünftig gelten werden, vorgestellt. Die Erarbeitung der tatsächlichen Anforderungen an Maschinenbauer, welche sich daraus ergeben, werden in Kapitel 3 folgen.

2.2.1 Entwicklung der Informationssicherheit in Deutschland

Das Bewusstsein für Informationssicherheit ist in Deutschland schon lange vor dem Internet existent. Die Zentralstelle für das Chiffrierwesen (ZfCh) beschäftigte sich seit den 1950er Jahren mit kryptografischen Verschlüsselungen zur Sicherung von Kommunikationskanälen. Natürlich waren diese Themen davor schon essenziell, allerdings hauptsächlich militärischer Natur. Die ZfCh wurde 1989 in die Zentralstelle für Sicherheit in der Informationstechnik (ZSI) umbenannt. Nur zwei Jahre später, im Gründungsjahr des WorldWideWebs 1991, wurde die ZSI in ein Bundesamt überführt [10]. Dieses Bundesamt, das Bundesamt für Sicherheit in der Informationstechnik (BSI), ist auch heute noch zuständig für die „Prävention, Detektion und Reaktion der Informationssicherheit für Staat, Wirtschaft und Gesellschaft“ in Deutschland [11].

Mit dem Inkrafttreten des Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes, am 20. August 2009, welches das Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik vom 01. Januar 1991 ablöste, wurden die Grundsteine des heute geltenden BSI-Gesetzes gelegt. Damit wurden dem BSI weitere Aufgaben und Befugnisse übermittelt, um den herrschenden Bedrohungen entgegenwirken zu können. Bereits 6 Jahre später wurde das BSI-Gesetz durch das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), am 25. Juli 2015, in größeren Umfang ergänzt. Ziel hierbei war es, die erkannten und entstandenen Defizite im Bereich der IT-Sicherheit, insbesondere außerhalb der

Bundesverwaltung im sogenannten KRITIS-Sektor, weiter wirksam begegnen zu können [12].

Ebenfalls 6 Jahre später war es wieder Zeit, den steigenden Herausforderungen entgegenzutreten, wodurch das IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0), am 18. Mai 2021, im Bundesgesetzblatt veröffentlich wurde. Das IT-SiG 2.0 stärkt das BSI dabei in folgenden Punkten [13]:

- Detektion und Abwehr
- Cybersicherheit in den Mobilfunknetzen
- Verbraucherschutz
- Sicherheit für Unternehmen
- Nationale Behörde für Cybersicherheitszertifizierung

Auch auf europäischer Ebene sind Regulatorien ein wichtiges Mittel, um der steigenden Bedrohungslage entgegenzuwirken. So wurde am 06. Juli 2016 die Richtlinie 2016/1148, über „Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union“, die sogenannten NIS-Richtlinie, verabschiedet. Der deutsche Staat hatte mit dem IT-SiG einige Punkte der NIS-Richtlinie bereits abgedeckt, hatte aber dennoch in anderen Punkten Nachholbedarf, weshalb das „Gesetz zur Umsetzung der NIS“ am 29.06.2017 verabschiedet wurde, um den Anforderungen der NIS gerecht zu werden [14].

Am 16. Januar 2023 trat die NIS2-Richtlinie in Kraft, mit dem Ziel, die NIS-Richtlinie zu erweitern und das gemeinsame Gesamtniveau der Cybersicherheit innerhalb der EU weiter zu erhöhen. Deutschland wird die NIS2-Richtlinie mit dem sogenannten NIS-2-Umsetzungs-und-Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) in nationales Recht umsetzen. Der Inhalt des NIS2UmsuCG wird in Kapitel 2.2.3 näher beleuchtet [9].

2.2.2 Europäischer Rechtsakt zur Cybersicherheit

Der europäische Rechtsakt zur Cybersicherheit (Cybersecurity Act) trat am 27. 06.2019 in Kraft (Verordnung (EU) 2019/881). Der Schwerpunkt liegt auf der Stärkung der ENISA (European Network and Information Security Agency), unter anderem durch ein permanentes Mandat. Ein weiterer Schwerpunkt ist die Einführung eines einheitlichen europäischen Cybersicherheitszertifizierungsrahmen für IKT-Produkte, -Dienstleistungen und -Prozesse. Mit dem Änderungsvorschlag der Kommission vom 18. April 2023, sollten auch Zertifizierungssysteme für verwaltete Sicherheitsdienste ermöglicht werden [15].

Um die Cybersicherheitszertifizierung zu etablieren, wurde am 31.Januar 2024 die Durchführungsverordnung (EU) 2024/482 der Kommission mit Durchführungsbestimmungen zur Verordnung (EU) 2019/881 geltend gemacht. In der Durchführungsverordnung wird die Cybersicherheitszertifizierung anhand der Common Criteria durchgeführt. Diese beruht auf der Norm ISO/IEC 15408 und bietet allgemeine Kriterien für die Bewertung der Sicherheit von Informationstechnologien. Diese Rechtsgrundlage soll harmonisierend mit den zukünftig kommenden Gesetzestexten einhergehen [16].

2.2.3 NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)

Das NIS2UmsuCG dient dazu, die EU-weiten Mindestanforderungen für Cyber Security der NIS2 in nationales Recht zu überführen.

Dem dieser Arbeit zugrunde liegende Stand des NIS2UmsuCG ist der Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ mit dem Bearbeitungsstand vom 22.07.2024 um 16:45 Uhr. Alle weiteren Ergänzungen, sowie den schlussendlichen Gesetzestext, können in dieser Arbeit daher nicht betrachtet und beachtet werden.

Einordung der Einrichtungen:

Im Gesetz werden drei unterschiedliche Gruppierungen definiert. In § 28 Abs. 1 NIS2UmsuCG wird die Gruppe der besonders wichtigen Einrichtungen eingeführt, § 28 Abs. 2 definiert die Gruppe der wichtigen Einrichtungen und § 29 die Einrichtungen der Bundesverwaltung. Mindestens 30.000 Unternehmen sind laut der OpenKRITIS damit von der NIS2UmsuCG in Deutschland betroffen [17].

Welche Rahmenbedingungen gelten, um den einzelnen Gruppierungen zugeordnet zu werden, wird in Bild 1 gezeigt.

Einrichtung	Größe	Rahmenbedingung	Sektoren
Besonders wichtig § 28 Abs. 1	Groß-unternehmen aus Anlage 1	> 249 Mitarbeiter oder JU von 50 Mio. € und JB von > 43 Mio. €	Energie, Transport/Verkehr, Finanzen/Versicherungen, Gesundheit, Wasser/Abwasser, IT und TK, Weltraum
	Mittlere TK Unternehmen	> 49 Mitarbeiter oder JU und JB von > 10 Mio. €	Anbieter öffentlicher TK-Netze und TK-Dienste
	Unabhängig	Keine	Qualifizierte Vertrauendienste, TLD-Registries, DNS-Dienste, Betreiber kritischer Anlagen (KRITIS-Betreiber)
Wichtig § 28 Abs. 2	Mittlere Unternehmen aus Anlage 1 Unternehmen aus Anlage 2	> 49 Mitarbeiter oder JU und JB von > 10 Mio. €	Energie, Transport/Verkehr, Finanzen/Versicherungen, Gesundheit, Wasser/Abwasser, IT, Weltraum, Post/Kurier, Siedlungsabfallentsorgung, Chemie, Lebensmittel, Verarbeitendes Gewerbe, Digitale Dienste, Forschung
	Kleine TK	< 50 Mitarbeiter oder JU und JB < 10 Mio. €	Anbieter öffentlicher TK-Netze und TK-Dienste
	Unabhängig	Keine	Vertrauensdienstanbieter
Bundes-verwaltung § 29	Stellen des Bundes, Körperschaften, Anstalten, Stiftungen des öffentlichen Rechts sowie ihre Vereinigungen, öffentliche Unternehmen die mehrheitlich im Eigentum des Bundes stehen und die IT-Dienstleistung für die Bundesverwaltung erbringen - die keine Institution der sozialen Sicherung sind		
JU = Jahresumsatz JB = Jahresbilanzsumme			

Bild 1: Einordnung der Einrichtungen im NIS2UmsuCG

Quelle: Eigene Darstellung nach [17]

Betroffenheit und Herausforderungen des Maschinenbaus:

Der Maschinen- und Anlagenbau (nachfolgend nur Maschinenbau genannt) ist nach der Definition im Sektor „Verarbeitendes Gewerbe“ angesiedelt und zählt somit zu den wichtigen Einrichtungen nach §28 Abs. 2 NIS2UmsuCG. Der Verein Deutscher Maschinen- und Anlagenbauer (VDMA) benennt eine Zahl von mehr als 3600 (3646 lt. Abbildung 1 [18]) betroffenen Maschinenbauer, was 58% der gesamten Branche bedeutet. Davon beschäftigen rund 75% der Unternehmen weniger als 250 Mitarbeiter und gelten damit, gemäß der EU-KMU-Definition, als kleine und mittelständische Unternehmen [19]. Damit zählt der Maschinenbau als am stärksten betroffene Branche des NIS2UmsuCG in Deutschland [18].

Die Herausforderungen im Maschinenbau in Verbindung mit dem NIS2UmsuCG sind vielseitig. Zum einem herrscht bei Maschinenbauern eine doppelte Betroffenheit, zum anderen sind die vorhandenen Ressourcen für die Umsetzung und das Personal meist begrenzt. Die doppelte Betroffenheit ergibt sich zum einen daraus, dass die eigene IT die eigenen Systeme auf die Mindeststandards des NIS2UmsuCG aufrüsten müssen, sowie die organisatorischen Anforderungen und Prozesse etabliert und anschließend gelebt werden müssen. Viele dieser mittelständischen Unternehmen haben meist nur eine kleine IT-Abteilung oder lassen sich sogar komplett von externen Dienstleistern administrieren. Hier besteht also ein enormer Schulungs-, Planungs-, Zeit- und Umsetzungsaufwand, welcher wiederum hohe finanzielle Kosten mit sich bringt.

Auf der anderen Seite sind viele mittelständische Maschinenbauer Dienstleister für große Unternehmen. Diese Unternehmen fallen ebenfalls unter das NIS2UmsuCG und könnten zu besonders wichtigen Einrichtungen zählen, wodurch die Anforderungen an die eigenen Systeme steigen, welche wiederum auf die Maschinen und Dienstleistungen der Maschinenbauer abgewälzt werden. Hier muss also maßgeblich die OT nachgebessert werden. Viele dieser Systeme werden jedoch als Insellösungen verkauft, wodurch Security-Maßnahmen daher nicht unbedingt dem Stand der Technik entsprechen.

Hinzu kommen mögliche Neuzertifizierungen, welche ebenfalls mit hohen Kosten und Zeitaufwänden verbunden sind. Die OpenKRITIS befürchtet: „Existierende ISMS-Zertifizierungen werden meist nicht ohne weiteres hinreichend für NIS2-Maßnahmen sein - der Geltungsbereich von NIS2 könnte über bestehende Zertifikate hinausgehen, die genannten Maßnahmen sind teils tiefer und weiter als übliche Rahmenwerke“ [17]. Ob dies tatsächlich der Fall sein wird, muss von den verschiedenen Prüfungseinrichtungen und den Gesetzgebern allerdings noch geprüft werden.

Pflichten wichtiger Einrichtungen:

Die Pflichten der Einrichtungen sind von der NIS2UmsuCG klar vorgegeben und im Vergleich zu älteren Gesetzen, wie den BSI-Gesetzen, teils verschärft, teils präzisiert und neu strukturiert. Für wichtige Einrichtungen gelten dabei folgende Pflichten [20]:

- Maßnahmen des Risikomanagements (§ 30)
- Meldepflichten (§ 32)
- Registrierung (§ 33 und § 34)
- Unterrichtungspflichten an Kunden (§ 35)
- Schulung und Verantwortung der Leitungsorgane (§ 38)
- Teilweise Nachweise nach § 39 i.V.m. § 66

Mögliche Bußgelder bei Nichtbeachtung:

Um einen hohen Druck und damit eine hohe Umsetzungsrate bei den verschiedenen Einrichtungen zu erzielen, definiert das NIS2UmsuCG einige Tatbestände, bei welchen ein Bußgeld fällig wird. Die Bußgelder variieren dabei zwischen 100.000 € und 7 Mio. €, oder 1,4 % des gesamten weltweiten, im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens. Diese Summen können sehr schmerzhaft sein und wirken dementsprechend abschreckend. Bei welchen Tatbeständen welches Bußgeld greift, wird in dieser Arbeit nicht näher erläutert. Diese sind entweder im Umsetzungsleitfaden online nachzulesen [21] oder direkt im entsprechenden Gesetzestext unter § 65 NIS2UmsuCG zu finden [20].

2.2.4 Cyber Resilience Act

Die „Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen“, auch Cyber Resilience Act (CRA) genannt, dient der Erhöhung der Cyber Security von digitalen Produkten im gesamten europäischen Wirtschaftsraum. Der CRA soll noch in der zweiten Hälfte des Jahre 2024 in Kraft treten. Bis 2027 müssen die Wirtschaftsakteure dann konforme Produkte auf dem Unionsmarkt in Verkehr bringen, während die daraus hervorgehenden Meldepflichten bereits bis 2026 gelten [22].

Der CRA wird sowohl Hardware als auch Software betreffen, solange diese eine digitale Komponenten besitzen. Dies bedeutet, dass es sich um Produkte handelt, „deren bestimmungsgemäße oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt“. Open-Source-Software ist dabei ebenso betroffen wie eigens geschrieben Software. [23]. Ausnahmen gibt es lediglich für Produkte, welche über andere Regulatorien überwacht werden, zum Beispiel Medizinprodukte oder Produkte für die Zivilluftfahrt.

Kategorien von Produkten:

Die Verordnung definiert vier unterschiedliche Produktkategorien. Besondere Anforderungen gelten dabei für die Kategorien der kritischen Produkte mit digitalen Elementen der Klasse 1 und 2, sowie hochkritischen Produkten. Sonstige „unkritische“ Produkte mit digitalen Elementen müssen keine Anforderungen erfüllen. Welche Produkte unter die Kategorien der kritischen Produkte fallen, ist in Anhang 3 des CRAs definiert. Hochkritische Produkte wurden zunächst noch keine definiert [23].

Ein Teil der industriellen Produkte wie Industrial Internet of Things-Geräte (IIoT) oder Inudstrial Automation and Control Systems (IACS) werden abhängig von ihrem Einsatzort eingeteilt. Werden diese für den Einsatz in wesentlichen Einrichtungen gemäß Anhang 1 der Richtlinie NIS2 bestimmt, so gehören diese der Klasse 2 an und sind damit auch relevant für den Maschinenbau. Eine Auswahl, der den Maschinenbau betreffenden Produkten ist in Bild 2 zusehen.

Es kann sein, dass durch individuelle Anwendungen und Umsetzungen weitere Produkte im industriellen Einsatz verwendet werden, welche hier nicht abgebildet sind, es ist daher empfehlenswert, sich an Anhang 3 des CRAs zu orientieren [23].

Kategorie	Betroffene Produkte
Maschinenbau-relevante Produkte der Klasse 1	Software für Identitätsmanagementsysteme und Software für die Verwaltung des privilegierten Zugangs, eigenständige und eingebettete Browser, Passwort-Manager, Software für die Suche/Entfernung/Quarantäne von Schadsoftware, Produkte mit digitalen Elementen mit der Funktion eines virtuellen privaten Netzes (VPN), Netzmanagementsysteme, Instrumente für die Netzkonfigurationsverwaltung, Systeme für die Überwachung des Netzverkehrs, SIEM-Systeme, Aktualisierungs- und Patchverwaltung, Software für Fernzugriff und gemeinsame Datennutzung, physische Netzschnittstellen, FPGAs für Einrichtungen gemäß Anhang 1 der NIS2
Maschinenbau-relevante Produkte der Klasse 2	Public-Key-Infrastrukturen und Aussteller digitaler Zertifikate, Firewalls/ Angriffs- und/oder -präventionssysteme für den industriellen Einsatz, Allzweck-Mikroprozessoren, Mikroprozessoren die für die Integration in speicherprogrammierbare Steuerungen und Sicherheitselemente bestimmt sind, Router, Modems für die Internetanbindung, Switche für den industriellen Einsatz, Sicherheitselemente, Hardware-Sicherheitsmodule, sichere Kryptoprozessoren, Chipkarten, Chipkartenleser, Token, IACS, IIoT-Geräte, Sensor- und Aktuatorkomponenten von Robotern und Robotersteuerungen

Bild 2: Maschinenbaurelevante Produktklassifizierung des CRA

Quelle: Eigene Darstellung nach Anhang des CRAs **[15]**

Die Anforderungen an den kritischen Produkten ergibt sich daraus, dass kritische Produkte der Klasse 1 und 2 den Konformitätsbewertungsverfahren nach Artikel 24 Abs. 2 und 3 unterliegen. Zusätzlich kann in Zukunft davon ausgegangen werden, dass ein zusätzlicher Rechtsakt, die Anforderungen an die verschiedenen Produkte ergänzen wird.

Betroffenheit und Herausforderungen des Maschinenbaus:

Der CRA definiert drei Wirtschaftsakteure, darunter den Hersteller, Einführer und Händler. Als Maschinenbauer zählt man dabei als Hersteller, da die Maschine als Produkt zählt. Durch die Kommunikationsfähigkeit der enthaltenen Komponenten, wird die Maschine zu einem Produkt mit digitalen Elementen.

Die Herausforderungen gehen hier einher mit den Pflichten der Hersteller, auf welche im nachfolgenden Kapitel eingegangen wird. Die Pflichten werden einen enormen Mehraufwand bei der Dokumentationspflicht mit sich bringen. Es müssen Prozesse zur Meldung von Mängeln der Produkte, sowie Verstöße gegen die Verordnung etabliert werden, welche sowohl den Kunden als auch zentrale Meldestellen betreffen. Bei der Heterogenität der eingesetzten Produkte in Maschinen im Maschinenbau wird es hier eine lange Liste an verschiedenen Hersteller- und Kundenkontakten geben, welche ordentlich gepflegt und im Falle eines Verstoßes informiert werden müssen.

Diese Maßnahmen erfordern ausgebildetes Fachpersonal, welches es laut der Deutschen Industrie und Handelskammer nur begrenz gibt. Diese teilte nämlich mit, dass: „Unternehmen [auch sehr häufig berichten], dass sie die dafür erforderlichen Fachkräfte nicht rekrutieren können“, weiter heißt es, dass eine Streckung der Übergangsfrist sinnvoll wäre, „um die sowieso bereits bestehenden Fachkräfteengpässe nicht weiter zu verschärfen“ [24].

Pflichten der Hersteller:

In § 10 werden verschiedene Pflichten an den Hersteller gestellt, darunter verschiedene Nachweis-, Melde- und Prüfungspflichten, welche in Kapitel 3.1 näher erläutert werden. Die Pflichten sind dabei sehr umfangreich und setzen vor allem eine erhöhte Dokumentation voraus. Unter anderem wird die Cyber Security Risikobewertung für den Maschinenbauer nun verpflichtend. Ebenso müssen Cyber Security Pflichten erfüllt sein, um das CE-Kennzeichen zu erlangen.

In § 9 wird eine doppelte Verpflichtung in Verbindung mit der Maschineverordnung und der darin enthalten EU-Konformitätserklärung erleichtert. Maschinenprodukte, welche die EU-Konformitätserklärung des CRAs erhalten, gelten in der Maschinenverordnung als grundlegend konform mit den dort enthaltenen Gesundheits- und Sicherheitsanforderungen im Anhang 3 Abschnitt 1.1.9 und 1.2.1 [23].

Mögliche Bußgelder bei Nichtbeachtung:

Der CRA nutzt ebenfalls das Mittel der Bußgelder, um einen hohen Umsetzungsdruck auf die verschiedenen Wirtschaftsakteure auszuüben. Diese fallen zudem um einiges höher und strenger aus als die aus dem NIS2UmsuCG, so mahnt § 53 Abs. 1 CRA: „Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein“ [23]. Hierbei variieren die Summen der Strafen zwischen 5 Mio. € bis 15 Mio. €, oder 1 % bis 2,5 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres. Dabei wird sich am höheren Betrag orientiert. Auf die genauen Tatbestände im CRA wird ebenfalls nicht näher eingegangen, diese sind im Umsetzungsleitfaden online [21] oder direkt im Gesetzestext unter § 53 CRA zu finden.

2.2.5 Maschinenverordnung

Die Europäische Maschinenverordnung (MVO) – Verordnung (EU) 2023/1230 über Maschinen – regelt ab dem 20.01.2027 das Inverkehrbringen von Maschinen im gesamten Europäischen Wirtschaftsraum [25]. Sie löst damit die bisher geltende Maschinenrichtlinie 2006/42/EG ab und sorgt, durch die Überführung in eine Verordnung, für eine europaweite gleichverpflichtende Erhöhung der Sicherheits- und Gesundheitsschutzanforderungen von Maschinen gegenüber Personen, gegebenenfalls Haustieren und Sachen, sowie, soweit anwendbar, der Umwelt.

Da die Vernetzung in Maschinen stetig steigt, gilt es, auch in Bezug auf die Sicherheits- und Gesundheitsschutzanforderungen, die Cyber Security als Kernaspekt für Zulassungen dieser Maschinen zu verankern. Da die funktionale Sicherheit kein Kernaspekt dieser Arbeit ist, wird nicht tiefer auf die Grundsätze

und Verpflichtungen der Maschinenverordnung eingegangen. Lediglich die Aspekte, welche die Cyber Security betreffen, werden kurz weiter ausgeführt.

Auswirkungen der Cyber Security auf die funktionale Sicherheit:

In Bezug auf die funktionale Sicherheit kann ein Cyberangriff fatale Folgen auf die rechtmäßige Funktion von Sicherheitseinrichtungen haben. Konkrete Beispiele wären hier die Manipulation von Sicherheitskommunikationskanälen, Veränderungen von Achsdaten oder das komplette Abschalten von Sicherheitseinrichtungen. Fehlen diese, ist ein sicherer Betrieb einer Maschine nichtmehr gewährleistet. Es könnte im schlimmsten Fall zu Naturkatastrophen kommen, wenn zum Beispiel Steuerungen oder Einrichtungen von Atomkraftwerken kompromittiert werden. Das dies technisch möglich ist, zeigte unter anderem der Computerwurm Stuxnet bereits im Jahre 2010 [26].

Cyber Security Pflichten der Maschinenbauer:

Die MVO besitzt zwei Unterkapitel, welche die Cyber Security von Maschinen adressiert. In Anhang 3 Abschnitt 1.1.9 wird der allgemeine Schutz einer Maschine oder eines dazugehörigen Produkts gegen Korrumpierung und in Abschnitt 1.2.1 die Sicherheit und Zuverlässigkeit von Steuerungen beschrieben. Beide Abschnitte setzen die Implementierung von Sicherheitsmaßnahmen und eine umfangreiche Dokumentation voraus. Diese Anforderungen müssen erfüllt sein, um die CE-Zertifizierung zu erhalten. Unter anderem ist die Risikobeurteilung daher nichtmehr nur für die funktionale Sicherheit verpflichtend, sondern auch für die Cyber Security. Besitzt man allerdings eine Cybersicherheitszertifizierung oder eine EU-Konformitätsbescheinigung, gelten die Abschnitte 1.1.9 und 1.2.1 als konform. Dies geht aus § 20 Abs. 9 hervor [25].

Auf die genaueren Pflichten, welche sich daraus ergeben, wird in Kapitel 3.1 näher eingegangen. Ebenso werden Maßnahmen zur Erfüllung der Pflichten in Kapitel 5 definiert.

2.3 Normative Grundlagen

Es existieren unterschiedliche Normen, welche das Thema der Cyber Security adressieren, darunter die ISO-27000-Reihe, die BSI-200-Reihe oder die VDI/VDE 2182. Für die Cyber Security im Bereich der Industriellen Kommunikationsnetze hat sich dabei vor allem die IEC-62443 etabliert. Der Fokus liegt in dieser Arbeit daher nur auf der IEC-62443, weitere Normen werden nicht beachtet.

2.3.1 Grundlagen der IEC-62443

Die IEC-62443, Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme, ist die führende Norm im Bereich der Sicherheit industrieller Netzwerke. Sie verfolgt einen risikobasierten Ansatz zur Bestimmung der Sicherheit betroffener Systeme. Die Norm spricht dabei verschiedene Akteure an und bietet somit ein Rahmenwerk über den gesamten Lebenszyklus und die gesamte Lieferkette von IACS. Diese besagten IACS sind dabei ein Begriff für eine große Gruppe von Systemen und Teilkomponenten, welche in der industriellen Umgebung verwendet werden. Darunter zählen Personen, speicherprogrammierbare Steuerungen, Sensoren und Aktoren, verschiedene Systeme zur Aufrechterhaltung und Planung der Produktion (Manufacturing Execution Systems, Manufacturing Operations Management Systems, Enterprise Ressource Planning Systems, …) und vielen mehr [27]. Nachfolgend werden die Grunddefinitionen und -prinzipien, sowie relevante Inhalte der Norm, näher erläutert.

Aufbau der IEC-62443-Reihe:

Die IEC-62443 besteht aus mehreren Teilen, welche in vier Bereiche eingeteilt werden. Jeder Bereich besitzt unterschiedliche Gebiete, welche berücksichtigt werden sollen. Die vier Bereiche sind dabei wie folgt gegliedert [27]:

IEC-62443-1-X General

- IEC-62443-1-1 Concepts and Models (TS)
- IEC-62443-1-2 Master glossary of terms and abbreviations
- IEC-62443-1-3 Security system conformance metrics
- IEC-62443-1-4 IACS security lifecycle and use cases

IEC-62443-2-X Policies and Procedures

- IEC-62443-2-1 Security program requirements for IACS asset owner
- IEC-62443-2-2 IACS security protection ratings
- IEC-62443-2-3 Patch management in the IACS environment (TR)
- IEC-62443-2-4 Requirements for IACS service providers
- IEC-62443-2-5 Implementation guidance for IACS asset owners

IEC-62443-3-X System

- IEC-62443-3-1 Security technologies for IACS
- IEC-62443-3-2 Security risk assessment and system design
- IEC-62443-3-3 System security requirments and security levels

IEC-62443-4-X Components and Requirements

- IEC-62443-4-1 Secure product development lifecycle requirements
- IEC-62443-4-2 Technical security requirements for IACS components

Klassifizierung der Akteure:

Die IEC-62443 definiert drei Hauptakteure nämlich: Betreiber, Integratoren und Hersteller. Eine Nebenrolle spielen sogenannte Service-Provider. Diese Akteure werden nachfolgend vorgestellt:

Betreiber (Asset Owner): Betreiber sind Endabnehmer, welche mit den Systemen einen Mehrwert generieren [28]. Dieser Mehrwert kann zum Beispiel durch Produkte oder Dienstleistungen geboten sein. Die Betreiber müssen daher die Systeme der Integratoren in ihr eigenes Unternehmensnetzwerk integrieren und betreiben. Dabei ist vor allem der sichere Betrieb besonders wichtig, um zum einen die Umwelt zu schützen, als auch die Maschine und den Betrieb an sich.

Integratoren (Integration Service Provider): Integratoren setzen verschiedene Komponenten und Produkte zu einem oder mehreren Systemen zusammen und sorgen dafür, dass das Gesamtsystem mit den einzelnen Komponenten funktioniert [28]. Integratoren können Maschinen- und Anlagenbauer sein, aber auch Hersteller von Produkten, wenn diese wiederum kleinere Teilkomponenten zusammenbauen.

Produkt-Hersteller (Product Supplier): Produkt-Hersteller sind für das Produktdesign, die Produktentwicklung, sowie die Herstellung verantwortlich [29]. Ihre Produkte werden von Integratoren in Systemen implementiert. Der Hersteller ist dafür verantwortlich, dass Produkte über den gesamten Lebenszyklus ihre Funktionalität beibehalten und rechtzeitig Patches zur Verfügung stellen, um bekanntgewordene Sicherheitslücken zu schließen.

Service-Provider (Maintenance Service Provider): Service-Provider sind Dienstleister, welche die Systeme optimieren oder warten [28]. Eine mögliche Dienstleistung könnte beispielsweise das Aufspüren von Sicherheitslücken im System sein (Pen-Testing) oder das Schließen von bekannten Sicherheitslücken (Patchen, Maschinenwartung). Auch das Optimieren von Systemen, wie zum Beispiel Predictive Maintenance oder Prozessoptimierungen mit künstlicher Intelligenz, fallen unter den Anwendungsbereich der Service-Provider.

Aufgaben und Beziehungen der Akteure:

In der Norm sind die Zuständigkeiten und Aufgaben der verschiedenen Akteure klar definiert. Ebenso wird beschrieben, welcher Akteur welche Verantwortlichkeit zu welchem Lebenszyklusprozess besitzt. Die Aufgabenverteilung in Bezug auf IACS ist in Bild 3 dargestellt.

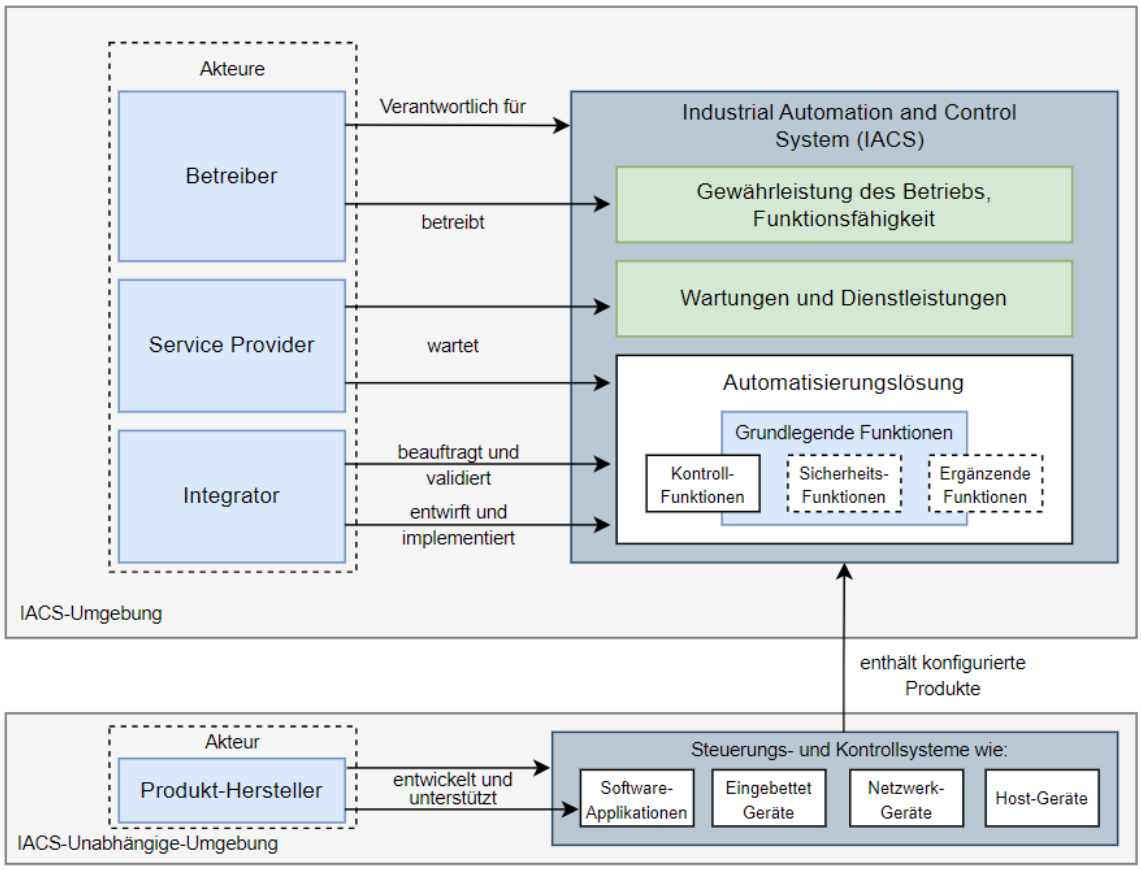


Bild 3: Aufgaben der Akteure in Bezug auf IACS

Quelle: Eigene Darstellung nach IEC-62443-2-4 [30, p. 11]

Die verschiedenen Verantwortlichkeiten der Akteure in Bezug auf den Lebenszyklusprozess eines IACS ist in Anhang 1 aufgezeigt. Zusätzlich werden die entsprechenden greifenden Normen des ausgewählten Prozesses aufgezeigt. In der Norm werden drei Verantwortlichkeiten unterschieden, welche im Englischen mit Accountable, Responsible und Contributor deklariert werden. Der Contributor ist als Mitwirkender zu übersetzen. Dieser hat keine direkte Verantwortung, muss jedoch mitwirken und ist maßgeblich am Prozess beteiligt.

Schwieriger ist die Übersetzung von Accountable und Responsible, da beides im Deutschen mit „Verantwortlich“ übersetzt wird. Die Norm grenzt die „Verantwortlichkeiten“ aber wie folgt voneinander ab:

Accountable: Gilt ein Akteur als Accountable, so ist dieser Hauptverantwortlich für den Prozess. Bei Fehlern wird dieser Verantwortliche entsprechend belangt. Er übernimmt die Führung des Prozesses und muss gewährleisten, dass alle Schritte und Vorgaben eingehalten werden.

Responsible: Gilt ein Akteur als Responsible, so ist dieser für die Durchführung des Prozesses verantwortlich. Alle Maßnahmen und Umsetzungen werden von ihm getrieben. Er wird dabei streng vom hauptverantwortlichen Akteur überwacht und muss diesem kontinuierliche Rückmeldungen über die Umsetzung der Prozesse geben.

In Anhang 1 ist zusehen, dass der Betreiber über den kompletten Lebenszyklus hinweg Accountable ist. Dies ist auch naheliegend, da dieser die Maschine mit seinen Vorstellungen, Rahmenbedingungen und Spezifikationen in Auftrag gibt. Nach Fertigstellung der Maschine wird diese beim Betreiber betrieben und in sein Netzwerk eingepflegt.

2.3.2 Kernprinzipien der IEC-62443

Die Norm definiert verschiedene Kernprinzipien, welche bekannt sein sollten. Diese sollen dabei helfen, die Implementierung mit einem dennoch hohen Sicherheitsziel in der Praxis einfacher zu gestalten.

Foundational Requirements (FRs):

Die CIA-Triade (Confidentiality, Integrity, Availability) ist nicht ausreichend, um die verschiedenen Anforderungen der IACS abzufangen. Daher beschreibt die IEC-62443-1-1 [27] sogenannte fundamentale Anforderungen (Foundational Requirements – kurz: FR). Die FRs bestehen dabei aus dem Access Control, Use Control, Data Integrity, Data Confidentiality, Restrict Data Flow, Timely Response to Event und Resource Availability. Die fundamentalen Anforderungen gilt es zu erfüllen, um ein System sicher gestalten zu können.

Defense in Depth:

Defense in Depth, zu Deutsch „Verteidigung in der Tiefe“, beschreibt einen Kernaspekt der IEC-62443. Dabei handelt es sich um eine Sicherheitsarchitektur nach dem „Zwiebelschalenmodell“. Viele verschiedene Sicherheitsmaßnahmen sollen dabei den Erfolg eines Angriffs erschweren und die Motivation des Angreifers beeinträchtigen. Dabei sind mehrere „kleinere“ Sicherheitsmaßnahmen effektiver als eine „große“ Sicherheitsmaßnahme. Die verschiedenen Sicherheitsmaßnahmen sollten dabei verschiedene Charakteristiken besitzen und sowohl technischer als auch organisatorischer Natur sein [27]. Das Prinzip von Defense in Depth ist in Bild 4 zusehen.

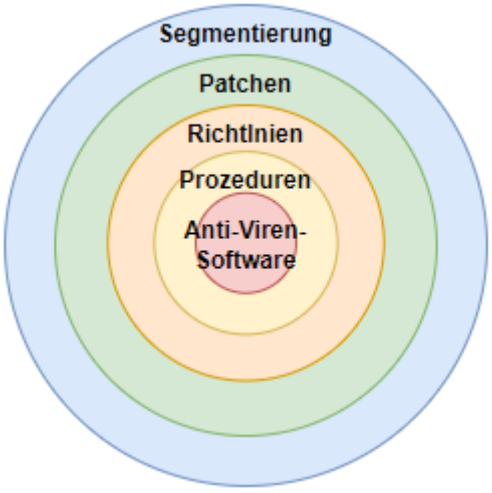


Bild 4: Prinzip von Defense in Depth

Quelle: Eigene Darstellung

Bei Defense in Depth sollte man abwägen, wie „teuer“ und „effizient“ verschiedene Sicherheitsmaßnahmen sind und wie groß der Aufwand der Implementierung ist. Zudem kann niemals eine hundertprozentige Sicherheit gewährleistet werden, weshalb hier nach dem „optimalen Maß“ der Implementierung gestrebt werden sollte, bei dem die Kosten nicht zu hoch, das Sicherheitsniveau aber auch nicht zu gering ist. Zusätzlich beschreibt das Pareto-Prinzip, dass 80% des Ergebnisses mit 20% des Gesamtaufwands erreicht werden kann. Heißt mit einer Implementierung von 20% der

Sicherheitsmaßnahmen wird bereits ein Sicherheitsniveau von 80% erreicht [5]. Das daraus resultierende Diagramm ist in Bild 5 zusehen.

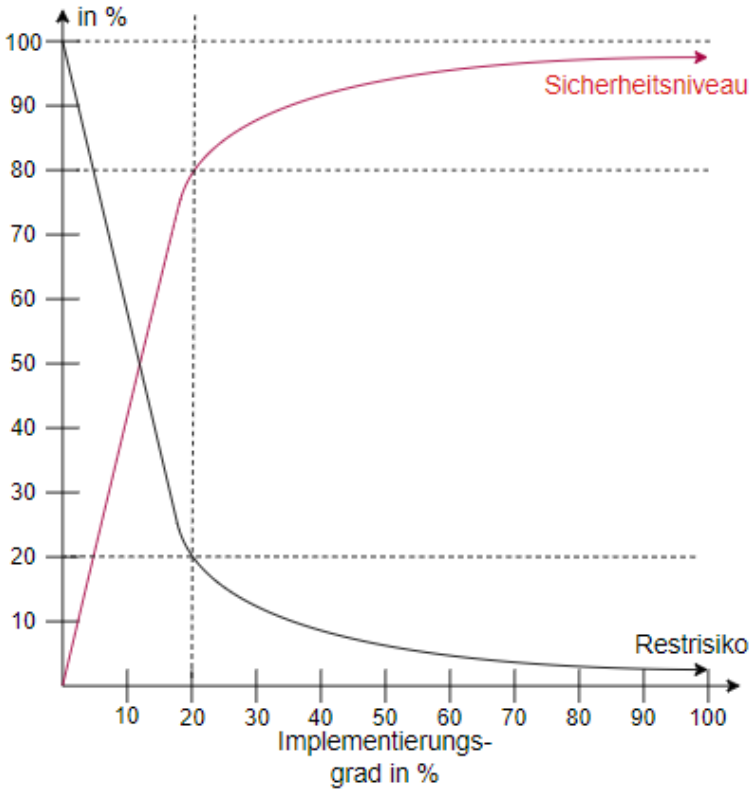


Bild 5: Pareto-Prinzip der Cyber-Security

Quelle: Eigene Darstellung nach [5, p. 49]

Zones & Conduits:

Zones & Conduits, also Zonen und Kanäle, beschreibt ein weiteren Kernaspekt bei dem Automatisierungssysteme in Zonen aufgeteilt werden. Die Aufteilung der Zonen kann dabei physikalisch oder logisch geschehen. Verbindungskanäle zwischen den Zonen werden Conduits genannt. Diese können ebenfalls physikalisch, durch beispielsweise Firewalls, Router oder VLANs oder logisch, durch zum Beispiel Access Control Lists, Policies oder definierten Kommunikationsbeziehungen realisiert werden [27].

Innerhalb einer Zone werden allen Geräten die Sicherheitsanforderungen der Zone zugeteilt. Dies spart Administrationsaufwand, da nicht jedes Gerät einzeln bewertet werden muss, sondern lediglich in die entsprechende Zone zugeteilt wird und dementsprechend passende Maßnahmen anhand einer Risikoanalyse

abgeleitet werden können.

Die Norm beschreibt erforderliche und empfehlenswerte Einteilungen der Zonen, diese lauten wie folgt:

Erforderliche Zonen [31]:

- IT-Netz / Business-Netzwerk
- OT-Netz / Produktions-Netzwerk
- Safety-Systeme / Sicherheitsrelevante-Netzwerke

Empfehlenswerte Zonen:

- Temporäre-Geräte / Portable Geräte (Laptops, USB-Sticks, Festplatten)
- Kabellose- / Funkgeräte (Mobile-Devices, WiFi-Geräte, 5G-Geräte)
- Externe-Netzwerke (weitere Unternehmensstandorte, Internetverbindungen, Fernwartungszugriffe)

Bei Conduits ist es wichtig, genau zu definieren, welcher Teilnehmer mit welchem Kommunikationspartner über welche Zonengrenzen hinaus kommuniziert, über welches Protokoll, welchen Dienst und im Bestfall auch in welchem Kommunikationszyklus mit welcher Datenmenge. Darüber erhält man eine genau Übersicht über die im Netzwerk vorhandenen Kommunikationsbeziehungen, wodurch sich Anomalien (Abweichungen des definierten „Normalzustandes“) leichter detektieren lassen.

Security Level (SL):

Security Levels bewerten wie Robust IACS gegenüber verschiedenen Angreiferklassen sind. Die Norm definiert in Teil 1-1 [27] 5 unterschiedliche Level, welche nachfolgend vorgestellt werden:

- SL 0: Keine spezifischen Anforderungen oder Sicherheitsmaßnahmen erforderlich
- SL 1: Schutz vor unbeabsichtigtem oder zufälligem Missbrauch
- SL 2: Schutz vor vorsätzlichem Missbrauch mit einfachen Mitteln mit geringen Ressourcen, allgemeinen Fähigkeiten und geringer Motivation

- SL 3: Schutz vor vorsätzlichem Missbrauch mit anspruchsvollen Mitteln mit moderaten Ressourcen, IACS-spezifischen Kenntnissen und moderater Motivation
- SL 4: Schutz vor vorsätzlichem Missbrauch unter Einsatz anspruchsvoller Mittel mit umfangreichen Ressourcen, IACS-spezifischen Kenntnissen und hoher Motivation

Wird ein System mit SL 3 bewertet, kann man davon ausgehen, dass es ein Schutz vor vorsätzlichem Missbrauch mit anspruchsvollen Mitteln mit moderaten Ressourcen, IACS-spezifischen Kenntnissen und moderater Motivation bietet. Um dieses System zu kompromittieren, würde man also mindestens den Einsatz von anspruchsvollen Mitteln mit umfangreichen Ressourcen, IACS-spezifischen Kenntnissen und einer hohen Motivation (SL 4) voraussetzen.

Die SLs werden durch die Implementierung von verschiedenen Systemanforderungen (System Requirements) erreicht. Für Systeme findet man die benötigten Systemanforderungen der verschiedenen SLs in der IEC-62443-3-3 [28], die Anforderungen an Produkte hingegen in der IEC-62443-4-2 [30].

Die Norm [27] definiert außerdem drei verschiedene Kategorien von Security Levels, welche nachfolgend kurz erläutert werden.

Security Level Target (SL-T): Das Security Level Target ist das Security Level, welches in einem System erreicht werden soll. Es bildet somit das Ziel-SL, welches es anzustreben gilt und solang Sicherheitsmaßnahmen zu implementieren, bis diese dem Wert des SL-Ts entsprechen.

Security Level Achieved (SL-A): Das Security Level Achieved ist das Security Level, welches ein System tatsächlich zu einem betrachteten Zeitpunkt mit all seinen Sicherheitsmaßnahmen erreicht.

Security Level Capability (SL-C): Das Security Level Capability ist das Security Level, welches ein System maximal mit allen implementierten Sicherheitsmaßnahmen erreichen kann. Dies ist vor Allem bei Produkten wichtig um zusehen welches Security Level mit diesem Produkt maximal möglich wäre.

Cyber Security Management System (CSMS):

Ein Cyber Security Management System dient dazu die Cyber Security in einem Unternehmen anhand von Regeln und Verfahren sicherzustellen, zu steuern, zu kontrollieren und kontinuierlich zu verbessern [31]. Daher ist ein CSMS hauptsächlich an Betreiber von Maschinen und Anlagen, sowie die interne IT der Maschinenbauer gerichtet. Maschinenbauer können ihren Kunden kein CSMS bereitstellen. Ein CSMS besteht dabei aus den in Bild 6 gezeigten Elementen.

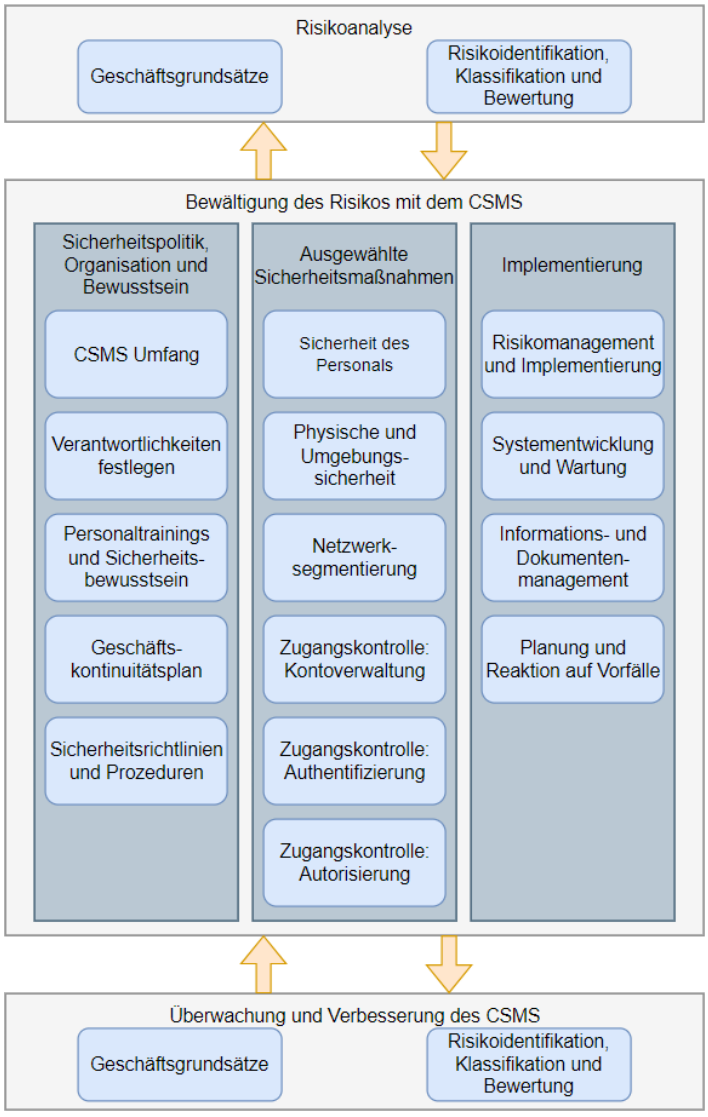


Bild 6: Kernkonzepte eines CSMS

Quelle: Eigene Darstellung nach IEC-62443-2-1 [31, p. 23]

3 Anforderungsanalysen

3.1 Rechtliche Anforderungen an Maschinenbauer

Die Analyse der rechtlichen Anforderungen betrachtet nur jene Artikel, welche den Maschinenbauer tatsächlich betreffen und aus denen konkrete Pflichten für den Maschinenbauer hervorgehen. Diese Pflichten wurden in zwei Kategorien aufgeteilt, den Handlungspflichten, bei denen der Maschinenbauer aktiv Maßnahmen treffen muss, und den Kommunikationspflichten, bei denen der Maschinenbauer gewisse Informationen weitergeben, bereithalten oder bereitstellen muss. Hierbei ist anzumerken, dass das NIS2UmsuCG hauptsächlich die IT des Maschinenbauers adressiert, während der CRA und die MVO die OT des Maschinenbauers in die Verantwortung nimmt. Für diese Arbeit ist daher vor Allem der CRA und die MVO von großer Bedeutung. Zur Vollständigkeit werden allerdings die Inhalte des NIS2UmsuCG ebenfalls analysiert, da aus dieser indirekte Anforderungen an die OT entstehen. Die Kunden-IT kann nämlich aufgrund der Anforderungen des NIS2UmsuCG direkte Anforderungen an die OT des Maschinenbauers stellen, wodurch der Maschinenbauer hier ebenfalls tätig werden muss.

3.1.1 Kommunikationspflichten

Innerhalb der Kommunikationspflichten wurde eine weitere Untergliederung unternommen. Aus diesen Untergliederungen wird bereits der Kern der Pflicht ersichtlich. Diese sollen nachfolgend knapp erläutert werden.

Kennungspflicht:

In Anhang 3 Teil B Absatz 1.1.9. der MVO wird eine Kennungspflicht beschrieben. Diese gilt für installierte Softwares der Maschine bzw. dazugehörigen Produkten, welche für den sicheren Betrieb erforderlich ist. Diese Softwares müssen kenntlich gemacht und Informationen jederzeit in leicht zugänglicher Form bereitgestellt werden.

Unterrichtungspflichten:

Im Falle eines erheblichen Sicherheitsvorfalls kann das BSI anordnen, dass der Maschinenbauer seine Kunden über diesen erheblichen Sicherheitsvorfall unterrichten muss. Dies geht aus § 35 Abs. 1 NIS2UmsuCG hervor. Des Weiteren kann das BSI die zuständige Aufsichtsbehörde in Kenntnis setzen. Die Unterrichtung zum Sicherheitsvorfall kann durch eine Veröffentlichung auf der Internetseite erfolgen.

§ 10 Abs. 14 CRA besagt zusätzlich, dass ein Maschinenbauer die Marktüberwachungsbehörde, sowie mit allen verfügbaren Mitteln und soweit möglich die Nutzer der in Verkehr gebrachten Produkte mit digitalen Elementen darüber unterrichten muss, wenn Dieser seine Betriebstätigkeit einstellt und infolgedessen nicht in der Lage ist, die festgelegten Pflichten aus dem CRA zu erfüllen.

Meldepflichten:

Aus dem NIS2UmsuCG gehen aus dem § 32 Abs. 1 und 2, sowie § 40 Abs. 1, Meldepflichten hervor. Die Meldestelle, an welche die Meldungen gemeldet werden müssen, ist das BSI. Meldungen müssen dabei nach einem erheblichen Sicherheitsvorfall erstellt werden. Dabei gelten folgende zeitliche Rahmen:

- Unverzüglich / spätestens innerhalb von 24 Stunden nach Kenntniserlangung des erheblichen Sicherheitsvorfalls: frühe Erstmeldung des Sicherheitsvorfalls mit Angabe, ob der Verdacht auf eine rechtswidrige oder böswillige Handlung zurückzuführen ist und/oder dieser grenzüberschreitende Auswirkungen haben könnte.
- Unverzüglich / spätestens innerhalb von 72 Stunden nach Kenntniserlangung des erheblichen Sicherheitsvorfalls: Meldung mit Bestätigung oder Aktualisierung des Verdachts aus Nummer 1, sowie weiteren Informationen wie Bewertung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkung, sowie gegebenenfalls die Angabe der Kompromittierungsindikatoren.

- Auf Ersuchen des BSI eine Zwischenmeldung über relevante Statusaktualisierungen.
- Spätestens ein Monat nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Nummer 2, vorbehaltlich Absatz 2, eine Abschlussmeldung mit folgendem Inhalt: ausführliche Beschreibung des Sicherheitsvorfalls einschließlich seines Schweregrads und seiner Auswirkungen, sowie Angaben zur Art der Bedrohung, beziehungsweise zugrunde liegende Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat, Angaben zu den getroffenen und laufenden Abhilfemaßnahmen und gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls.

Dauert der Sicherheitsvorfall länger als den in Punkt 4 genannten Zeitpunkt an, so ist, anstatt einer Abschlussmeldung eine Fortschrittsmeldung vorzulegen, welche dieselben Informationen enthält. Spätestens ein Monat nach Abschluss der Bearbeitung des Sicherheitsvorfall muss eine Abschlussmeldung vorgelegt werden.

Die Meldepflicht aus dem NIS2UmsuCG bezieht sich dabei vor Allem auf eigene Systeme und liegt daher in der Verantwortung der IT. Für die Maschinen des Maschinenbauers gilt diese Pflicht nicht und wird daher nicht weiter beachtet.

Aus dem § 11 Abs. 1, 2, 4 und 7 CRA gehen weitere Meldepflichten für den Maschinenbauer hervor. Wenn das Produkt mit digitalen Elementen ein erhebliches Cybersicherheitsrisiko birgt oder Schwachstellen bekannt werden, muss der Maschinenbauer dies der ENISA unverzüglich mitteilen. Des Weiteren müssen die Kunden, welchen das Produkt verkauft wurde, über den Vorfall informiert werden und erforderlichenfalls über Korrekturmaßnahmen zur Minderung des Risikos aufgeklärt werden. Geht das Cybersicherheitsrisiko aus einer Komponente innerhalb des Produkts hervor, so muss die Einrichtung oder Person, die diese Komponente wartet, informiert werden. Dies gilt auch für Open-Source-Software.

Nachweispflichten:

Bei Zuwiderhandlung oder unzureichender Umsetzung der Anforderungen aus § 30 Abs. 1 Satz 1, § 32 Abs. 1 bis 3 und § 38 Abs. 3 NIS2UmsuCG, kann das BSI gemäß § 62 NIS2UmsuCG weitere Maßnahmen nach § 61 NIS2UmsuCG treffen, darunter die Verlangung umfangreicher Nachweise der Umsetzungen des NIS2UmsuCG im Unternehmen.

Der CRA definiert umfangreiche Nachweispflichten in § 10 Abs. 3, 5, 7, 8, 9, 10, 11 und 13 CRA sowie § 17 Abs. 1 und Abs. 2 CRA. Zu den Maschinen müssen Cyber Security Risikobewertungen durchgeführt werden. Diese müssen aktuell gehalten werden und, im Falle eines Sicherheitsvorfalls oder einer Schwachstelle, überarbeitet werden. Diese Risikobewertung muss der allgemeinen technischen Dokumentation beiliegen. Die Maschine muss durch Konformitätsbewertungsverfahren bewertet werden, wobei ein Teil der Bewertung, das Vorhandensein der Risikobewertung prüfen muss. Diese gesamten Dokumentationen müssen pro Maschine bis zehn Jahre nach Inverkehrbringen gespeichert werden. Bei Serienmaschinen muss nachgewiesen werden können, dass Abweichungen vom Standard berücksichtigt und neubewertet wurden. Jegliche Dokumentationen müssen als Nachweis der Maschine beigelegt werden oder über eine Website erreichbar sein. Diese Dokumentationen müssen dabei in leicht verständlicher Sprache vorliegen. Zu den Dokumentationen zählen auch die Konformitätsbewertungen. Auf Anfrage müssen alle Dokumente und Konformitätsbewertungen, dem BSI nachgewiesen werden.

Auf Anfrage des BSI übermittelt der Maschinenbauer zudem folgenden Informationen, sofern diese verfügbar sind:

- Name und Anschrift aller Wirtschaftsakteure, von denen sie Produkte mit digitalen Elementen bezogen haben,
- Name und Anschrift aller Wirtschaftsakteure, an die sie Produkte mit digitalen Elementen abgegeben haben.

Diese Informationen müssen vom Maschinenbauer zehn Jahre nach dem Bezug eines Produkts mit digitalen Elementen (Maschinenkomponente), sowie zehn Jahre nach Abgabe des Produkts mit digitalen Elementen (Maschine an sich), vorgelegt werden können.

Gemäß Anhang 3 Teil B Absatz 1.2.1. der MVO, gilt die Nachweispflicht ebenso für Rückverfolgungsprotokolle der Daten, die im Zusammenhang mit einem Eingreifen in die Maschine generiert wurden und der Versionen der Sicherheitssoftware, die nach Inverkehrbringen oder der Inbetriebnahme der Maschine hochgeladen wurden. Diese Informationen müssen bis 5 Jahre nach dem Hochladen, ausschließlich zum Nachweis der Konformität der Maschine oder des dazugehörigen Produkts auf begründete Anforderungen des BSI, zugänglich sein.

3.1.2 Handlungspflichten

Die Handlungspflichten werden ebenfalls weiter untergliedert, um ein genaueres Augenmerk auf die tatsächlichen Pflichten der Maschinenbauer zulegen, welche nachfolgend erläutert werden.

Prüfungspflichten:

Der Maschinenbauer muss, gemäß § 10 Abs. 4 CRA, Komponenten von Dritten, welche in das eigene Produkt integriert werden sollen, auf die Cybersicherheitsrisiken prüfen. Die Sicherheit der Maschine darf durch solche Komponenten nicht beeinträchtigt werden. Dazu dient unter anderem die Prüfung der Konformitätsbewertungen.

Korrekturpflicht:

Der Maschinenbauer muss über die erwartete Produktlebensdauer oder während eines Zeitraums von fünf Jahren ab dem Inverkehrbringen (je nachdem, welcher Zeitraum kürzer ist), Schwachstellen des Produkts wirksam und im Einklang mit den grundlegenden Anforderungen in Anhang 1 Abschnitt 2 behandeln. Dies geht aus § 10 Abs. 6 CRA hervor. Darauf aufsetzend muss der Maschinenbauer, gemäß § 10 Abs. 12 CRA, Korrekturmaßnahmen ergreifen, wenn das Produkt

oder festgelegte Verfahren des Maschinenbauers, den grundlegenden Anforderungen aus Anhang 1 nicht genügen. Kann die Konformität nichtmehr hergestellt werden, muss der Maschinenbauer das Produkt vom Markt nehmen oder zurückrufen.

Kooperationspflichten:

Gemäß § 62 NIS2UmsuCG kann das BSI den Maschinenbauer zur Kooperation verpflichten und anordnen, dass dieser Maßnahmen nach § 61 NIS2UmsuCG ergreifen muss. Dies ist aber nur der Fall, wenn Tatsachen die Annahme rechtfertigen, dass der Maschinenbauer die Anforderungen aus den §§ 30, 32 und 38 NIS2UmsuCG nicht oder nicht richtig, im eigenen Netzwerk, umsetzt.

Auf begründetes Verlangen des BSI ist der Maschinenbauer gemäß § 10 Abs. 13 CRA dazu verpflichtet, dem BSI alle Informationen und Unterlagen, die für den Nachweis der Konformität der Maschine dienen, in leichter Sprache, in elektronischer Form oder Papierform zukommen zu lassen. Auf Verlangen des BSI muss mit diesen bei allen Maßnahmen zur Abwendung der Cybersicherheitsrisiken, die mit dem vom Maschinenbauer in Verkehr gebrachten Produkt steht, zusammengearbeitet werden.

Schulungspflichten:

Der § 38 Abs. 3 NIS2UmsuCG schreibt vor, dass Geschäftsleitungen regelmäßig an Schulungen teilnehmen müssen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken, sowie Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik und die Auswirkungen von Risiken, ebenso wie Risikomanagementpraktiken auf die vom Maschinenbauer erbrachten Dienste, zu erwerben.

Für die Belegschaft geht die Schulungspflicht aus § 30 Abs. 2 NIS2UmsuCG hervor, indem beschrieben wird, dass Maßnahmen nach § 30 Abs. 1 NIS2UmsuCG den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und auf einem gefahrenübergreifenden Ansatz beruhen sollen. Die Maßnahmen müssen verschiedene Bereiche umfassen, auf die später näher eingegangen wird. Ein

Bereich beschreibt, dass grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik vorhanden sein sollten.

Dies betrifft vorerst nur die Belegschaft des Unternehmens und liegt daher im Verantwortungsbereich der IT als auch der IT des Betreibers. Der Maschinenbauer ist nicht verpflichtet die Belegschaft seines Kunden für die entsprechende verkaufte Maschine zu schulen.

Umsetzungspflichten:

Die umfangreichsten Pflichten ergeben sich aus den Umsetzungspflichten. Hier stellt der Gesetzgeber verschiedene Paragrafen mit konkreten Maßnahmen bereit. Für die IT sind dieser vor allem in § 30 Abs. 1 und 2 NIS2UmsuCG zu finden. Aus § 61 i.V.m. § 62 NIS2UmsuCG könne zudem weitere Maßnahmen vom BSI angeordnet werden, welche verpflichtend umgesetzt werden müssen. Auf diese Pflichten wird nicht näher eingegangen.

Die für die OT bedeutenden Umsetzungspflichten finden sich im CRA und in der MVO. § 10 Abs. 1 CRA besagt dabei, dass der Hersteller eines Produkts mit digitalen Elementen, vor in Verkehr bringen, gewährleisten muss, dass das Produkt gemäß den grundlegenden Anforderungen in Anhang 1 Abschnitt 1 konzipiert, entwickelt und hergestellt worden ist. Weiter heißt es in § 10 Abs. 2 CRA, dass für die Zwecke der Erfüllung der in § 10 Abs. 1 CRA festgelegten Pflichten eine Bewertung der Cybersicherheitsrisiken durchgeführt werden muss.

Die in Anhang 1 Abschnitt 1 aufgelisteten Anforderungen lauten dabei wie folgt:

- Produkte werden so konzipiert, entwickelt und hergestellt, dass sie angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten;
- Produkte werden ohne bekannte ausnutzbare Schwachstellen ausgeliefert;
- Auf der Grundlage der Risikobewertung müssen Produkte gewisse Anforderungen erfüllen, diese sind in Anhang 2 dieser Arbeit zu finden.

§ 10 Abs. 6 CRA setzt zudem voraus, dass der Maschinenbauer geeignete Strategien und Verfahren zur Schwachstellenmeldung und -behandlung etablieren muss.

Aus Anhang 3 Teil B Absatz 1.1.9. der MVO werden weitere Umsetzungspflichten konkret. Unter anderem die folgenden Punkte:

- Fernwartungszugriffe dürfen nicht zu einer gefährlichen Situation führen
- Konstruktion der Maschine muss vor unbeabsichtigtem oder vorsätzlichem Missbrauch schützen
- Logging der Sicherheitsfunktionen sowohl rechtmäßiger als auch unrechtmäßiger Eingriffe
- Software und Daten müssen dokumentiert und vor unbeabsichtigtem oder vorsätzlichem Missbrauch geschützt werden
- Jegliche Eingriffe in die Software oder Veränderungen an der Maschine sowohl unbeabsichtigt als auch beabsichtigt müssen nachgewiesen werden

In Anhang 3 Teil B Absatz 1.2.1. der MVO kommen folgende hinzu:

- Steuerungen müssen so ausgelegt und beschaffen sein, dass:
    - Sie durch unbeabsichtigte oder beabsichtigte Fremdeinflüsse, auch die vernünftigerweise vorhersehbaren böswilligen Versuche Dritter standhalten können und nicht zu Gefährdungssituationen führen
    - Ein Defekt der Hard- oder Software nicht zu Gefährdungssituationen führt
    - Keine Änderungen durch die Maschine, des dazugehörigen Produkts oder den Bediener generierten Einstellungen oder Regeln durchgeführt werden dürfen, wenn solche Änderungen zur Gefährdungssituation führen
- Die Maschine oder das dazugehörige Produkt darf nicht unbeabsichtigt in Gang gesetzt werden können
- Die Parameter der Maschine oder des dazugehörigen Produkts dürfen sich nicht unkontrolliert ändern lassen, wenn derartige Änderungen zu Gefährdungssituationen führen können

- Bei kabelloser Steuerung darf ein Ausfall der Kommunikation, Verbindung oder eine fehlerhafte Verbindung nicht zu einer Gefährdungssituation führen

Die Anforderungen sind in den Regulatorien sehr allgemein gehalten, dennoch schärfer und genauer als in den bisher regulierenden Gesetzen. Der Bezug auf die einschlägigen nationalen und europäischen Normen bezieht sich dabei auf die IEC-62443, welche in den Regulatorien als aktueller Stand der Technik definiert ist. Aufgrund dessen müssen die Anforderungen der IEC-62443-3-3 im nachfolgenden Kapitel 3.2 genauer analysiert werden.

3.2 Normative Anforderungen an Maschinenbauer

Die Analyse der System Requirements wäre mit 50 System Requirements aus der IEC-62443-3-3 bereits sehr umfangreich und würde die Übersichtlichkeit des Dokuments sprengen. Zu den 50 SRs würden zusätzlich 49 Requirements Enhancements (RE) hinzukommen. Die IEC-62443-3-3 verlangt die Erfüllung von 99 Anforderungen, um das höchste Security Level für Systeme zu erreichen. Eine enorme Aufgabe für all diejenigen, die das höchste Security Level erreichen wollen. Der Fokus auf dem allgemeinen Maschinenbau in dieser Arbeit reduziert die Anforderungen, wodurch ein Security Level von 2 anzustreben gilt.

Zur Erreichung des zweiten Security Levels werden 60 SRs und REs benötigt. Welche SRs und REs dabei berücksichtigt werden müssen, wird anhand einer Einordnung in Gruppen dargestellt, welche aus der IEC-62443-3-3 erarbeitet wurde [28].

3.2.1 Identifikationsmanagement

Das Identifikationsmanagement verfolgt das Ziel, alle Benutzer zu identifizieren und zu authentifizieren. Dabei betrifft dies sowohl alle Menschlichen (SR 1.1), als auch alle Softwareprozesse und Geräte (SR 1.2). Die menschlichen Nutzer müssen zudem eindeutig identifiziert werden (SR 1.1 RE 1).

3.2.2 Accountmanagement

Das Accountmanagement beschreibt, dass Benutzeraccounts verwaltbar sein müssen (SR 1.3). Die Identifikatoren des Systems müssen diese Accountverwaltung unterstützen (SR 1.4). Alle Authentifikatoren, welche Benutzer authentifizieren, müssen zudem bestimmte Rahmenbedingungen erfüllen (SR 1.5). Werden Passwörter zur Authentifizierung verwendet, müssen diese eine gewisse Stärke vorweisen (SR 1.7). Werden zur Authentifizierung Zertifikate verwendet, müssen diese, nach dem Stand der Technik, mit PKIs realisiert werden (SR 1.8 und SR 1.9). Bei jedem Anmeldeversuch muss der Authentifikator in der Lage sein, eine Rückmeldung zum Anmeldeversuch zu geben (SR 1.10) und nach einer definierten Zahl von gescheiterten Anmeldeversuchen, diesen Account temporär sperren (SR 1.11). Das Accountmanagement muss in der Lage sein, Benutzer zu bestimmten Rollen mit entsprechenden Rechten zuzuordnen und diese auch durchzusetzen, unabhängig davon, ob der Benutzer menschlich, ein Softwareprozess oder ein Gerät ist (SR 2.1, SR 2.1 RE 1 und SR 2.1 RE 2).

3.2.3 Drahtlose Kommunikation

Bei der drahtlosen Kommunikation muss beachtet werden, dass alle beteiligten Benutzer ebenfalls eindeutig identifiziert und authentifiziert werden. Die Eindeutigkeit bezieht sich bei drahtlosen Kommunikationsteilnehmern sowohl auf Menschen als auch Softwareprozessen und Geräten (SR 1.6 und SR 1.6 RE 1). Die Berechtigungen der Nutzer für drahtlose Kommunikation müssen dabei dem allgemeinen Accountmanagement entsprechen (SR 2.2).

3.2.4 Netzwerkmanagement

Beim Netzwerkmanagement muss darauf geachtet werden, dass alle Zugriffe von nicht-vertrauenswürdigen Netzen überwacht und kontrolliert werden (SR 1.13) und diese ablehnen, soweit diese nicht von einer zugewiesenen Rolle explizit genehmigt wurden (SR 1.13 RE 1). Fernwartungszugriffe müssen zudem nach einer konfigurierten Zeit der Inaktivität oder durch den Nutzer, der die

Verbindung einleitet, beendet werden (SR 2.6). Das Netzwerk muss logisch segmentiert werden. Die Segmentierung muss zwischen Kontrollsystemen und Nicht-Kontrollsystemen, sowie kritischen Kontrollsystemen (unter Anderem Safety-Relevante Systeme) und nicht-kritischen Kontrollsystemen, stattfinden (SR 5.1). Diese Segmentierung muss sowohl logisch als auch physikalisch geschehen (SR 5.1 RE 1). Die Zonengrenzen der Segmentierungen müssen überwacht und kontrolliert werden (SR 5.2), dabei den gesamten Netzwerkverkehr per Standardeinstellung unterbinden und nur explizit erlaubte Verbindungen durchlassen (SR 5.2 RE 1). Des Weiteren muss jegliche Mensch-zu-Mensch-Kommunikation über die Zonengrenzen hinaus unterbunden werden (SR 5.3). Die Netzwerkkomponenten der Systeme müssen nach vorhandenen Sicherheitsrichtlinien des Komponentenherstellers konfiguriert werden und eine Schnittstelle speziell zur Konfiguration bereitstellen (SR 7.6). Bei Konfigurationen, die das Netzwerk betreffen, muss immer die geringste Funktionalität beachtet werden (SR 7.7). Darunter zählt die Abschaltung von ungenutzten Ports, Diensten und Protokollen.

3.2.5 Auditierungsmanagement

Für das Auditierungsmanagement müssen verschiedene Ereignisse aufgezeichnet und protokolliert werden. Diese Ereignisse sind sehr umfassend und in SR 2.8 zu finden. Die Speicherkapazität dieser Protokolle muss ausreichend sein und frühzeitig eine Meldung senden, wenn der Speicherplatz knapp wird (SR 2.9). Bei Fehlern der Auditierung oder bei Verlust wesentlicher Dienste und Funktionen, muss eine Meldung an das zuständige Personal gesendet werden und automatisch geeignete Maßnahmen nach anerkannten Branchenpraktiken und -empfehlungen unterstützen (SR 2.10). Für alle Protokolle und Ereignisse müssen legitime Zeitstempel hinzugefügt werden (SR 2.11). Unautorisierter Zugriff auf gespeicherte Software und Informationen muss protokolliert werden (SR 3.4). Alle Audit-Protokolle müssen vor unbefugten Zugriffen, Veränderungen und Löschungen geschützt werden (SR 3.9). Für autorisierte Benutzer dürfen die Audit-Protokolle nur über eine Nur-Lesenden-Zugriff zugänglich sein (SR 6.1). Die Auditierung muss kontinuierlich alle Sicherheitsmaßnahmen gemäß den akzeptierten Industriestandards

überwachen, Verstöße erkennen und melden (SR 6.2).

3.2.6 Sitzungsmanagement

Bevor Benutzer sich an einem System anmelden, muss das System eine Meldung zur Systemnutzung anzeigen. Diese Meldung muss von autorisiertem Personal konfigurierbar sein (SR 1.12). Sitzungen müssen nach einer konfigurierbaren Zeit der Inaktivität oder nach manueller Auslösung einer Sitzungssperre weitere Zugriffe verhindern. Diese Sitzungssperre muss so lange aktiv bleiben, bis der Benutzer der Sitzung oder ein anderer autorisierter Benutzer den Zugang unter Verwendung geeigneter Identifizierungs- und Authentifizierungsverfahren wiederherstellt (SR 2.5). Die Integrität der Sitzungen muss zudem gesichert werden und ungültige Sitzungs-IDs abgelehnt werden (SR 3.8).

3.2.7 Ressourcenmanagement

Daten, Applikationen und Dienste müssen anhand ihrer Kritikalität und nach einem geeigneten Zonenmodell partitioniert werden (SR 5.4). Die Systemressourcen verschiedener Geräte und Dienste müssen auf Denial-of-Service-Angriffe vorbereitet sein und unter einem solchen Angriff weiterhin in einem gewissen Grad erreichbar sein (SR 7.1). Die Netzwerkgeräte müssen zudem den Netzwerkverkehr bei einem Denial-of-Service so verwalten, dass es nicht zu Ausfällen ganzer Kommunikationskanäle kommt (SR 7.1 RE 1). Auch unter normalen Umständen müssen Systemressourcen so verwaltet werden, dass es nicht zu Systemabstürzen durch mangelnde Ressourcen kommt (SR 7.2). Alle Ressourcen, Software, Hardware und Versionsstände müssen in Verbindung mit ihrer Nutzung und Eigenschaften dokumentiert werden (SR 7.8).

3.2.8 Kommunikationssicherheit

Innerhalb des Systems müssen alle Kommunikationskanäle die Integrität der übertragenen Informationen schützen (SR 3.1). Die Vertraulichkeit der Informationen des Systems müssen ebenfalls geschützt sein, unabhängig ob die

Informationen gespeichert oder übertragen werden. Dies gilt besonders für schreibgeschützte Informationen (SR 4.1). Die Vertraulichkeit muss auch über nicht-vertrauenswürdige Netzwerke gewährleistet sein (SR 4.1 RE 1). Werden kryptografische Methoden zur Sicherung der Vertraulichkeit und Integrität verwendet, müssen diese dem Stand der Technik entsprechen (SR 4.3).

3.2.9 Systemsicherheit

Um die Sicherheit des Systems zu gewährleisten, muss unter anderem eine Nutzungskontrolle für tragbare und mobile Geräte, gemäß den etablierten Sicherheitsrichtlinien, eingeführt werden (SR 2.3). Für Mobile Code muss eine Nutzungsbeschränkung im System durchgesetzt werden, die verschiedene Rahmenbedingungen voraussetzt (SR 2.4). Das System muss Sicherheitsmechanismen zur Erkennung, Schutz, Meldung und Eindämmung von bösartigem Schadcode implementieren. Diese Sicherheitsmechanismen müssen patchbar sein (SR 3.2). Der Schutz vor bösartigem Schadcode muss an allen Ein- und Ausgängen zum System implementiert sein (SR 3.2 RE 1). Das System muss in der Lage sein, Verifizierungen von Sicherheitsfunktionalitäten zu unterstützen. Diese Verifizierung muss alle definierten Sicherheitsfunktionalitäten der IEC-62443-3-3 betreffen (SR 3.3). Das System muss alle Eingaben anhand ihrer Syntax und ihres Inhalts validieren, wenn diese Eingaben das Verhalten des Systems ändern können (SR 3.5). Das System muss bei einem Angriff in einen definierten sicheren Zustand verfallen (SR 3.6). Fehler des Systems müssen identifiziert und so behandelt werden, dass eine wirksame Behebung erfolgen kann. Die Behebung des Fehlers darf dabei keine Informationen an unbefugte Dritte weitergeben, welche für Angriffe auf das System genutzt werden könnten (SR 3.7). Bei Informationen, welche ausdrücklich Leseberechtigungen benötigen, muss das System in der Lage sein, diese Informationen aus allen Komponenten zu löschen (SR 4.2). Das System muss Backups zur Konfiguration bereitstellen. Zusätzlich müssen Backups den Benutzern des Systems, sowohl auf Systemebene als auch Nutzerebene, bereitstellen (SR 7.3). Der Mechanismus zur Backuperstellung muss verifiziert werden (SR 7.3 RE 1). Zudem muss das System in der Lage sein in einen definierten, sicheren Status, nach einem Fehler oder Ausfall wiederherstellbar zu sein (SR 7.4). Für Ausfälle der

Stromversorgung muss mit Notstromversorgungen für kritische Komponenten vorgesorgt werden (SR 7.5).

3.3 Prüfung der gesetzlichen Konformität der IEC-62443

In diesem Kapitel soll geprüft werden, ob und wie die IEC-62443 die regulatorischen Anforderungen erfüllen kann. Die Überprüfung bezieht sich dabei auf die in Kapitel 3.1 erarbeiteten Anforderungsgruppen.

3.3.1 Kennungspflicht

Die Kennungspflicht wird von der IEC-62443 anhand der Cyber Security Requirements Specification (CRS) erfüllt. Die CRS ist eine Spezifikation (bestehend aus mindestens einem Dokument), in welcher alle Informationen zum System und der Risikobewertung des Systems zusammengetragen werden. Eine fundamentale Information im CRS ist die Inventarisierungsliste über das System. Darin enthalten sind neben den verschiedenen Geräten auch die auf den Geräten installierte Software mit Versionsnummern. Die sicherheitsrelevante Software kann hierbei hervorgehoben und dadurch kenntlich gemacht werden.

3.3.2 Unterrichtungspflicht

Aus der IEC-62443 geht keine Praktik hervor, um die Unterrichtungspflichten aus den regulatorischen Anforderungen zu erfüllen. Diese müssen also anderweitig abgefangen werden, wie in Kapitel 5.5 ersichtlich.

3.3.3 Meldepflicht

Zu den Meldepflichten sind keine Maßnahmen in der IEC-62443 aufgeführt. Diese werden daher gesondert in Kapitel 5.5 behandelt. Grundsätzlich definiert die IEC-62443 mit der CRS die grundlegenden Informationen über ein System, die bei einer Meldung an das BSI entscheidend sein könnte. Ist die CRS gut geführt, kann das BSI daraus schon einen Großteil der benötigten Informationen herausnehmen.

3.3.4 Nachweispflicht

Wie bei der Meldepflicht bietet die IEC-62443 nicht die benötigten Informationen zur Erfüllung der Nachweispflicht. Jedoch gilt auch hier, dass die CRS einen Großteil der benötigten Informationen bereitstellt. Es werden allerdings weitere Dokumente benötigt, auf welche in Kapitel 5.5 näher eingegangen wird.

3.3.5 Prüfungspflicht

Eine Prüfungspflicht ist in der IEC-62443 zwischen Maschinenbauer und Produkt-Hersteller nicht vorgesehen. Es wird in der Norm davon ausgegangen, dass jeder Wirtschaftsakteur seine Pflichten erfüllt und gewissenhaft handelt. So stellt ein Produkthersteller alle benötigten Dokumente und Konformitätserklärungen korrekt und vollständig zur Verfügung. Die Gesetzgeber verlangen hier allerdings eine Kontrolle des Produktherstellers durch den Maschinenbauer. Wie dies umgesetzt wird, wird in Kapitel 5.5 näher betrachtet.

3.3.6 Korrekturpflicht

Die Korrekturpflichten werden über den IACS Security Lifecycle der IEC-62443-1-4 abgefangen. Dieser Teil der Norm ist allerdings noch in Entwicklung, weshalb noch keine konkreten Vorgaben daraus erarbeitet werden können. Doch auch im Security Level Lifecycle der IEC-62443-1-1 sind grundlegende Vorgaben zum Patchmanagement enthalten [32].

In dem Security Level Lifecycle werden Vorgaben zum Patchmanagement gemacht, wie bspw. verschiedene Vorgaben zum Testen von Firmware-Updates, bevor diese in der Produktion ausgerollt werden. Diese Patches müssen vom Produkthersteller bereitgestellt und anschließend getestet werden. Der Maschinenbauer muss bewerten, ob der Patch für die Produktionsumgebung zugelassen werden kann, während der Betreiber dafür ein geeignetes Zeitfenster bereitstellt.

Bei den Korrekturzeiten gibt es jedoch große Unterschiede zwischen den rechtlichen Anforderungen und den normativen Vorgaben. Rechtlich bezieht man

sich dabei auf die „unverzügliche“ Korrektur. Unverzüglich kann nach § 121 Absatz 1 Satz 1 BGB als „ohne schuldhaftes Zögern“ verstanden werden, gilt aber dennoch als unbestimmter Rechtsbegriff und muss daher je nach Umständen des Einzelfalls bewertet werden. Die Norm sieht für Korrekturmaßnahmen größere Zeiträume vor. Der Zeitraum hängt hier von der jeweiligen Risikobeurteilung des Unternehmens ab und ist daher variabel. In der Praxis haben sich dabei die Abstufungen in Tabelle 1 als sinnvoll erwiesen:

Tabelle 1: Best Practices Patch-Zeiträume in der Industrie [32]

Priorität	Installationszeitraum nach Veröffentlichung des Patches durch den Hersteller
Hoch	Innerhalb einer Woche
Mittel	Innerhalb drei Monate
Niedrig	Innerhalb zwei Jahre oder beim nächsten geplanten Wartungsfenster
Keine	Nie

3.3.7 Rückrufpflicht

In der IEC-62443 sind keine Praktiken bezüglich einer Rückrufpflicht oder eines Zurückrufvorgangs dokumentiert. Lediglich die Korrektur von Systemen wird berücksichtigt. Für den Rückrufvorgang werden daher gesonderte Informationen in Kapitel 5.5 bereitgestellt.

3.3.8 Kooperationspflicht

Die Wirtschaftsakteure sind in der IEC-62443 klar definiert. Ein Bundesamt oder Regierungsorgan wird dabei aber nicht als solches definiert. Somit ist in der Norm auch keine Information bezüglich Kooperationspflichten mit einem Bundesamt zu finden. Eine Umsetzung wird in Kapitel 5.5 gesondert betrachtet.

3.3.9 Schulungspflicht

Schulungspflichten gehen bei der IEC-62443 mit einem CSMS einher. Ein Kernaspekt des CSMS ist eine saubere Cybersicherheitshygiene und damit auch die Schulung des Personals. Diese liegt allerdings in der Verantwortung des Betreibers. Der Maschinenbauer kann lediglich Dokumente und Schulungsunterlagen zu seinem System bereitstellen, ist allerdings nicht dazu verpflichtet Schulungen zu geben.

3.3.10 Umsetzungspflicht

Die Umsetzungspflichten sind in der IEC-62443 vollumfänglich abgefangen. Die Anforderung eines risikobasierten Ansatzes in Verbindung mit einer umfangreichen Dokumentation erfüllt die Norm durch die ausführliche Risikoanalyse in Verbindung mit der CRS. Auch das Schwachstellenmanagement ist fester Bestandteil der Norm.

Die definierten Anforderungen bezüglich technischer und organisatorischer Maßnahmen werden allesamt durch die verschiedenen System Requirements der IEC-62443-3-3, welche in Kapitel 3.2 erarbeiteten wurden, abgefangen.

4 Beschreibung des Umsetzungsleitfaden

In diesem Kapitel wird die Umsetzung des Umsetzungsleitfadens erklärt. Da das Ziel dieser Arbeit ein umfangreicher Umsetzungsleitfaden sein soll, welcher jedoch aufgrund des Umfangs nicht im Detail beschrieben wird, wird in diesem Kapitel zunächst erklärt, welche Teilkomponenten im Umsetzungsleitfaden benötigt werden, ehe diese in den nachfolgenden Kapiteln erarbeitet werden. Der fertige Leitfaden kann nicht als Teil dieser Arbeit veröffentlich werden, sondern wird über GitBook (Quelle: https://umsetzungsleitfaden.gitbook.io/leitfaden-zur-erhohung-der-security-von-maschinen [21]) zur Verfügung gestellt und kontinuierlich erweitert. Die Anwendung von GitBook ist kein Gegenstand der Arbeit und dient lediglich der Veröffentlichung der Arbeit. Wie welche Seiten erstellt wurden, wird daher nicht näher erläutert. Mit dieser Arbeit soll die Erstellung des Leitfadens mitsamt dessen Inhalt berücksichtigt werden, welche wiederum als Eigenleistung zum Bestehen der Master-Thesis dient. Hier wird also die akademische Arbeit klar von dem praktisch umsetzbaren Umsetzungsleitfaden abgegrenzt.

4.1 Teilkomponenten des Umsetzungsleitfaden

Da der Umsetzungsleitfaden für viele verschiedene Maschinenbauer nutzbar sein soll, sollte dieser so umfangreich wie möglich, mit einem gleichzeitig nicht zu strengem Handlungsspielraum sein. Es werden daher verschiedene Vorgehensweisen, Kataloge und Handlungsempfehlungen gegeben. Die Vorgehensweisen sollten dabei befolgt werden, die Kataloge dienen zur Unterstützung, um passende Maßnahmen zu definieren und die Handlungsempfehlungen sind lediglich Empfehlungen, welche nicht zwingend, in der beschriebenen Weise, umgesetzt werden müssen.

Die Teilkomponenten des Umsetzungsleitfaden lassen sich in drei Hauptkategorien aufteilen.

- Die Kataloge
- Der Cyber Security Risikobewertungsprozess
- Das Abnahmeprotokoll

Die Kataloge werden sowohl technische als auch organisatorische Sicherheitsmaßnahmen enthalten, welche wiederum auf Implementierungsdokumentationen verweisen. Zusätzlich zu den Sicherheitsmaßnahmen werden Prüfverfahren und Prüftools dokumentiert, welche zur Validierung der Sicherheitsmaßnahmen dienen, sowie eine Sammlung verschiedener Bedrohungsszenarien.

Der Cyber Security Risikobewertungsprozess ist die zentrale Komponente des Umsetzungsleitfadens. Mit ihm wird ein Verfahren bereitgestellt, die Sicherheit der Maschine zu bewerten, zu verbessern und zu validieren. Dies geschieht dabei dokumentenbasiert. Begleitdokumente müssen dafür in dieser Arbeit erarbeitet werden, da der Standard keine vorgibt.

Das Abnahmeprotokoll dient dazu, die erstellten Dokumentationen und Verfahren zusammenzuführen und damit ein lückenloses Dokument mit allen getroffenen Annahmen, Verfahren, Betrachtungen, Implementierungen, Rahmenbedingungen und Bewertungen zu erstellen, welches wiederum als Nachweis der Sicherheit der Maschine dient.

4.2 Anwendung des Umsetzungsleitfaden

Der Umsetzungsleitfaden besteht aus dem gesamten Cyber Security Risikobewertungsprozess, unter Zuhilfenahme der Kataloge zur einfacheren und schnelleren Durchführung, sowie verschiedenen Begleitdokumenten für das Abnahmeprotokoll. Durch die Erarbeitung der rechtlichen und normativen Anforderungen in Kapitel 3 wurden zudem die Kernprinzipien erarbeitet, welche für eine rechtliche Konformität erreicht werden müssen. Diese Erkenntnisse fließen ebenfalls in den Umsetzungsleitfaden mit ein und sorgen dafür, dass der

Maschinenbauer alle Anforderungen, nach durchlaufen des Leitfadens, erfüllt. Der Prozess des Umsetzungsleitfadens ist in Bild 7 zu sehen und wird nachfolgend kurz erklärt.

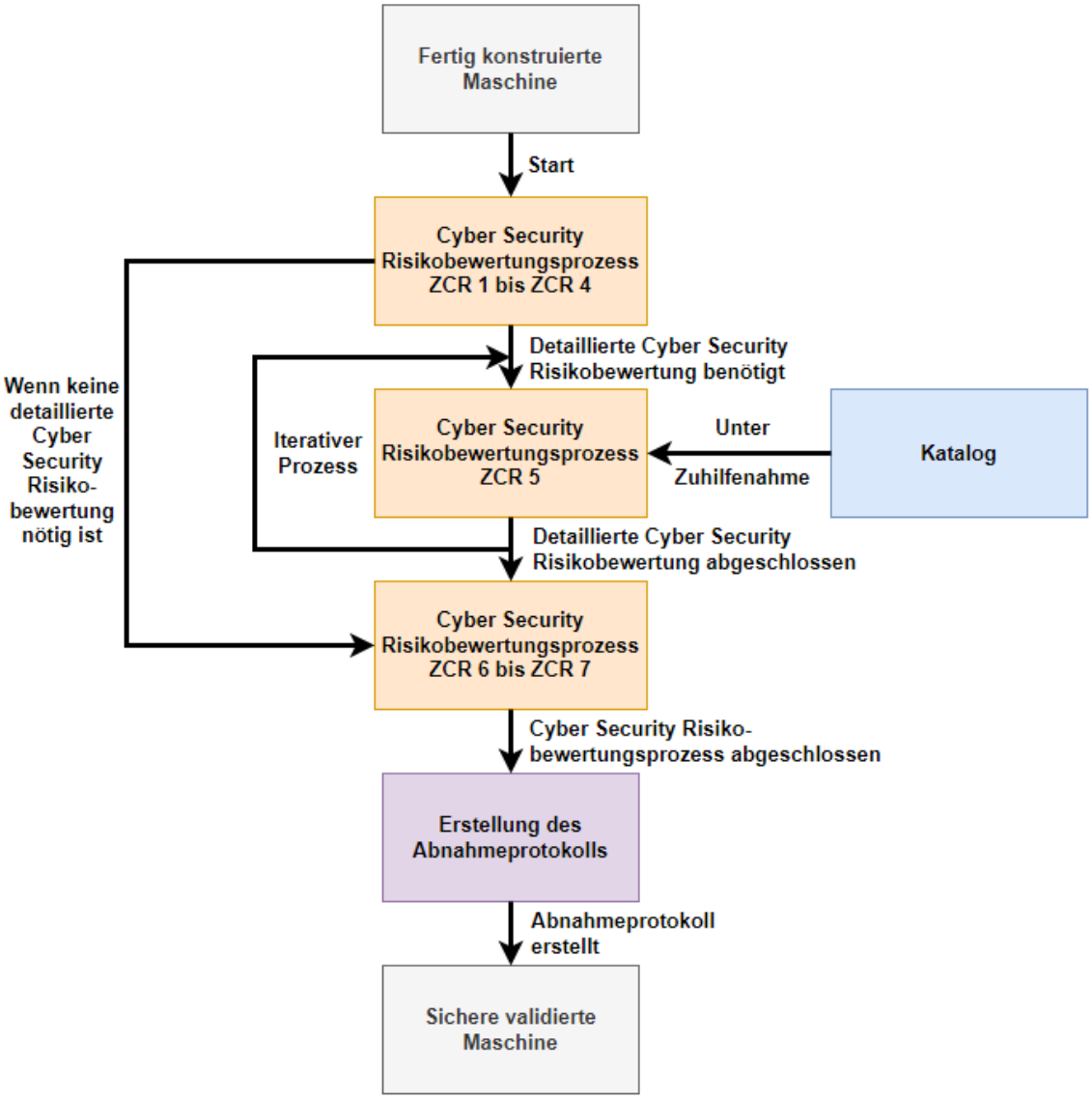


Bild 7: Prozess des Umsetzungsleitfadens

Quelle: Eigene Darstellung

Wenn die Maschine fertig konstruiert ist, kann mit dem Cyber Security Risikobewertungsprozess angefangen werden, welcher in Kapitel 6 genauer erklärt wird. Dabei wird das Risiko der Maschine bewertet. Ist das Risiko zu hoch, müssen Maßnahmen ergriffen werden, welche in der detaillierten Cyber Security Risikobewertung definiert werden. Hierbei kommen die verschiedenen Kataloge zur Anwendung. Um Bedrohungen zu definieren, kann der Bedrohungskatalog

verwendet werden. Zur Identifikation von Schwachstellen unterstützt der Prüfverfahren-Katalog. Um zusätzliche Sicherheitsmaßnahmen nach dem Stand der Technik zu implementieren, dient der technische und organisatorische Sicherheitsmaßnahmenkatalog. Um diese Sicherheitsmaßnahmen zu validieren kann ebenfalls der Prüfverfahren-Katalog verwendet werden und zu guter Letzt bietet der Grundlagen Katalog alle grundlegenden Bedingungen, welche für eine gesetzliche Konformität ebenfalls implementiert werden müssen.

Wurde der Risikobewertungsprozess abgeschlossen, dient zudem das Abnahmeprotokoll als Checkliste, um sicher zu gehen, dass alles Nötige implementiert und beachtet wurde und die Dokumentation vollständig ist. Ebenfalls dient das Abnahmeprotokoll dazu, dem Kunden die Sicherheit der Maschine zu bestätigen.

5 Erstellung der Kataloge

Da weder die Regulatorien noch die Normen den genauen Stand der Technik ausformulieren, ist es umso schwerer, in der Praxis geeignete Sicherheitsmaßnahmen ausfindig zu machen. Es ist ebenso nicht definiert, bei welchem Risiko welche Maßnahme implementiert werden müssen. Eine Segmentierung kann technisch unterschiedlich aussehen. Wie dies dann schlussendlich umgesetzt wird ist jedem überlassen, was jedoch, vor allem im Bereich der OT, zu Überforderung führt.

Um dem entgegenzuwirken, sollen Kataloge erstellt werden, welche den Stand der Technik als reale Sicherheitsmaßnahmen enthalten. Die Sicherheitsmaßnahmen sollen dabei sowohl technisch als auch organisatorisch sein und soweit ausformuliert und beschrieben werden, dass diese einfach in der Praxis umgesetzt werden können. Um dem Umfang der Arbeit gerecht zu werden, wird die Ausformulierung der Umsetzung nur an zwei Maßnahmen, einer technischen und einer organisatorischen, auszugsweise aufgezeigt. Weitere Sicherheitsmaßnahmen und ausführliche Beschreibungen werden nach der Abgabe der Arbeit weiter ergänzt, um dementsprechend den Stand der Technik aktuell zu halten.

5.1 Auswahl technischer Sicherheitsmaßnahmen

Technische Maßnahmen sind all jene Maßnahmen, welche durch technische Mittel ein Eindringen in ein System verhindern, entdecken, abmildern oder erschweren. Technische Sicherheitsmaßnahmen können dabei sehr umfangreich sein und sowohl zusätzlich hinzugefügt, als auch standardmäßig in Systemen vorhanden sein. Die Sicherheitsmaßnahme von Verschlüsselungen ist beispielsweise bei bestimmten Protokollen, wie IPSec oder TLS, schon vorhanden. Integritätssicherrungen werden ebenfalls in gewissen Protokollen berücksichtigt. Andere Sicherheitsmaßnahmen wie Firewalls müssen jedoch speziell konfiguriert werden, dass diese Sicherheit gewährleisten.

5.1.1 Katalog der technischen Sicherheitsmaßnahmen

Der Katalog ist alphabetisch aufgebaut und simpel gehalten, um die Übersichtlichkeit und Nutzerfreundlichkeit zu gewährleisten. Im Katalog werden lediglich die Namen der Sicherheitsmaßnahmen, in Verbindung mit einem Link zur Umsetzungsdokumentation genannt, in welcher weiterführende Informationen sowie eine ausführliche Implementierungsbeschreibung zu finden sind. Ein Ausschnitt aus dem technischen Katalog ist in Bild 8 zusehen.

Bild 8: Technischer Katalog

Quelle: Auszug aus dem erstellten Leitfaden [21]

Die Verlinkung zu den Umsetzungsdokumentationen ist anhand eines Beispiels in Bild 9 dargestellt:

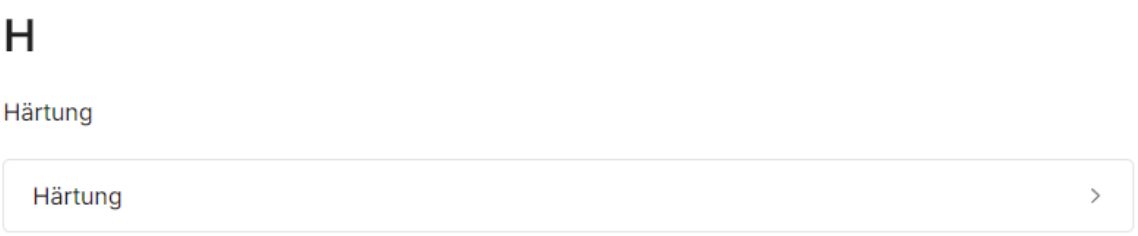


Bild 9: Verlinkung zur Umsetzungsdokumentation

Quelle: Auszug aus dem erstellten Leitfaden [21]

5.1.2 Umsetzungsdokumentation der technischen Sicherheitsmaßnahmen

Mit einem Klick auf Härtung gelangt man zur Beschreibungsseite der technischen Maßnahme zur Härtung von Systemen, wie in Bild 10 aufgezeigt.

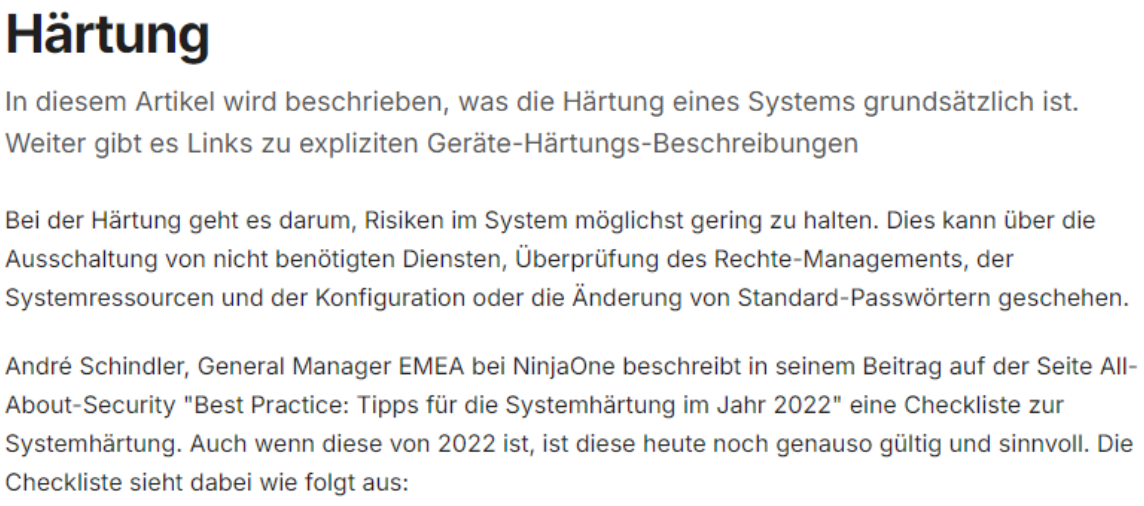


Bild 10: Beschreibungsseite der technischen Maßnahme "Härtung"

Quelle: Auszug aus dem erstellten Leitfaden [21]

Gibt es zu einem Thema spezifischere Anleitungen, beispielsweise durch unterschiedliche Hard- und Software, bei der man die Vorgehensweise unterschiedlich anwenden muss, so wird in der Umsetzungsdokumentation darauf verwiesen und eine spezifischere Anleitung zu diesen spezifischen Geräten gegeben. Ein solches Beispiel betrifft die Härtung von Siemens SCALANCE-Switchen, welche weitverbreitet in der Industrie Verwendung finden. Die Härtung eines Siemens-Switches ist dabei auf einer weiteren Seite detaillierter erklärt. Auszüge davon sind in Bild 11 und Bild 12 zusehen.

Härtung Scalance XC Siemens

Hier wird die Härtung von Siemens Scalance XC Switchen beschrieben.

Die Siemens Scalance XC Switche sind Industrie-Switche der Firma Siemens. Sie sind für rauere Umgebungen geschaffen, dazu zählt ein erhöhter Betriebstemperaturenbereich, Staub und Vibrationsresistenzen. Hinzukommt, dass für den Scalance XC Switch eine IEC-62443-4-2:2019 Zertifizierung besteht, wodurch gewährleistet ist, dass das Gerät über die grundlegenden Sicherheitsstandards nach dem Stand der Technik verfügt.

Nachfolgend wird die sichere Konfiguration des Scalance XCs gezeigt:

Bild 11: Härtung SCALANCE XC Siemens 1

Quelle: Auszug aus dem erstellten Leitfaden [21]

Wie zusehen ist, sind in den Standard-Einstellungen verschiedene sicherheitskritische Einstellungen voreingestellt. Zum einen sollte Telnet nicht mehr unterstützt werden, da bei diesem Protokoll keine Verschlüsselung erfolgt und Passwörter dabei im Klartext übertragen werden. Das selbe gilt für HTTP. Bei der Minimum TLS-Version von TLS 1.1 ist zu erwähnen, dass TLS 1.1 seit März 2021 als überholt gilt und daher nicht mehr verwendet werden sollte. Im Simple Network Management Protocol (SNMP) gibt es in den Versionen 1 und 2 kaum bis keine Sicherheitsmechanismen. Auch hier werden Passwörter im Klartext übertragen. Um den Scalance dahingehend zu härten empfiehlt sich daher die folgende Einstellung:

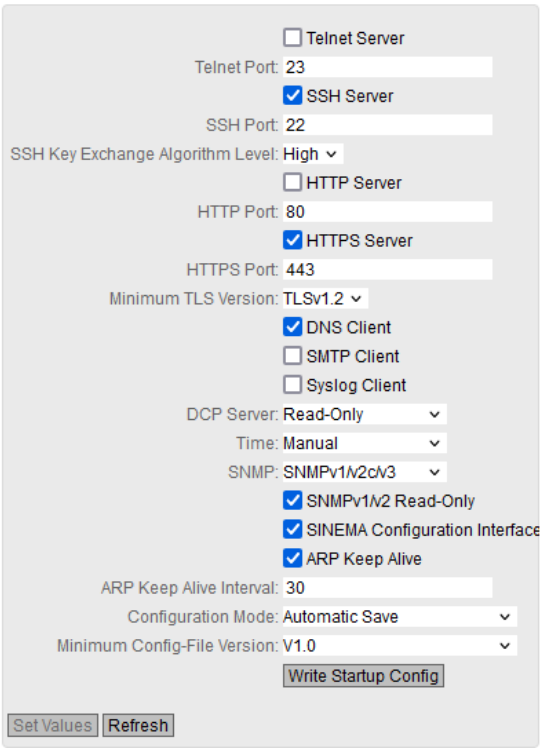


Bild 12: Härtung SCALANCE XC Siemens 2

Quelle: Auszug aus dem erstellten Leitfaden [21]

5.2 Auswahl organisatorischer Sicherheitsmaßnahmen

Organisatorische Maßnahmen sind Maßnahmen, welche von der Umsetzung der beteiligten Personen abhängt. Der Grad der Sicherheit kann daher kaum bestimmt werden. Durch systematische Fehler kann eine organisatorische Maßnahme niemals vollen Schutz gewährleisten. Dennoch sind organisatorische Maßnahmen ein gutes Mittel, um das Sicherheitsniveau zu erhöhen, sei es durch Schulungen, Richtlinien oder etablierten Prozesse, an welche sich zwingend gehalten werden sollten.

5.2.1 Katalog der organisatorischen Sicherheitsmaßnahmen

Der Katalog der organisatorischen Sicherheitsmaßnahmen ist wie der Katalog der technischen Sicherheitsmaßnahmen aufgebaut, zusehen in Bild 13.

Bild 13: Organisatorischer Katalog

Quelle: Auszug aus dem erstellten Leitfaden [21]

5.2.2 Umsetzungsdokumentation der organisatorischen Sicherheitsmaßnahmen

Die Dokumentation der organisatorischen Maßnahmen kann nicht analog zu den technischen Sicherheitsmaßnahmen durchgeführt werden. Während technische Maßnahmen reproduzierbar bei jeder Umsetzung sind, werden organisatorische Maßnahmen immer, aufgrund verschiedener Rahmenbedingungen unterschiedlich sein. Im Umsetzungsdokument werden daher vorerst lediglich Empfehlungen und Beispiele gegeben. Eine strikte Vorgehensweise kann nicht gegeben werden und würde auch nicht zum gewünschten Ergebnis führen, da jedes Unternehmen und jeder Anwender die verschiedenen organisatorischen Maßnahmen auf sich und seine Umgebung anpassen sollte. Ein Auszug aus der Empfehlung der organisatorischen Maßnahme der Schulungen ist in Bild 14 dargestellt.

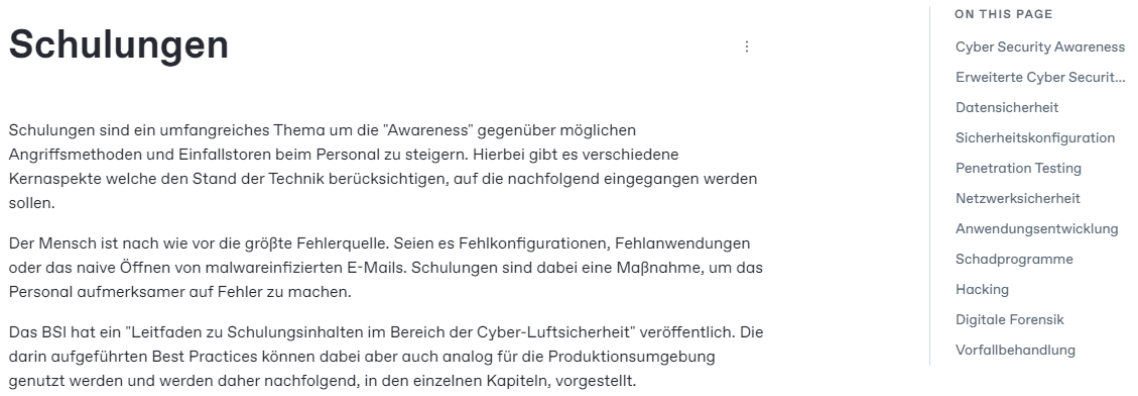


Bild 14: Beschreibung der organisatorischen Maßnahme "Schulungen"

Quelle: Auszug aus dem erstellten Leitfaden [21]

5.3 Auswahl verschiedener Prüftools und Prüfverfahren

Da Sicherheitsmaßnahmen falsch implementiert, falsch designt oder auch falsch gelebt werden können, sollten diese auf ihre Funktionsfähigkeit geprüft werden. Hierzu werden verschieden Prüftools und Prüfverfahren definiert, welche dabei helfen sollen, verschiedene Sicherheitsmaßnahmen zu validieren. Die Validierung soll dabei möglichst detailliert dokumentiert werden, um den Betreibern später die Funktionsfähigkeit bei Auslieferung nachweisen zu können.

5.3.1 Katalog der Prüftools und Prüfverfahren

Der Katalog der Prüftools und Prüfverfahren ist genauso aufgebaut wie die technischen und organisatorischen Kataloge. Ebenfalls führen hier Verlinkungen zu den eigentlichen Umsetzungsdokumentationen, wie in Bild 15 zusehen:

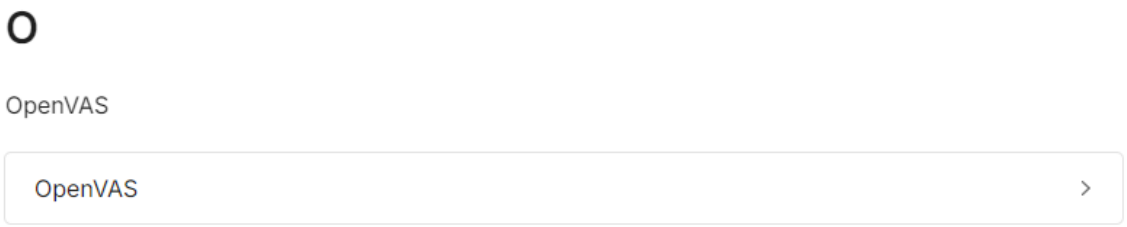


Bild 15: Verlinkung der Umsetzungsdokumentationen im Prüftool-Katalog

Quelle: Auszug aus dem erstellten Leitfaden [21]

5.3.2 Umsetzungsdokumentation der Prüftools und Prüfverfahren

Die Umsetzungsdokumentation der Prüftools und Prüfverfahren soll erklären, wie man Schwachstellen findet und die Sicherheit der Komponenten und des Systems validiert. Dazu sollen sowohl einfache Beispiele gegeben werden, um grundlegende Funktionen erfüllen zu können als auch detailliertere Beschreibungen, um tiefere Schwachstellenanalysen durchführen zu können. Ein Auszug aus der Umsetzungsdokumentation zur Suche von Schwachstellen anhand von OpenVAS wird in Bild 16 gezeigt.

OpenVAS

OpenVAS ist ein vollumfänglicher Schwachstellen-Scanner. Dieser scannt Geräte oder Netzwerk auf potenzielle offene Ports, Dienste und das laufende Betriebssystem und gleicht die Ergebnisse mit einer Schwachstellendatenbank ab. Sind in der Datenbank Schwachstellen zu bestimmten Protokollversionen o.Ä. bekannt, welche ebenfalls auf dem Gerät gefunden wurde, so wird dies als gefundene Schwachstelle angezeigt, welche es zu patchen gilt. OpenVAS wird dabei vom BSI empfohlen: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Freie-Software/Tools/OpenVAS/OpenVAS.html

Nachfolgend soll ein Scan mit OpenVAS aufgezeigt werden. Die Installation wird dabei vorausgesetzt oder kann unter folgendem Link heruntergeladen werden: https://www.openvas.org/

Konfiguration eines Scans:

Bevor man mit der Konfiguration anfangen kann, muss man sich mit dem Web-Frontend von OpenVAS verbinden. Dazu muss man OpenVAS über folgenden Befehl starten:

```
// sudo gvm-start
```

Kommt die folgende Meldung, so ist das Frontend erreichbar:

```
// Opening Web UI (https://127.0.0.1:9392) in: 5 ...  4 ...  3 ...  2 ...  1 ...
```

Nun kann das Frontend über einen beliebigen Web-Client unter dem Link https://127.0.0.1:9392 aufgerufen werden:

Bild 16: Auszug aus der Umsetzungsdokumentation zum Einsatz von OpenVAS

Quelle: Auszug aus dem erstellten Leitfaden [21]

Das Ergebnis der durchgeführten Schwachstellenanalyse der OpenVAS-Beschreibung ist in Bild 17 zusehen:

Schwachstelle	Schweregrad ▼
SSL/TLS: Certificate Expired	5.0 (Mittel)
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Mittel)
FTP Unencrypted Cleartext Login	4.8 (Mittel)
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Mittel)
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Mittel)

Bild 17: Auszug aus den Ergebnissen des Schwachstellenscans via OpenVAS

Quelle: Auszug aus dem erstellten Leitfaden [21]

Bei Beschreibungen, in denen Schwachstellen gefunden werden können, sollen zudem Verlinkungen vorhanden sein, um Hilfestellungen bei der Schließung der Schwachstellen zu erhalten. Da OpenVAS vor allem Ports und Dienste prüft, wurde der Beschreibung eine Verlinkung zur Sicherheitsmaßnahme der „Härtung“ hinzugefügt, zusehen in Bild 18.

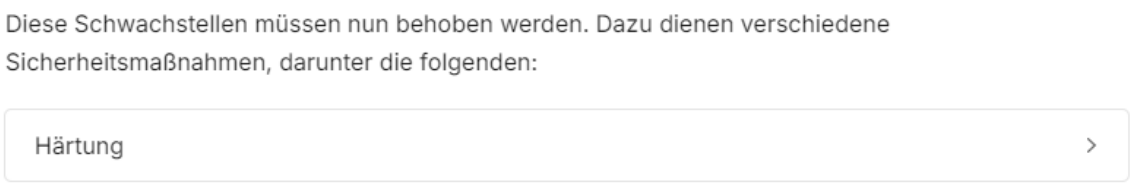


Bild 18: Auszug aus den Empfehlungen der Schwachstellenminimierung

Quelle: Auszug aus dem erstellten Leitfaden [21]

5.4 Katalog der Bedrohungen

Der Bedrohungskatalog dient dazu viele verschiedene Bedrohungen abzubilden, welche zur Bewertung des Risikos herangezogen werden können. Es erleichtert die Arbeit, da vorgefertigte Bedrohungsszenarien auf die eigenen Systeme angewendet werden können. Der Katalog beruht dabei auf verschiedenen Quellen, darunter dem Gefährdungskatalog des BSI aus dem RECPLAST GmbH Arbeitsbeispiel [33] und dem MITRE ATT&CK Framework [34].

Der Katalog enthält dabei, alphabetisch sortiert, die Überbegriffe der verschiedenen Bedrohungen, zusehen in Bild 19.

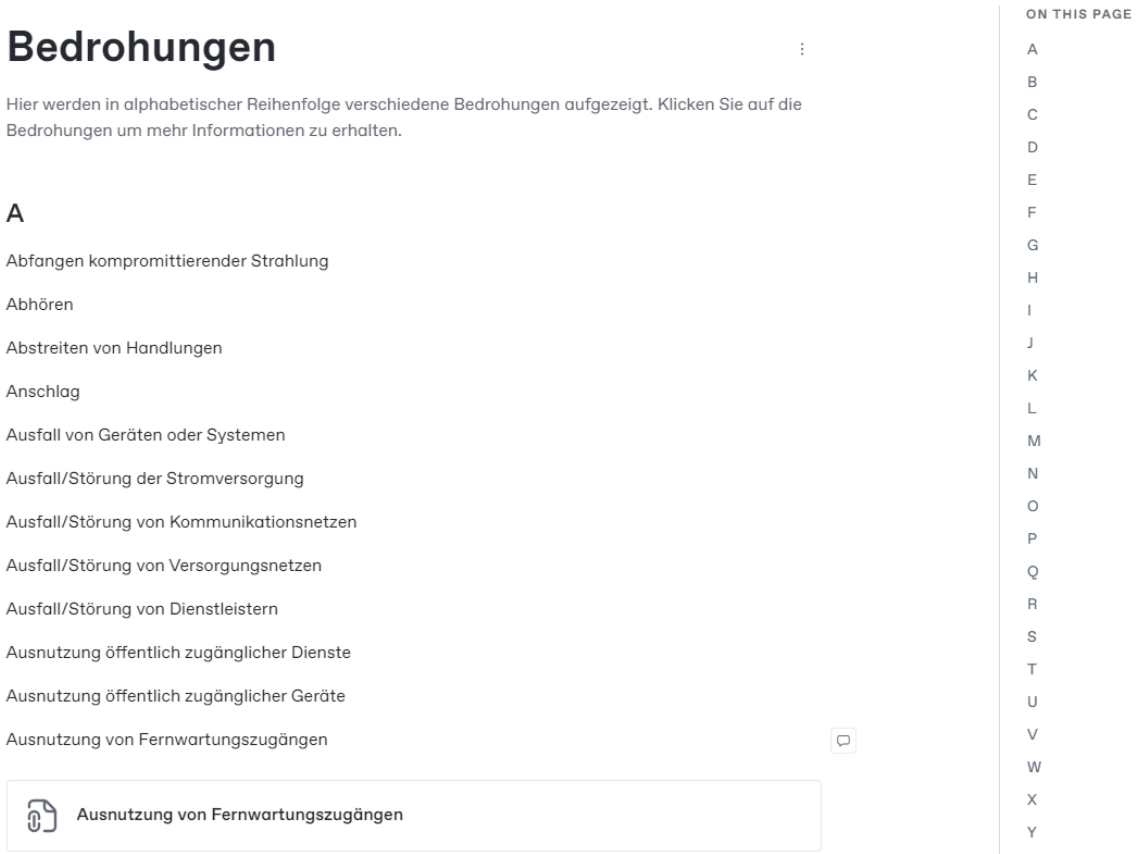


Bild 19: Bedrohungs-Katalog

Quelle: Auszug aus dem erstellten Leitfaden [21]

Von den einzelnen Überbegriffen führt ein Link zu genaueren Beschreibungen der Bedrohungen, welche ebenfalls die Dokumentation der Risikoanalyse vereinfachen. Zusätzlich werden Sicherheitsmaßnahmen, welche gegen diese Bedrohungen helfen können, ebenfalls verlinkt. Die Beschreibungsseite der Bedrohungen ist exemplarisch, für die Bedrohung „Ausnutzung von Fernwartungszugängen“, in Bild 20 dargestellt.

Bild 20: Ausnutzung von Fernwartungszugängen

Quelle: Auszug aus dem erstellten Leitfaden [21]

5.5 Katalog der grundlegenden Maßnahmen

Im Katalog der grundlegenden Maßnahmen werden auf all diejenigen Maßnahmen aus Kapitel 3.3 verwiesen, welche zur Erfüllung der Gesetzeskonformität benötigt werden und nicht durch Verfahren oder Maßnahmen der IEC-62443 abgedeckt werden, zusehen in Bild 21. Während die anderen Kataloge lediglich eine Sammlung und Hilfestellung darstellen, ist der grundlegende Maßnahmenkatalog zwingend erforderlich, um Gesetzeskonform zu sein.

Bild 21: Verzeichnis des grundlegenden Katalogs

Quelle: Auszug aus dem erstellten Leitfaden [21]

In Bild 22 ist dabei ein Auszug aus dem Katalog zusehen. Dabei werden unter anderem Prozesse zum Umgang der Unterrichtungspflicht definiert, um ein klares Vorgehen zu gewährleisten.

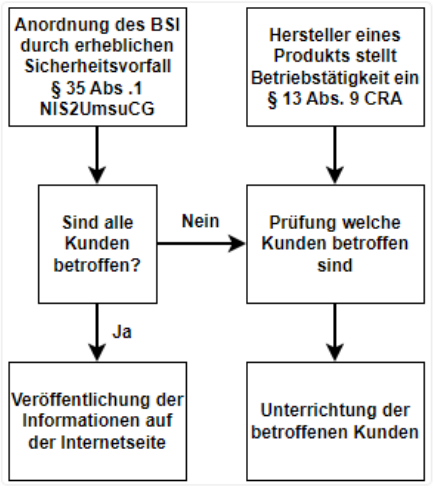
Grundlegende Maßnahmen

Hier werden grundlegende Maßnahmen und Verfahren erklärt welche zwingend notwendig sind um eine gesetzliche Konformität zu erreichen und nicht über Verfahren der IEC-62443 abgedeckt werden.

Durch die Erarbeitung der gesetzlichen Anforderungen und der Analyse der Konformität der IEC-62443 mit den gesetzlichen Anforderungen, sind Defizite aufgefallen. Einige Anforderungen werden dabei nicht durch die Norm abgedeckt. Diese müssen daher zwingend zusätzlich berücksichtigt und implementiert werden, wenn eine Gesetzeskonformität erreicht werden soll. Daher sollen nachfolgend diese Anforderungen betrachtet werden und geeignete Maßnahmen definiert werden.

Unterrichtungspflicht

Um den Unterrichtungspflichten gerecht zu werden, müssen Prozesse etabliert werden welche einen reibungslosen Ablauf der Kommunikation und Unterrichtung ermöglicht. Das Vorgehen sieht dabei wie folgt aus:



Prozess zur Unterrichtungspflicht (Eigene Darstellung)

Bild 22: Auszug aus dem grundlegenden Katalog

Quelle: Auszug aus dem erstellten Leitfaden [21]

6 Durchführung des IEC-62443-3-2 Cyber Security Risikobewertungsprozess

In diesem Kapitel wird der gesamte Cyber Security Risikobewertungsprozess der IEC-62443-3-2 [35] aus der Sicht des Integrators erklärt, sodass Integratoren in der Lage sind, diesen Risikobewertungsprozess auch ohne Informationen eines Betreibers (dazu mehr in Kapitel 6.2) durchzuführen. Die Arbeit soll den gesamten Risikobewertungsprozess den Integratoren näherbringen und wird daher mit weiteren Informationen untermauert. Im Anhang werden zudem Begleitdokumente und Vorlagen bereitgestellt, welche im Zusammenhang mit dieser Arbeit erstellt wurden, die Umsetzung des Risikobewertungsprozess erleichtern und eine nahezu vollständige Dokumentation ermöglichen sollen.

6.1 Rechtliche Notwendigkeit

Durch § 10 Abs. 1 CRA, welcher auf die grundlegenden Anforderungen in Anhang 1 Abschnitt 1 verweist, entsteht die Notwendigkeit einer Risikobewertung. So müssen Produkte so konzipiert, entwickelt und hergestellt werden, dass sie angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten [23]. Die Stickpunkte „Risiken“ und „Cybersicherheitsniveau“ deuten dabei ganz klar auf eine Cyber Security Risikobewertung hin. § 10 Abs. 2 CRA wird dabei noch deutlicher und fordert, dass für die Zwecke der Erfüllung von § 10 Abs. 1 CRA, eine Bewertung der Cybersicherheitsrisiken durchgeführt werden muss.

6.2 Umsetzung in der Praxis

Die IEC-62443-3-2 definiert den Cyber Security Risikobewertungsprozess als Aufgabe der Betreiber von Maschinen und Anlagen, da nur diese die erforderlichen Grundlagen besitzen und Rahmenbedingungen kennen. Darunter bspw. das akzeptierbare Unternehmensrisiko, die komplette Systemlandschaft, in welche die Maschine integriert wird, sowie verschiedene Verantwortlichkeiten oder mögliche Umwelteinflüsse des Standorts der Maschine.

In der Praxis ist es jedoch meist so, dass der Betreiber die Aufgabe des Risikobewertungsprozesses an den Integrator, mit dem Argument auslagert, dass der Betreiber schließlich eine sichere Maschine in Auftrag gibt und die Konstruktion, das Design und die Implementierung im Handlungsbereich des Integrators liegt. Die Norm sieht hierbei aber, wie in Kapitel 2.3.1 aufgezeigt, den Betreiber als Verantwortlichen für den kompletten Lebenszyklus einer Maschine, inkludierend der Entstehungsphase. Der Betreiber kann die Aufgabe der Risikobewertung an die Integratoren abwälzen, müsste dann aber alle benötigten Dokumente für den Integrator bereitstellen. Da diese Dokumente zum Teil jedoch vertraulich sind, hier seien zum Beispiel der Business Continuity Plan, die verfügbaren Ressourcen oder weitere unternehmensinterne Dokumente genannt, wird der Betreiber die grundlegenden Informationen nur geringfügig und unvollständig bereitstellen. Eine Risikobewertung ohne umfangreiche Grundlagen ist aber nichtig, da hier nicht das eigentliche Risiko zu den realen Rahmenbedingungen aufgrund mangelnder Informationen bewertet werden kann.

Eine Möglichkeit wäre also die Maschine einer Bedrohungsanalyse nach IEC-62443-4-1 zu unterziehen und das gesamte Automatisierungssysteme nicht als eigentliches „System“ zusehen, sondern als einzelnes „Produkt“, welches der Integrator vermarktet. Hier gibt der Standard verschiedene, grundlegende Komponentenanforderungen (Components Requirements) vor, welche ähnlich zu den System Requirements, jedoch speziell auf Komponenten bezogen sind. Zusätzlich dazu werden spezielle Anforderungen an spezielle Komponenten definiert, darunter für Softwareapplikationen, eingebettete Systeme, Host- und Netzwerkgeräte [36]. Spätestens an diesem Punkt ist unklar, wie das betrachtete System analysiert werden muss, da die verschiedenen Komponenten innerhalb des Systems verschiedene Anforderungen haben .

Der Ansatz, der in dieser Arbeit forciert und empfohlen wird, ist daher der gesamte Risikobewertungsprozess anhand der IEC-62443-3-2 mit Annahmen des Integrators. Wenn also Informationen vom Betreiber fehlen, um die Risikobewertung durchzuführen, so trifft der Integrator Annahmen dazu, dokumentiert diese, führt die Risikobewertung durch und hat eine Bewertung des

Risikos anhand dieser Annahmen für den Kunden. Die Akzeptanz dieser Bewertung liegt danach in der Verantwortung des Betreibers. Ist die Bewertung dem Betreiber nicht ausreichend genug, muss dieser selbst nachbessern oder eine eigene Bewertung durchführen. Wichtig für das weitere Vorgehen in diesem Kapitel ist jedoch zu beachten, dass im Falle der Annahmen die Risikobewertung kein „Taget-Security Level“ (SL-T) betrachtet, sondern ein „Capable-Security Level“ (SL-C). Das System kann also mit den getroffenen Annahmen zu einem bestimmten Security Level unter Beachtung dieser Annahmen fähig sein, daher „capable“. Das Target-Security Level liegt wiederum in der Verantwortung des Betreibers. Wenn dieser mit seinen Risikobewertungen ein SL-T von 2 erreichen muss und der Integrator ein SL-C von 2 anhand seiner Annahmen erreicht hat, muss der Betreiber nur noch prüfen, dass die Annahmen geringer oder gleichbedeutend mit den eigenen realen Rahmenbedingungen sind.

6.3 Beschaffung notwendiger Grundlagen

Bevor mit dem Risikobewertungsprozess gestartet werden kann, müssen verschiedene Grundlagen geschaffen und beschaffen werden. Darunter fallen grundlegende Beschreibungen über das System, die Anordnung von Ressourcen und des Personals sowie die Verteilung der Zuständigkeiten verschiedener Prozesse. Auch der Kunde sollte dabei mit eingebunden werden, da nur dieser fähig ist, gewissen Informationen bereitzustellen.

6.3.1 Definition der Risikobewertung

Eine Risikobewertung ist ein fortlaufender und nicht abschließbarer Prozess, weshalb ein Projektplan definiert werden muss, an welchem sich orientiert werden kann. Die Norm gibt hier ebenfalls Unterstützung und bietet ein fertiges Modell, welches zeigt, wie solch ein Prozess ablaufen kann. An diesem Modell, zusehen in Bild 23, kann sich orientiert werden. Dabei wird ersichtlich welche Informationen und Dokumente für welchen Prozess benötigt oder aus diesen generiert werden.

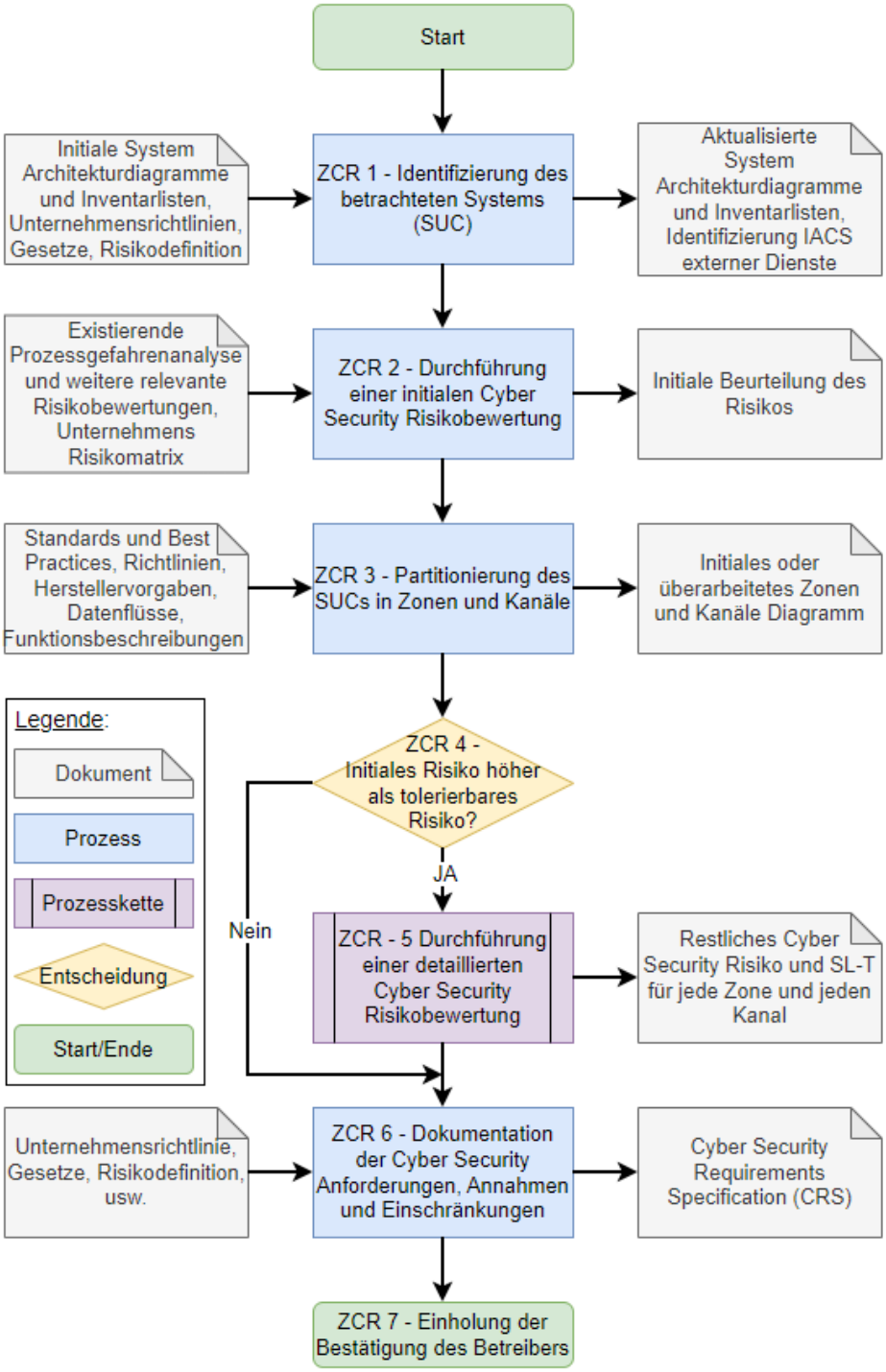


Bild 23: Prozess der Cyber Security Risikobewertung

Quelle: Eigene Darstellung nach IEC-62443-3-2 [35, p. 18]

Das Ergebnis dieses Prozesses ist die Cyber Security Requirements Specification. Ein Dokument, welches aus mehreren Dokumenten bestehen kann und alle Informationen zur durchgeführten Cyber Security Risikobewertung eines Systems mitsamt den Definitionen, Anforderungen, Prozessen und Maßnahmen,

welche betrachtet worden sind, enthält. Diese CRS zeigt die potenzielle Sicherheit des Systems zu dem Zeitpunkt an, an welchem die Risikobewertung durchgeführt wurde. Sollten andere Gegebenheiten eintreffen, wie beispielsweise das Bekanntwerden von Schwachstellen oder Sicherheitslücken in Verbindung mit dem System, so muss die Risikobewertung und damit auch die CRS überarbeitet werden. Dies ist der Grund, weshalb eine Risikobewertung kein abschließbarer Prozess sein kann, sondern immer fortlaufend betrachtet werden muss.

Des Weiteren muss während der Definition der Risikobewertung auch das System, welches betrachtet werden soll, definiert und dokumentiert werden. Im Falle des Integrators wäre dies immer die Maschine oder Anlage, welche für den Betreiber gebaut werden soll.

6.3.2 Informationsbeschaffung

Bei der Informationsbeschaffung sollten alle benötigten Informationen eingeholt werden, welche für die weitere Durchführung der Risikobewertung von Bedeutung sind. Dazu gelten unter anderem folgende Informationen:

- System Architekturdiagramme des Kunden (mindestens Informationen darüber, wie die Maschine an das System des Kunden gekoppelt wird)
- Netzwerkdiagramme des betrachteten Systems
- Asset-Inventarlisten (für Hardware, Software und virtualisierte Hardware)
- Datenfluss-Beziehungen
- Prozessbeschreibungen der Maschine
- Geltende Regulatorien (Industriestandards, internationale und nationale Normen, Unternehmensstandards und – Richtlinien)
- Unternehmensrisikodefinition und Risikomatrix

Weitere Informationen werden im Verlaufe der Risikobewertung erarbeitet. Umso umfangreicher und detaillierter die Dokumentationen sind, desto genauer und umfangreicher wird die Risikobewertung. Einige dieser Dokumente liegen in der Verantwortung des Kunden, eventuell sogar in der Verantwortung der Geschäftsleitung des Kunden. Sollte es hier Probleme bezüglich der

Informationsbeschaffung geben, durch beispielsweise vertrauliche Informationen, welche nicht weitergeben werden dürfen, empfiehlt es sich jedenfalls Annahmen zu treffen, welche als solche dokumentiert werden. Die Risikobewertung gilt dann nur in Verbindung mit den Annahmen. Sollte der Kunde seine Umgebung anpassen, so geschieht dies in seiner Verantwortung.

6.3.3 Risikodefinition

Wie die Risikobewertung bereits im Wort beschreibt, muss ein gewisses Risiko bewertet werden. Dafür muss allerdings definiert werden, was ein Risiko ist und wie dieses bestimmt werden kann. Die Norm definiert das Risiko als Produkt aus Bedrohung, Schwachstelle und Auswirkung, zusehen in Bild 24.

Bild 24: Risikoformel

Quelle: Eigene Darstellung nach IEC-62443-2-1 [31, p. 61]

Der Hintergrund ist, dass ein Risiko nur dann besteht, wenn es eine Bedrohung gibt, wie beispielsweise einen Angreifer, welche eine vorhandene und bekanntgewordene Schwachstelle ausnutzen kann, um das System zu beeinträchtigen und diese Beeinträchtigung eine Auswirkung zur Folge hat, wie beispielsweise einem wirtschaftlichen Verlust oder dem Diebstahl von Knowhow. Ist eines dieser drei Faktoren nicht vorhanden, so gibt es auch kein Risiko, denn eine existierende Schwachstelle, die niemand ausnutzt, birgt erstmal keine Gefahr.

Bedrohung:

Als Bedrohung gelten sowohl Personen und Programme als auch Geräte und Umwelteinflüsse. Eine Bedrohungsquelle kann dabei alles sein, was eine mögliche Bedrohung zum Vorschein bringen kann. Einige Beispiele wären:

- Internes und Externes Personal
- Hacker oder Hackergruppen
- Schadsoftware

- Infizierte Geräte / nicht ordnungsgemäß funktionierende Geräte
- Überschwemmungen, Brände, Erdbeben

Schwachstelle:

Eine Schwachstelle ist jeglicher Fehler eines oder jegliches Einfallstor in ein System. Ausgenutzt werden, könnten dabei Fehler im System-Design, Fehlkonfigurationen und -implementierungen oder Fehlfunktionen, welche das System kompromittieren. Beispiele zu Schwachstellen sind:

- Unzureichende / Nicht-gelebte Richtlinien und Prozeduren
- Fehlerhafte Architekturen & Designs
- Fehlkonfigurationen
- Softwarefehler
- Ausnutzbare Netzwerkzugriffe

Auswirkung:

Eine Auswirkung wird als unerwünschtes Ergebnis eines Vorfalls definiert. Dabei wird immer die am schlimmsten ausfallende Auswirkung betrachtet. Mögliche Auswirkungen können dabei

- Personenschäden
- Imageschäden
- Produktionsstillstände
- Datendiebstahl
- Geschäftsstillstände
- Umweltschäden

sein, die ebenfalls im Zusammenhang mit dem Ausmaß steht. Dieses wird verwendet, um die Auswirkung numerisch darzustellen.

Eintrittswahrscheinlichkeit:

Um das Risiko leichter bestimmen zu können, empfiehlt die Norm die Bedrohung und die Schwachstelle als Eintrittswahrscheinlichkeit zusammenzufassen. Die Eintrittswahrscheinlichkeit ist dabei die quantitative Chance, dass eine Aktion, ein Ereignis oder ein Vorfall auftritt. Dadurch wird das Risiko nur noch mit 2 Faktoren berechnet, wie in Bild 25 abgebildet ist.

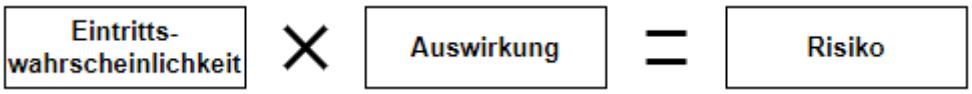


Bild 25: Vereinfachte Risikoformel

Quelle: Eigene Darstellung nach IEC-62443-2-1 [31, p. 61]

Die Bestimmung der Eintrittswahrscheinlichkeit erweist sich häufig als schwierig, da es hierfür keine greifbaren Werte gibt und die Motivation von Angreifern schlecht vorausgesagt werden kann. Ebenso sind potenzielle Schwachstellen noch gar nicht bekannt und können daher nicht berücksichtigt werden.

Risikomatrix:

Die Risikomatrix dient schlussendlich dazu, das Risiko in Werten darzustellen. Dabei ergibt sich das Risiko aus der Eintrittswahrscheinlichkeit in Verbindung mit den Ausmaßen der Auswirkungen. Der Kunde muss dabei bestimmen, welches die Worst-Case-Szenarien bei welcher Auswirkung sind, sowie welche Grenzwerte bei der Eintrittswahrscheinlichkeit genutzt werden. Zur besseren Vorstellung ist in Anhang 3 ein Beispiel einer solchen Risiko-Matrix dargestellt. Das Beispiel kann verwendet werden, es empfiehlt sich jedoch die Worst-Case-Szenarien an das jeweilige Unternehmen anzupassen. So sind für ein kleines Unternehmen bereits 250.000 € ein finanzieller Worst-Case wohingegen größere Unternehmen erst ab Millionenbeträgen vom Worst-Case ausgehen.

Tolerierbares Risiko:

Der Kunde muss ein tolerierbares Risiko vorgeben. Dies ist das Risiko, welches vom Kunden noch akzeptiert wird. Ist ein Risiko höher als das tolerierte Risiko, so müssen Maßnahmen zur Risikominderung unternommen werden. Sollte ein

Risiko geringer sein als das tolerierbare Risiko, so besteht kein weiterer Handlungsbedarf. Bei der Bestimmung des tolerierbaren Risikos empfiehlt es sich die Risikomatrix zu verwenden und zu bestimmen, welche Risiken für das Unternehmen tolerierbar sind und daher als Grenzwert dienen. Gibt der Kunde kein Risiko vor, so kann eine Annahme getroffen werden. Diese Annahme sollte dabei verhältnismäßig in Bezug auf die betrachtete Maschine sowie die zukünftigen Rahmenbedingungen (Standort, Betreiber, Größe des Unternehmens, geopolitische Einflüsse, usw.) sein, soweit diese eingeordnet werden können.

6.4 Identifizierung des betrachteten Systems (ZCR 1)

Nachdem die grundlegenden Dokumente vorliegen, ist der erste Schritt die Identifizierung des betrachteten Systems (im folgenden SUC, von System under Consideration). Im Falle des Integrators wäre dies die Maschine oder Anlage, welche er dem Betreiber baut. Die Identifizierung besteht daraus, Inventarisierungslisten zu Komponenten und Netzwerkdiagramme zu erstellen.

6.4.1 Inventarisierungslisten:

Bei den Inventarisierungslisten sollten drei Kategorien abgedeckt werden, nämlich die der Hardware, der virtuellen Hardware und der Software. Die Inventarisierungslisten geben einen guten Überblick über den Inhalt des Systems. Diese sind auch bezüglich der Rückverfolgbarkeit von Komponenten von Bedeutung. Im Falle einer neuen Schwachstelle einer Komponente kann über die Inventarisierungsliste bewertet werden, ob die entsprechenden Maschinen betroffen sind.

Hardwareinventar:

In der Hardware-Inventarisierungsliste sollten alle Kommunikationsfähigen-Komponenten mit folgenden Angaben zu den einzelnen Komponenten notiert sein:

- Geräte oder Systemname
- Gerätekennung (in Form einer ID)
- Gerätetyp
- Funktionsbeschreibung
- Vorhandene Netzwerkschnittstellen
- Netzwerkadressen
- Hersteller
- Model
- Artikelnummer
- Betriebssystem mit Version
- Firmware-Version
- Verantwortliche Abteilung / Person
- Standort
- Zusätzliche Notizen

Virtuelle-Hardwareinventar:

Alle verwendeten virtuellen Maschinen (VM) sollten ebenso dokumentiert werden. Dabei sollten auch solche dokumentiert werden, welche bspw. den Remote-Zugriff ermöglichen. Folgende Informationen sollten vermerkt werden:

- VM-Name
- VM-Typ
- Funktionsbeschreibung
- Vorhandene Netzwerkschnittstellen
- Netzwerkadressen
- Host Name oder ID
- Host Typ
- Betriebssystem mit Version

- Verantwortliche Abteilung / Person
- Administrator
- Zusätzliche Notizen

Softwareinventar:

Die Dokumentation von verwendeter Software ist ebenfalls von hoher Bedeutung. Dabei sollten nachstehende Informationen vorhanden sein:

- Name
- Betriebssystem für das die Software entwickelt wurde
- Funktionsbeschreibung
- Firmware
- Benötigte Datenbanken und Bibliotheken
- Link zur Website (bspw. bei Open Source)

Zur Erstellung der Inventarisierungslisten kann eine Software zur Unterstützung verwendet werden. Ein Beispiel zur Hardware-Inventarisierung wäre ein Netzwerkplaner, welcher über Protokolle, wie Simple Network Management Protocol (SNMP), die Informationen der Geräte ausliest. Zur Erstellung der Tabelle in Bild 26 wurde der Siemens Network Planner (SINETPLAN V2.0) verwendet. Dieser kann neben Netzwerkdiagrammen auch Hardwareeigenschaften aus einem bestehenden Netzwerk auslesen.

SIEMENS

1 Liste der Geräte

#	Name	Gerätetyp	IP-Adresse	Subnetz-Maske	Gateway	Rolle	Hersteller	Artikelnummer	SW-Version	HW-Version
1	Switch2	SCALANCE XC216	192.168.0.4	255.255.255.0	192.168.0.4	SWITCH	SIEMENS	6GK5216-0BA00-2AC2	V3.0	1
2	KeyPanel10	KP8F PN	192.168.0.139	255.255.255.0	192.168.0.139	HMI	SIEMENS	6AV3688-3AF37-0AX0	R01.00.00	1
3	Roboter2	STAUBLI CS9	192.168.0.181	255.255.255.0	192.168.0.181	GENERIC	STAUBLI FAVERGES	Unbekannt	Unbekannt	
4	SafetyFieldBox5	SFB-PN-IRT-8M12-IOP-V2	192.168.0.44	255.255.255.0	192.168.0.44	GENERIC	K. A. Schmersal GmbH & Co. KG	Unbekannt	Unbekannt	
5	ExtensionUnit1	ExtUnit	192.168.0.30	255.255.255.0	192.168.0.30	GENERIC	SIEMENS AG	6AV7 674-1LA63-0AA0	V1.2.2	
6	CodeLeser3	SR-X1H3HX	192.168.0.162	255.255.255.0	192.168.0.162	GENERIC	KEYENCE CORPORATION	0015028352	S1.0	
7	CodeLeser1	SR-X1H3HX	192.168.0.160	255.255.255.0	192.168.0.160	GENERIC	KEYENCE CORPORATION	0015028788	S1.0	
8	CodeLeser2	SR-X1H3HX	192.168.0.161	255.255.255.0	192.168.0.161	GENERIC	KEYENCE CORPORATION	0015028781	S1.0	
9	Servoregler7	C1250xPD	192.168.0.86	255.255.255.0	192.168.0.86	GENERIC	NTI AG	Unbekannt	Unbekannt	
10	Buskoppler2	IM 157-1 PN	192.168.0.51	255.255.255.0	192.168.0.51	IO	SIEMENS	6ES7157-1AB00-0AB0	V1.0	1
11	Servoregler19	S210	192.168.0.98	255.255.255.0	192.168.0.98	IO	SIEMENS	6SL3210-5Hx1x-xxFx	V5.1	V1.0
12	Servoregler15	S210	192.168.0.94	255.255.255.0	192.168.0.94	IO	SIEMENS	6SL3210-5Hx1x-xxFx	V5.1	V1.0
13	Servoregler10	C1250xPD	192.168.0.89	255.255.255.0	192.168.0.89	GENERIC	NTI AG	Unbekannt	Unbekannt	
14	Servoregler8	C1250xPD	192.168.0.87	255.255.255.0	192.168.0.87	GENERIC	NTI AG	Unbekannt	Unbekannt	
15	Switch3	SCALANCE XC216	192.168.0.5	255.255.255.0	192.168.0.5	SWITCH	SIEMENS	6GK5216-0BA00-2AC2	V3.0	1
16	Frequenzumrichter2	G120C PN	192.168.0.93	255.255.255.0	192.168.0.93	IO	SIEMENS	6SL3210-1KExx-xxFx	V4.7	V1.0

© Siemens AG - Siemens Network Planner Seite 3 von 8 13.08.2024

Bild 26: Beispiel einer automatisch generierten Inventarisierungsliste

Quelle: Selbstgeneriert mit SINETPLAN

Wie in der Tabelle zusehen ist, kann das Programm nicht alle Informationen auslesen. Zum einen sind Rollen von Fremdgeräten (Gelb markiert als Nicht-Siemens-Geräte) unklar, zum anderen ist das Auslesen der Hardware-Software, Artikelnummer und Software-Version nicht immer erfolgreich. Hinzukommt, dass die Tabelle nicht vollständig mit den zuvor definierten Informationen der Hardwareinventarisierung gefüllt ist. Daher empfiehlt es sich manuelle Listen zu führen, welche mit Hilfe von Software gefüllt werden. Ein Beispiel einer manuellen Liste ist in Anhang 4 zu finden.

6.4.2 Netzwerkdiagramme

Bei den Netzwerkdiagrammen geht es darum, die Architektur des SUC sowohl logisch, als auch physikalisch, darzustellen. Dazu werden die Switche, Router, Hosts und weitere netzwerkrelevante Geräte, welche im Netzwerk vorhanden sind, mit den IP-Adressen des dazugehörigen Netzes, angezeigt. VLANs sollten ebenfalls angezeigt werden. Die einzelnen Verbindungen zwischen den Geräten

sollten auch die tatsächlichen Schnittstellen (Ports) anzeigen, welche physikalisch verwendet werden. Bei unterschiedlichen Bussystemen würde es sich anbieten, diese Verbindungen in unterschiedlichen Farben anzuzeigen. Bei größeren Systemen, wie beispielsweise großen Produktionslinien, würde es sich anbieten, für jede kleine Teilzelle ein eigenes Netzwerkdiagramm, sowie ein übergeordnetes Diagramm anzufertigen, welches bei den Zellen nur die Zelle an sich anzeigt und auf die jeweils detaillierteren Diagramme verweist. Die Zutrittspunkte zum System sollten ebenfalls dokumentiert und markiert werden. Dazu zählen Verbindungen an überlagerte Systeme oder auch Fernwartungsverbindungen.

Bei den Netzwerkdiagrammen bietet es sich ebenfalls an eine Software zur Unterstützung zu verwenden. So wurde in Anhang 5 beispielsweise ebenfalls SINETPLAN zur Erstellung eines Netzwerkdiagramms verwendet. Aufgrund dessen, dass SINETPLAN auf dem offenen industriellen Ethernetstandard PROFINET basiert, können auch nur die Eigenschaften von PROFINET-Geräten ausgelesen werden, oder Geräten die SNMP unterstützen. Für größere IT-Netze empfiehlt es sich daher umfangreichere Tools zu nutzen oder die Diagramme manuelle anzufertigen. Zur manuellen Anfertigung gibt es ebenfalls frei zugängliche Unterstützungsprogramme wie Draw.io, in dem fertige Netzwerkvorlagen zu finden sind. Hier müssen jedoch alle Geräte einzeln eingetragen und Verbindungen manuell definiert werden.

6.4.3 Systembesichtigung

Es empfiehlt sich das System physikalisch zu begutachten, um dabei die Korrektheit der Netzwerkdiagramme zu validieren. Dabei sollten auch die physischen Sicherheitsmaßnahmen dokumentiert werden, welche bereits für das System vorhanden sind. Dazu zählen bspw. Türen, Tore oder Schränke. Auch das Interviewen von Bedienern und vertrautem Personal des Systems sollte dabei durchgeführt werden, um die Funktionsweise des Systems besser zu verstehen. Dies ist essenziell, um mögliche Auswirkungen in Bezug auf einen Systemausfall besser verstehen zu können.

6.5 Durchführung einer initialen Cyber Security Risikobewertung (ZCR 2)

Bei der initialen Cyber Security Risikobewertung geht es darum, die Worst-Case-Szenarien in Verbindung mit dem SUC zu identifizieren, wenn keine Sicherheitsmaßnahmen integriert wären. Dabei lohnt es sich die folgenden Punkte in Worst-Case-Szenarien zu bewerten:

- Gesundheitliche Schäden
- Funktionsfähigkeit der Safety-Komponenten
- Umweltschäden
- Geschäftsunterbrechungen
- Produktionsverlust
- Produktionsqualität
- Finanzielle Schäden
- Rechtliche Konsequenzen
- Ansehen/Reputation

Die initiale Cyber Security Risikobewertung sollte von Personal durchgeführt werden, welches tiefgreifendes Knowhow im Bereich der industriellen Steuerungssysteme hat sowie den Prozess des Systems versteht. Für die Einschätzung des Prozesses können, wenn vorhanden, Prozessgefahrenanalysen herangezogen werden. Umso genauer das Verständnis des Prozesses des Systems ist, desto besser können mögliche Auswirkungen identifiziert werden.

In der initialen Risikobewertung sollen die Ausfälle des Systems lediglich die Worst-Case-Szenarien betreffen, so zum Beispiel:

- Der Ausfall mehrerer oder aller Server
- Der Ausfall mehrerer oder aller speicherprogrammierbaren Steuerungen
- Komplette oder weitläufige Störung der Stromversorgung
- Eine böswillige Person hat kompletten Zugriff auf Steuerungssysteme

Die initiale Cyber Security Risikobewertung sollte mit einem Risiko, dem initialen Risiko, abgeschlossen werden. Dazu bewertet man das Risiko der Worst-Case-Szenarien durch die Risikomatrix.

Um die initiale Cyber Security Risikobewertung nicht bei null anfangen zu müssen, empfiehlt es sich grundlegende Gefährdungen aus vorhandenen Leitfäden zu verwenden. Einen umfangreichen Gefährdungskatalog findet man zum Beispiel beim vom BSI gefertigten RECPLAST GmbH Arbeitsbeispiel zur Implementierung eines Informationssicherheits-Managementsystems.

Ein Auszug aus der initialen Cyber Security Risikobewertung, welche hier erarbeitet wurde, ist in Bild 27 zusehen.

Gefährdung:		Ausfall von mehreren Systemen oder Geräten				
Gesundheitliche Schäden:		Kritisch				
Funktionsfähigkeit der Safety-Komponenten:		Kritisch				
Umweltschäden:		Trivial				
Geschäftsunterbrechungen:		Bedeutend				
Produktionsverlust:		Kritisch				
Produktionsqualität		Mäßig				
Finanzielle Schäden:		Mäßig				
Rechtliche Konsquenzen:		Trivial				
Ansehen/Reputation:		Mäßig				
Beschreibung des Worst-Cases:		Durch den Ausfall der SPS oder weiteren netzwerkkrischen Geräten oder safety-integrierten Systemen kann die gesamte Maschine zum erliegen kommen.				
Beschreibung der Auswirkungen:		Durch nicht Funktionsfähigkeit der Safety-Komponenten kann es zu tödlichen Unfällen innerhalb und im Einflussbereich der Maschine kommen. Auch der Produktionsverlust der Maschine durch einen langfristigen Ausfall der Systeme wäre nicht tragbar da Kunden unzufrieden werden, Aufträge verloren gehen und finanzielle Schäden auf das Unternehmen zukommen.				
Beschreibung der Eintrittswahrscheinlichkeit		Der Ausfall mehrere Systeme oder Geräte scheint möglich auf Grund von äußeren Einflüssen (Erdbeeben, keine Spannungsversorgung), sowie durch Sabotage				
Kritische Komponenten:		SPS, Netzwerkgeräte, Safety-integrierte Systeme				
		Unwahrscheinlich	**Selten**	**Möglich**	**Wahrscheinlich**	**Definitiv**
		1	**2**	**3**	**4**	**5**
Trivial	**1**	1	2	3	4	5
Gering	**2**	2	4	6	8	10
Mäßig	**3**	3	6	9	12	15
Bedeutend	**4**	4	8	12	16	20
Kritisch	**5**	5	10	15	20	25

Bild 27: Ausschnitt aus der initialen Cyber Security Risikobewertung

Quelle: Eigene Darstellung aus Anlage 3

6.6 Partitionierung des SUCs in Zonen und Kanäle (ZCR 3)

Bei der Partitionierung des SUCs wird das System in verschiedene Zonen und Kanäle aufgeteilt. Die Aufteilung beruht zum einen auf den Ergebnissen der initialen Cyber Security Risikobewertung (welche Komponenten sind besonders schützenswert) und zum anderen auf Kriterien wie der Funktionalität der Komponenten, dem physischen Standort, Zuständigkeiten oder den benötigten Zugriffsrechten. Die Partitionierung erleichtert den Umgang mit der Norm, da so lediglich die Zonen und Kanäle als Ganzes betrachtet werden müssen und die einzelnen Komponenten in der Zone, die Sicherheitsanforderung der gesamten Zone erhalten. Die Aufteilung der Zonen und Kanälen wir dabei bei den grundlegenden Informationen in der CRS dokumentiert, zusehen in Anhang 6.

6.6.1 Trennung zwischen IT und OT - Systemen

Der Standard gibt bestimmte Zonierungen vor, welche teils verpflichtend oder empfehlend sind. Die Trennung zwischen IT und OT ist eine solcher verpflichtenden Trennungen. Dies geht einher mit den großen Unterschieden der Sicherheitsziele zwischen IT und OT. Bei der OT steht vor allem die Verfügbarkeit der Systeme im Vordergrund. Bei der IT die Vertraulichkeit von Informationen. Zusätzlich betrifft die OT direkt die Gesundheit, Sicherheit und Umwelt durch die Prozesse, welche dort stattfinden.

6.6.2 Trennung Safety-relevanter Komponenten

Des Weiteren sollten im OT-Bereich Safety-relevante Komponenten von den restlichen Komponenten getrennt werden. Die Safety spielt eine übergeordnete Rolle, da diese einen noch höheren Stellenwert für die Gesundheit, Sicherheit und Umwelt hat. Um die Safety besser gewährleisten zu können, sollte diese daher in eine eigene Zone mit höherem Sicherheitsniveau. In der Praxis benutzen Safety-Komponenten meist denselben Datenbus (ProfiSafe über PROFINET) und in einigen Fällen sogar dieselbe SPS zur Verarbeitung (Failsafe SPSen Siemens S7-1500er Reihe). Kann die normale Maschinensteuerung nicht von der Safety-Steuerung getrennt werden, so müssen diese in dieselbe Zone und für die

gesamte Maschinensteuerung gilt dann dasselbe Sicherheitsniveau wie für die Safety.

6.6.3 Trennung temporär verbundener Geräte

Auch temporär verbundene Geräte sollten in eine eigene Zone. Dazu zählen beispielsweise USB-Geräte, portable Festplatten oder Engineering-Laptops. Bei diesen ist nicht nachweisbar, wo sie verwendet werden, weshalb von ihnen ein erhöhtes Sicherheitsrisiko ausgeht und daher ein höheres Sicherheitsniveau benötigt wird. Eine Ausnahme bilden hierbei mobile Bedienpanels, welche zwar temporär an die Maschine verbunden werden, aber ausschließlich nur für diese Maschine konfiguriert werden und dementsprechend ein Bestandteil des eigentlichen Maschinenetzes sind.

6.6.4 Trennung drahtloser Geräte

Da drahtlose Geräte keine physischen Zonengrenzen beachten, bis außerhalb des Firmengeländes strahlen könnten und daher zugänglicher sind, bedarf es höherer Sicherheitsniveaus als bei normalen Maschinengeräten. Daher sollten auch drahtlose Geräte in eine eigene Zone zusammengefasst werden, wozu neben WLAN und 5G auch RFID, ZigBee oder LoRaWAN zählen. Ein Wireless Access Point (WAP) wird dabei als eigener Kanal zwischen einer kabellosen und einer kabelgebundenen Zone dargestellt.

6.6.5 Trennung von Komponenten mit externen Netzanschlüssen

Geräte mit externen Netzanschlüssen finden vermehrt Einzug in die Produktionsumgebung. Dies betrifft nicht mehr nur VPN-Router, um Fernwartungen zu ermöglichen. Durch die Digitalisierung werden auch Edge-Device verwendet, welche eine ständige Verbindung ins Internet benötigen, um Maschinendaten in die Cloud auszulagern. Solche Geräte bieten durch den Zugriff ins Internet eine erhöhte Angriffsfläche, weshalb diese in eine eigene Zone mit erhöhtem Sicherheitsniveau eingeteilt werden sollten.

6.7 Prüfung des tolerierbaren Risikos (ZCR 4)

Nun muss überprüft werden, ob das initial bestimmte Risiko aus Kapitel 6.5 (ZCR 2) das tolerierbare Risiko des Betreibers oder der Annahmen übersteigt. Sollte dies der Fall sein, so muss eine detaillierte Cyber Security Risikobewertung durchgeführt werden, um das Risiko auf ein niedrigeres oder gleiches Niveau mit dem tolerierbaren Risiko zu bringen. Ist das initiale Risiko geringer oder gleichgroß wie das tolerierbare Risiko, kann die detaillierte Cyber Security Risikobewertung übersprungen werden und bei Kapitel 6.9 fortgefahren werden, da es kein Bedarf gibt das Risiko weiter zu senken. In dem Fall ist die Maschine initial bereits ausreichend abgesichert. Die Prüfung kann dabei anhand einer Tabelle erfolgen, zusehen in Anhang 7.

6.8 Durchführung einer detaillierten Cyber Security Risikobewertung (ZCR 5)

Die detaillierte Cyber Security Risikobewertung, zusehen in Bild 28 besteht aus 13 Teilprozessen und dient dazu, die Sicherheit des Systems maßgeblich zu erhöhen. Hierbei ist es ebenfalls unerlässlich alle Schritte umfangreich zu dokumentieren.

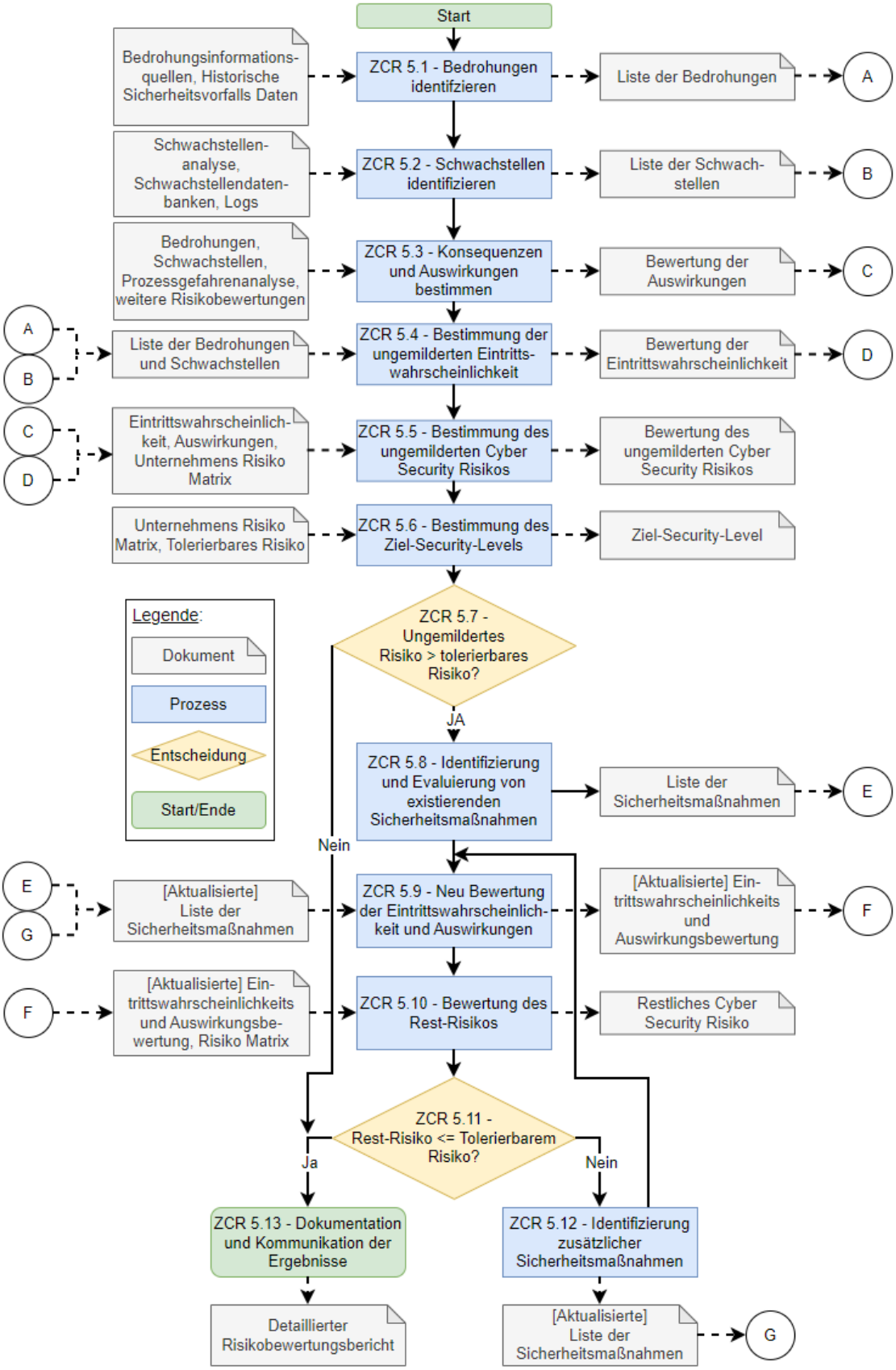


Bild 28: Prozess der detaillierten Cyber Security Risikobewertung

Quelle: Eigene Darstellung nach IEC-62443-3-2 [35, p. 23]

Um eine effektive Cyber Security Risikobewertung sicherzustellen, sollte ein Moderator hinzugezogen werden, welcher weder beim Design, noch bei der Umsetzung des Systems involviert war und wenn möglich eine Weiterbildung für die Durchführung von Risikobewertungen durchlaufen hat. Zusätzlich benötigt es ein Team aus verschiedenen qualifizierten Personen, wie:

- Moderator
- Schriftführer
- Automatisierungsingenieur
- Netzwerkingenieur
- Cyber Security Fachexperte
- Safety Fachexperte
- Bediener mit Erfahrungen zum Prozess des Systems

Zusätzlich sollten wichtige Informationen zum Beginn der detaillierten Cyber Security Risikobewertung zur Verfügung stehen. Dabei empfehlen sich die Informationen aus Kapitel 6.3.2.

6.8.1 Identifizierung von Bedrohungen (ZCR 5.1)

Die Identifikation von Bedrohungen dient dazu mögliche Szenarien in Bezug auf einen Angriff auf das Automatisierungssystem besser bewerten zu können. Es gibt dabei in der Praxis verschiedene Möglichkeiten Bedrohungen zu identifizieren. Eine sehr umfangreiche Möglichkeit ist die Hinzunahme des in Kapitel 5.4 erstellten Bedrohungskatalog. In dieser sind verschiedene Bedrohungsszenarien speziell auf IACS mit entsprechenden Anmerkungen zum Vorgang, Beispielszenarien, betroffenen Geräten und Sicherheitsmaßnahmen zu finden. Damit können Bewertungen an ausgewählten Bedrohungsszenarien, welche auf das System zutreffen, erstellt werden.

Bei der Dokumentation der Bedrohungen sollten mindestens folgende Informationen beachtet werden:

- Beschreibung der Bedrohungsquelle
- Beschreibung des Fähigkeitsniveaus der Bedrohungsquelle
- Beschreibung möglicher Bedrohungsvektoren
- Identifizierung möglicher betroffener Komponenten

Weitere Informationen wie eine ausführliche Beschreibung, betroffene Zonen oder interne Zuständigkeiten für diese Bedrohungen sind nicht verpflichtend, allerdings empfehlenswert. Ein Beispiel einer Bedrohungsanalyse ist in Anhang 8 zusehen.

6.8.2 Identifizierung von Schwachstellen (ZCR 5.2)

Bei der Identifizierung von Schwachstellen (nachfolgend Schwachstellenanalyse genannt) geht es darum bereits vorhandene Eintrittstore für Angriffe aufzuspüren, um diese in der Risikobewertung zu berücksichtigen und später zu schließen. Mit der Information welche Schwachstellen vorhanden sind, als auch welche Schwachstellen die Systeme im Allgemeinen betreffen oder betroffen haben, lassen sich mögliche Konsequenzen aber auch Maßnahmen ableiten.

Die Schwachstellenanalyse kann dabei über zwei Methoden realisiert werden, der passiven oder aktiven Schwachstellenanalyse. Bei der passiven Schwachstellenanalyse erhält man Informationen aus Schwachstellen-Datenbanken, wie dem CVE – Common Vulnerabilities and Exposures, Log-Files, Herstellerinformationen, Betriebsanleitungen, Code-Reviews, Dokumentations-Analysen (Netzwerkverkehr, Netzwerkdiagramme), Prüfungen von Konfigurationen oder Informationsaustausche mit anderen Unternehmen und Einrichtungen.

Bei der aktiven Schwachstellenanalyse wird das Netzwerk, durch aktive Programme wie beispielsweise Nmap oder Superscan, auf Kommunikationsteilnehmer gescannt. Auch das aktive Scannen nach Schwachstellen durch Schwachstellenscanner wie OpenVAS oder Nessus fallen

in die Kategorie der aktiven Schwachstellenanalyse. Dabei wird nach Kommunikationsteilnehmern gesucht, Informationen von diesem eingeholt, wie Betriebssystem, Firmware und offene Ports. Diese Informationen werden mit einer Schwachstellen-Datenbank abgeglichen, um darüber mögliche aktive Schwachstellen zu finden.

Im erstellten Katalog der Prüftools- und Verfahren in Kapitel 5.3.1, sind dabei verschiedene Vorgehen und Tools beschrieben, welche zur Schwachstellenanalyse dienen. Ein Beispiel der Schwachstellenanalyse ist in Anhang 9 zusehen.

6.8.3 Bestimmung der Konsequenzen und Auswirkungen (ZCR 5.3)

Um das Risiko zu bestimmen, muss der Faktor der Konsequenzen und Auswirkungen beachtet werden. Dabei werden allerdings nur die Worst-Case-Szenarien von Konsequenzen zu jeder identifizierten Bedrohung in Verbindung mit Überkategorien wie beispielsweise Personensicherheit, Finanzieller Schaden, Produktionsunterbrechung, Imageschäden und Umweltschäden berücksichtigt. Die Auswirkungen stellen diese Konsequenzen entweder qualitativ (bspw. reparable oder irreparable Personenschäden) oder quantitativ (eine oder mehrere verletzte Personen) dar. Dabei kann eine einheitliche Konsequenzen-Skala des Betreibers genommen werden, oder andernfalls die angenommenen Dokumente aus Kapitel 6.3. Eine Beispiel-Bestimmung der Konsequenzen und Auswirkung in Anhang 10 abliegt.

6.8.4 Bestimmung der ungemilderten Eintrittswahrscheinlichkeit (ZCR 5.4)

Zu jeder Bedrohung sollte die ungemilderte Eintrittswahrscheinlichkeit bestimmt werden. Dabei können auch die gefunden Schwachstellen hinzugezogen werden, um die Wahrscheinlichkeit genauer bestimmen zu können. Ungemildert bedeutet hierbei, dass keine zusätzlichen Sicherheitsmaßnahmen berücksichtigt werden, die Bedrohung also direkt und ungemildert das System trifft. Die Bestimmung der Eintrittswahrscheinlichkeiten berücksichtigt dabei vor Allem

Zeitperioden, in denen die Bedrohung eintreten könnte oder mit welcher Häufigkeit solch eine Bedrohung realistisch ist.

Um die Bestimmung der Eintrittswahrscheinlichkeit zu erleichtern, hat das Nationale Cyber Security Centrum (Nationaal Cyber Security Centrum) der Niederlande die „Inschalingsmatrix“ erstellt. Diese Matrix stellt zehn Fragen, welche für jede Bedrohung mit drei unterschiedlichen Optionen beantwortet werden kann. Abhängig von den ausgewählten Optionen, wird dabei die Höhe Eintrittswahrscheinlichkeit bestimmt [37]. Ein Beispiel der „Inschalingsmatrix“ ist in Anhang 11 zu finden.

6.8.5 Bestimmung des ungemilderten Cyber Security Risikos (ZCR 5.5)

Durch die ermittelten Auswirkungen aus Kapitel 6.8.3 und der ermittelten Eintrittswahrscheinlichkeit aus Kapitel 6.8.4 sind beide Faktoren fürs Risiko vorhanden. Damit wird nun das ungemilderte Cyber Security Risiko für jedes Bedrohungsszenario bestimmt. Dadurch erhält man Informationen darüber, wie anfällig die Maschine, bzw. wie hoch das Risiko für die einzelnen Bedrohungsszenarien ohne zusätzliche Sicherheitsmaßnahmen sind. Zur Bestimmung kann hierbei die Risikomatrix verwendet werden, zusehen in Anhang 3.

6.8.6 Bestimmung des Ziel-Security-Levels (ZCR 5.6)

Mit dem Wissen über das ungemilderte Risiko in Verbindung mit den Unternehmensrichtlinien und des tolerierbaren Risikos wird für jede Zone und jeden Kanal ein eigenes SL-T bestimmt. Fehlen vom Betreiber Informationen und wird mit Annahmen gearbeitet, so wird in diesem Teil ein SL-C für Zonen und Kanäle bestimmt welches mit den getroffenen Annahmen erreichbar sein soll.

6.8.7 Prüfung der Einhaltung des tolerierbaren Risikos (ZCR 5.7)

Nachdem das ungemilderte Cyber Security Risiko in Kapitel 6.8.5 bestimmt wurde, muss dieses nun mit dem tolerierbaren Risiko verglichen werden. Je nach tolerierbarem Risiko könnte das ungemilderte Risiko geringer sein als das

tolerierbare Risiko. In diesem Fall würden keine weiteren Sicherheitsmaßnahmen benötigt werden wodurch direkt in Kapitel 6.8.13 mit der Dokumentation und Kommunikation der Ergebnisse fortgesetzt werden kann. Sollte das ungemilderte Risiko höher als das tolerierbare Risiko sein, kann das Risiko entweder akzeptiert, gemildert oder transferiert werden. Bei der Akzeptanz ist wichtig zu dokumentieren auf welcher Grundlage diese Entscheidung getroffen wird. Beim Transfer des Risikos könnte das übrige Risiko beispielsweise durch Cyber Security Versicherungen angegangen werden. In dem Fall wird das Risiko toleriert da im Falle eines Eintretens die Versicherung die Konsequenzen übernimmt. Am empfehlenswertesten ist jedoch das Risiko weiter zu mildern, in Form von weiteren Sicherheitsmaßnahmen.

6.8.8 Identifizierung und Evaluierung existierender Sicherheitsmaßnahmen (ZCR 5.8)

Bisher wurde lediglich das ungemilderte System betrachtet. Um das Risiko weiter zu senken, werden nun die bisher implementierten Sicherheitsmaßnahmen des Systems betrachtet. Dabei kann es sich um existierende Segmentierungen, vorhandene Sicherheitsimplementierung in Komponenten oder verwendete standardisierte Protokolle handeln. Auch die Schwachstellenanalyse liefert gute Grundlagen über die Eigenschaften der Systeme und vorhanden Sicherheitsmaßnahmen (Aktuelle Firmware, sichere verwendete Protokolle, Segmentierung).

Um die Sicherheitsmaßnahmen zu evaluieren, können die Prüftools aus Kapitel 5.3.1 verwendet werden.

6.8.9 Neubestimmung der Eintrittswahrscheinlichkeit und Auswirkung (ZCR 5.9)

Mit den identifizierten, existierenden Sicherheitsmaßnahmen im System, sinkt das Risiko. Dieses neue Risiko bedarf einer Neubestimmung der Eintrittswahrscheinlichkeiten und Auswirkungen. Durch bestimmte Sicherheitsmaßnahmen wie gehärtete Komponenten, aktuelle

Firmwareversionen und Virenscanner oder umfangreiche Zugriffsrechte, kann die Eintrittswahrscheinlichkeit stark reduziert werden. Diese wird daher, wie in Kapitel 6.8.4, neubestimmt. Ebenfalls können andere Sicherheitsmaßnahmen die Auswirkungen eines Angriffs senken, so zum Beispiel strengere Segmentierungen, physikalische Standorte von Systemen oder fehlersichere Komponenten, die dafür sorgen, dass die Auswirkungen ebenfalls neu bestimmt werden müssen.

6.8.10 Bestimmung des Restrisikos (ZCR 5.10)

Mit den neubestimmten Eintrittswahrscheinlichkeiten und Auswirkungen wird nun das verbleibende Risiko bestimmt, welches Restrisiko genannt wird. Das Restrisiko ist jenes Risiko, welches verbleibt, wenn die Sicherheitsmaßnahmen des Systems greifen würden. Mit dem Restrisiko hat man damit eine erste Aussage über die tatsächliche Sicherheit des Systems. Hierzu kann die Rest-Risikobewertung in Anhang 12 verwendet werden.

6.8.11 Prüfung der Konformität zwischen Restrisiko und tolerierbarem Risiko (ZCR 5.11)

Ist das Restrisiko mit den bereits implementierten Sicherheitsmaßnahmen dennoch nicht ausreichend und höher als das tolerierbare Risiko, so ist das System nicht abgesichert genug. Ist das Restrisiko allerdings kleiner gleich dem tolerierbaren Risiko, bedeutet dies, dass das System ausreichend abgesichert ist. In dem Fall kann mit Kapitel 6.8.13 weiter gemacht werden, andernfalls mit Kapitel 6.8.12.

6.8.12 Identifizierung zusätzlicher Sicherheitsmaßnahmen (ZCR 5.12)

Sollte das Restrisiko höher sein als das tolerierbare Risiko, müssen weitere Sicherheitsmaßnahmen identifiziert werden, um das Risiko weiter zu senken. Hierfür steht der Katalog aus Kapitel 5 bereit. In ihm sind verschiedene Sicherheitsmaßnahmen aufgelistet und beschrieben. Diese können verwendet werden, um die Sicherheit weiter zu erhöhen und dementsprechend das Risiko

zu senken. Durch die Neubestimmung der Eintrittswahrscheinlichkeiten und Auswirkungen aus Kapitel 6.8.9 wird unter anderem ersichtlich, in welchen Punkten noch weiterer Bedarf an Sicherheitsmaßnahmen von Nöten ist. Auch die Evaluierung von existierenden Sicherheitsmaßnahmen aus Kapitel 6.8.8, den Schwachstellenanalyse aus Kapitel 6.8.2 sowie den Bedrohungsanalysen aus Kapitel 6.8.1, dienen als Grundlage, um Defizite in der Cyber Security zu finden und entsprechend weitere Maßnahmen zu ergreifen. Des Weiteren können auch die SL-Cs betrachtet werden. Soll ein gewisses SL-C erreicht werden, so benötigt man die entsprechend erfüllten SRs und REs, welche wiederum weitere Vorgaben an spezifischen Sicherheitsmaßnahmen vorgeben.

Nach der Implementierung der neuen Sicherheitsmaßnahmen müssen die Prozesse ab der Neubestimmung der Eintrittswahrscheinlichkeit und Auswirkung in Kapitel 6.8.9 wiederholt werden, solange, bis das Restrisiko kleiner gleich dem tolerierbaren Risiko ist oder das Restrisiko transferiert oder akzeptiert wird.

6.8.13 Dokumentation und Kommunikation der Ergebnisse (ZCR 5.13)

Abschließend müssen alle Ergebnisse dokumentiert werden. Dabei sollte ein Großteil der Dokumentation bereits während der Durchführung der detaillierten Cyber Security Risikoanalyse entstanden sein. Diese sollte aber nochmals auf Vollständigkeit geprüft werden. Hinzu kommen die Ablage und Bereitstellung der Dokumente für die entsprechenden Fachkreise sowie die Kommunikation der Ergebnisse, sowohl intern an die Fachkreise, bspw. welche Sicherheitsmaßnahmen noch implementiert werden müssen, als auch an externe Personen wie dem Betreiber, um diesen über das Vorgehen und die Ergebnisse zu informieren.

6.9 Dokumentation der Cyber Security Anforderungen, Annahmen und Einschränkungen (ZCR 6)

Nun muss der gesamte Cyber Security Risikobewertungsprozess dokumentiert werden. Daraus entsteht die sogenannte Cyber Security Requirements Specification (CRS). In dieser sollten alle Informationen, die während der gesamten Risikobewertung angefallen sind, enthalten sein. Mindestens aber folgende:

- Beschreibung des SuC
- Zonen und Kanäle Charakteristiken
- Annahmen zur Betriebsumgebung
- Bedrohungsumgebung/ -abschätzung
- Sicherheitsrichtlinien des Unternehmens
- Tolerierbares Risiko
- Regulatorische Anforderungen

Beschreibung des SuC:

Bei der Beschreibung des SuC geht es darum, das betrachtete System klar zu definieren, um dabei den Rahmen der gesamten Betrachtung der Cyber Security Risikobewertung festzulegen und später nachvollziehbar zu haben. Dabei sollte die Beschreibung des SuC folgendes umfassen:

- Name des SuC / Name der Maschine
- Grobe Beschreibung des Systems
- Bestimmungsgemäße Verwendung
- Architektur Diagramme
- Netzwerk Diagramme
- Sicherheitsbereiche und Zugriffspunkte
- Systeminventar
- Datenflüsse
- Prozessabläufe

Zonen und Kanäle Charakteristiken:

Für die Dokumentation der Charakteristiken der Zonen und Kanälen, sollte diese Dokumentation pro Zone und pro Kanal vorliegen und dabei mindestens folgende Informationen enthalten:

- Verantwortliche Abteilung
- Beschreibung der logischen Grenzen
- Beschreibung der physischen Grenzen
- Safety-Kennzeichnungen
- Verbundene Zonen und Kanäle
- Ziel-Security Level
- Anwendbare SRs
- Anwendbare Sicherheitsrichtlinien
- Annahmen und externe Abhängigkeiten
- Logische Zugriffspunkte
- Physische Zugriffspunkte
- Datenflüsse
- Inventarisierung der Komponenten

Die restlichen benötigten Inhalte sind in Anlage 1, der Cyber Security Requirements Specification, zu finden.

6.10 Einholung der Bestätigung des Betreibers (ZCR 7)

Zum Schluss geht aus dem Cyber Security Risikobewertungsprozess hervor dass eine Einholung der Bestätigung des Betreibers nötig wird. Dies dient dazu, den gesamten Prozess und Dokumentation vom Betreiber zu bestätigen. In dieser Arbeit wird die Einholung jedoch in das Abnahmeprotokoll in Kapitel 7 ausgelagert.

7 Erstellung des Abnahmeprotokolls

Das Abnahmeprotokoll soll dazu dienen, beim Ausliefern einer Maschine oder Anlage dem Kunden alle Maßnahmen, Sicherheitsniveaus und Maschineninformationen zur Verfügung zu stellen, um diesem die normative Konformität mit der IEC-62443 auszuweisen. Letztere ist damit nicht gleichbedeutend mit einer Zertifizierung, sondern vielmehr als Selbstauskunft, wie bei der CE-Kennzeichnung, zu verstehen.

Um ein aussagekräftiges Abnahmeprotokoll erstellen zu können, werden viele verschiedene Informationen benötigt. Dazu zählen grundlegende Informationen über das Unternehmen, welche die Maschine oder Anlage gebaut hat, allgemeine Informationen zur Maschine oder Anlage, die Implementierung des Katalogs und dadurch eine Auflistung der implementierten Sicherheitsmaßnahmen, das Hinzufügen der Test-Ergebnisse der Prüfverfahren zur Validierung der Sicherheitsmaßnahmen und abschließend die Cyber Security Risikobewertungsdokumentation.

7.1 Erstellung grundlegender Informationen

Zu Beginn des Protokolls müssen grundlegende Informationen über den Integrator dokumentiert werden. Dies dient zum einen als Information für den Betreiber weitergehend aber auch, um konform mit den gesetzlichen Anforderungen, wie die Ausweisungspflicht aus 3.1.1, zu sein. Die grundlegenden Informationen, welche erarbeitet wurden, sind in Bild 29 zusehen.

Abnahmeprotokoll

für sichere Maschinen

Grundlegende Informationen:

	Maschinenbauer	Abnehmer / Kunde
Handelsname/ - marke	Musterbau AG	Kunden AG
Postanschrift	Musterstraße 10 00000 Musterstadt	Kundenstraße 1 00000 Kundenstadt
Kontakt	mustermann@musterbau.com	Kundenmann@kunden.com
Website	www.musterbau.com	www.kunden.com

Maschineninformationen:

Typ	Nummer	Baujahr
Beispiel-Typ	XXXXXXXXX	2024
BeispielNameDerMaschine		

Meldestelle für Sicherheitsvorfälle:

Kontakt	security@musterbau.com
Security-Advisory	www.musterbau.com/security

Bild 29: Grundlegende Informationen des Abnahmeprotokolls

Quelle: Eigene Darstellung aus Anlage 3

7.2 Implementierung der Cyber Security Risikobewertungsdokumentation

Im Abnahmeprotokoll sollte auch die komplette Cyber Security Risikobewertungsdokumentation enthalten sein. Dies ist wichtig, um nachzuweisen, dass ein risikobasierter Ansatz zur Erhöhung der Sicherheit der Maschine angewendet wurde. Ebenso stehen darin die verschiedenen Annahmen und Rahmenbedingungen, welche betrachtet wurden.

Im Abnahmeprotokoll selbst wird die Cyber Security Risikobewertung nicht als Ganzes implementiert. Vielmehr ist eine Checkbox hinterlegt, welche angekreuzt werden kann, wenn die Cyber Security Risikobewertungsdokumentation im

Anhang oder als Anlage beigefügt ist. Zusätzlich zur Checkbox sind einige wenige, aber prägnante Informationen aus der Cyber Security Risikobewertungsdokumentation zu hinterlegen. Dazu zählen die in Bild 30 zusehenden Informationen.

Cyber Security Risikobewertung:

☐ Cyber Security Risikobewertung wurde durchgeführt

☐ Cyber Security Risikobewertungsdokumentation wurde beigefügt

Tolerierbares Risiko	SL-C der Maschine	Durchgeführt von
10 / SL-2	SL-C 2	MusterPrüfer
dd.mm. jjjj	Musterstadt	
Am	Ort	Unterschrift

Bild 30: Bestätigung der Cyber Security Risikobewertung

Quelle: Eigene Darstellung aus Anlage 3

Um zu gewährleisten, dass der Maschinenbauer keine essenziellen Schritte vergessen hat, wurde zudem eine Checkliste implementiert. Zusätzlich wurde eine Tabelle erstellt, zusehen in Bild 31, in welche die „Verzeichnisse/Links“ zu den entsprechenden Dokumentationen hinterlegt werden können und durch eine Checkbox ebenfalls das Vorhandensein der Dokumentationen zu bestätigen.

Cyber Security Risikobewertungs-Checkliste:

☐ Grundlagen Informationen vollständig

☐ Inventarisierungsliste erstellt

☐ Initiale Risikobewertung durchgeführt max. initiales Risiko: _____

☐ Tolerierbares Risiko wurde vorgegeben Tolerierbares Risiko: _____

☐ Bedrohungsanalyse durchgeführt

☐ Schwachstellenanalyse durchgeführt

☐ Auswirkungsbestimmung durchgeführt

☐ Eintrittswahrscheinlichkeiten bestimmt

☐ Rest-Risiko bewertet Rest-Risiko: _____

☐ Tolerierbares Risiko erreicht

Dokumentationen-Verzeichnis:

Dokumentation	Abgelegt unter	
Architekturdiagramme	XXX	☐
Netzwerkdiagramme	XXX	☐
Handbücher	XXX	☐
Prozessbeschreibungen	XXX	☐
Datenflussdokumentation	XXX	☐
Sicherheitsrichtlinien	XXX	☐
		☐

Bild 31: Checkliste zur Cyber Security Risikobewertung

Quelle: Eigene Darstellung aus Anlage 3

7.3 Implementierung der Kataloge

Auch die Kataloge sollten ins Abnahmeprotokoll implementiert werden. Zumindest muss aus dem Protokoll hervorgehen, welche Sicherheitsmaßnahmen aus den Katalogen verwendet wurden, um die Sicherheit zu erhöhen. Hierzu wird auf GitBook [21] der Download der Tabelle, mit entsprechenden Checkboxen zu den einzelnen Sicherheitsmaßnahmen, ermöglicht. Darin kann angekreuzt werden, welche Sicherheitsmaßnahmen implementiert sind. Mit dem Verweis auf den Katalog und der Umsetzungsbeschreibung ist zudem belegt, wie die Konfiguration durchgeführt wurde und dient damit gleichzeitig als Nachweis. Die Bestätigungen, dass die Tabellen vorhanden sind, erfolgt ebenfalls über eine kleine Tabelle, zusehen in Bild 32.

Implementierte Maßnahmen:

Dokumentation	Abgelegt unter	
Technische Maßnahmen	XXX	☐
Organisatorische Maßnahmen	XXX	☐
Grundlegende Maßnahmen	XXX	☐

Bild 32: Bestätigung der Implementierung der Kataloge

Quelle: Eigene Darstellung aus Anlage 3

7.4 Implementierung der Test-Ergebnisse der Prüfverfahren

Um die Funktionalität der Sicherheitsmaßnahmen zu validieren, sollten auch die Test-Ergebnisse der Prüftools und Prüfverfahren ins Protokoll aufgenommen werden. Dadurch kann gewährleistet werden, dass die vorgesehenen Sicherheitsmaßnahmen zum Zeitpunkt der Auslieferung funktionsfähig waren und der Integrator damit seinen Pflichten nachkam. Die Dokumentationen der einzelnen Prüftools- und Verfahren, bzw. den Messergebnissen dieser, müssen beim Abnahmeprotokoll mitgegeben werden. Über eine weitere Checkbox, in der in Kapitel 7.3 erwähnten Tabelle der Sicherheitsmaßnahmen, kann gezeigt werden, für welche Sicherheitsmaßnahmen Prüfverfahren oder Tools zur Validierung eingesetzt wurden. Hier kann dann der Dokumentenname der

Messerergebnisse hinterlegt werden, um eine genaue Zuordnung zu ermöglichen. Im Abnahmeprotokoll direkt, wird ebenfalls eine Tabelle verwendet, um das Vorhandensein der Dokumentationen zu gewährleisten, zusehen in Bild 33. Hierbei sollten alle Dokumentationen zu den einzelnen geprüften Sicherheitsmaßnahmen abgelegt werden.

Prüfverfahren- und Tools:

Dokumentation	Abgelegt unter	
Prüfungsdokumentationen	XXX	☐

Bild 33: Bestätigung der Durchführung der Prüfverfahren

Quelle: Eigene Darstellung aus Anlage 3

7.5 Bestätigung des Betreibers

Zu guter Letzt, muss der Betreiber das gesamte Vorgehen des Maschinenbauers, sowie die Sicherheit der Maschine bestätigen. Mit einer Unterschrift soll damit die Sicherheit der Maschine endgültig abgenommen werden. Dafür entstand ein Unterschriftenfeld, zusehen in Bild 34.

Bestätigung des Betreibers:

Der Betreiber bestätigt, dass der Maschinenbauer die Sicherheit nach bestem Wissen und Gewissen bewertet hat. Er bestätigt, dass ihm die vorliegende Dokumentation als Nachweis dient und die Sicherheit der Maschine damit abgenommen wird.

_____ _____

Datum Unterschrift

Bild 34: Bestätigung des Betreibers

Quelle: Eigene Darstellung aus Anlage 3

8 Validierung durch externes Fachpersonal

Um die Inhalte und die Vorgehensweise der vorliegenden Arbeit validieren zu können, wurde ein Interview mit Dr.-Ing. Christian Haas durchgeführt. Herr Haas ist Gruppenleiter für die „Industrielle Cybersicherheit“ am Fraunhofer-Institut für Optronik, Systemtechnik und Bildverarbeitung (IOSB). Nebenbei ist Herr Haas tätig als „Qualified Instructor“ der IEC-62443, ausgestellt von der ISA, wodurch er sich ebenfalls gut mit der Norm auskennt.

Die Transkription des Interviews ist in Anlage 2 aufgeführt.

Herr Haas konnte im Interview bestätigen, das die Industrie mit den kommenden Regulatorien viel Arbeit haben wird. Zum einen durch die Erfüllung der Anforderungen, zum anderen aber auch, da davon auszugehen ist dass die Regulatorien sich auch jährlich anpassen könnten, wodurch Unternehmen immer wieder nachschärfen müssen. Herr Haas stellt zudem fest, dass der Implementierungsgrad an Sicherheitsmaßnahmen in der Industrie sehr heterogen ist. Es gibt Unternehmen, die schon sehr viel gemacht haben, andere wiederum fangen gerade erst an [38].

In Bezug auf den Stand der Technik und wie man Informationen zu konkreten Sicherheitsmaßnahmen ableiten kann sagt Herr Haas: „Naja, ich glaube da hilft auch manchmal Google benutzen […]. Ich glaube hier gibt es mittlerweile sehr sehr viele Quellen […] es gibt so viele und dann sich zu entscheiden, was genau macht man jetzt ist dann das größere Problem, weil ich glaube es gibt einfach zu viele Standards und zu viele Informationen dazu […]“ [38]. Hier wäre es also von Vorteil, wenn genau eine Quelle existiert, in der man diese verschiedenen Informationen einheitlich finden kann.

Ebenfalls konnte Herr Haas bestätigen, dass das Vorgehen der IEC-62443-3-2 zur Bewertung der Sicherheit der Maschine über den Cyber Security Risikobewertungsprozess der richtige Ansatz ist. Allerdings fügt er hinzu, dass dies ohne den Betreiber eigentlich nicht möglich sei, da schließlich zu viele Informationen vom Betreiber benötigt werden um hier als Maschinenbauer eine

eigene Bewertung durchführen zu können. Diese Aussage korrigiert er später, im Kontext der Annahmen, die der Maschinenbauer treffen kann und sagt: „Das kann man machen, und das macht insbesondere dann Sinn, wenn es keine Sondermaschinen sind, sondern wenn das Maschinen sind, die immer sehr ähnlich aufgebaut sind. Dann kann man eine Standardmaschine definieren und es (die Risikobewertung) dafür machen. Aber das entbehrt einen nicht davon dass man als Betreiber nochmal verifizieren muss dass die Annahmen stimmen […]“ [38].

Das Interview bestätigt die Problemstellung der vorliegenden Arbeit. Zusätzlich wird durch das Interview der Inhalt, das Vorgehen und die Notwendigkeit dieser Arbeit validiert. Abschließend kann man Herr Haas zitieren, um den Nutzen der Arbeit zu bekräftigen, denn den Umsetzungsleitfaden „Glaube ich würden sehr viele Leute dankbar annehmen, weil eben hier auch sehr viel Unsicherheit besteht, wie man sowas machen soll. Von daher glaube ich, würden viele Leute sich Das anschauen. Gegebenenfalls adaptieren wenn Sachen doch speziell anders sein müssen, aber das könnte sehr hilfreich sein für viele Maschinenbauer“ [38].

9 Fazit

Das Ziel dieser Arbeit war die Erstellung eines Umsetzungsleitfaden informationstechnischer Sicherheitsmaßnahmen für Maschinen anhand der IEC-62443, wobei der Fokus dabei auf den allgemeinen Maschinenbau gelegt wurde. Dazu wurden zu Beginn rechtliche und normative Grundlagen erläutert, ehe konkrete Anforderungen aus den Gesetzen und Normen analysiert wurden und geprüft wurde, inwieweit die normativen Anforderungen den Rechtlichen gerecht werden.

Anschließend wurde eine Einführung in den Umsetzungsleitfaden gegeben mit Informationen darüber, was in ihm enthalten ist und wie dieser anzuwenden ist. Mit dem darauffolgenden Kapitel wurden, die für den Leitfaden essenziellen, Kataloge erstellt. Darunter Kataloge mit technischen und organisatorischen Maßnahmen zur Erhöhung der Sicherheit von Systemen, einem Katalog für Prüftools und -verfahren zur Validierung der Sicherheitsmaßnahmen und einen Katalog in dem grundlegende Bedrohungsszenarien aufgelistet sind. Ein weiterer Katalog, der grundlegende Katalog, beschreibt zudem weitere Anforderungen, welche so nicht durch die Norm abgedeckt, für die rechtliche Konformität aber bedeutend sind.

Nach dem mit den Katalogen die Grundlagen des Umsetzungsleitfadens geschaffen waren, ging es dann an die Durchführung des Cyber Security Risikobewertungsprozess der IEC-62443-3-2, als zentrales risikobasiertes Vorgehen zur Bewertung und Erhöhung der Sicherheit des Systems. Die Arbeit erklärt dabei den gesamten Prozess aus der Norm, mit Best-Practices, konkreten Empfehlungen sowie Begleitdokumente, welche die Durchführung erleichtern sollen.

Im Anschluss daran wurde ein Abnahmeprotokoll erstellt, welcher die gesamten Dokumentationen, Annahmen, Rahmenbedingungen und Durchführungsbeschreibungen beinhaltet, als Checkliste dient und dem Betreiber die Sicherheit der Maschine bestätigt, sowie die Bestätigung zur Abnahme der Sicherheit der Maschine des Betreibers einholt.

Um den Inhalt und die Vorgehensweise der Arbeit validieren zu können, wurde ein Interview mit externem Fachpersonal durchgeführt. Dieser konnte sowohl den Inhalt der Arbeit als auch deren Nutzen bestätigen.

Die Arbeit hat damit das Fundament für den Umsetzungsleitfaden gelegt. Abgeschlossen ist der Umsetzungsleitfaden nicht, kann dieser aber auch nicht sein! Die gesetzlichen Anforderungen müssen fortlaufend überarbeitet werden, da die Arbeit nur die bis dahin veröffentlichten Entwürfe des NIS2UmsuCG und dem CRA betrachten konnte. Zusätzlich müssen die Kataloge mit weiteren Maßnahmen und Szenarien gefüllt werden und zu den existierenden Maßnahmen Umsetzungsbeschreibungen erstellt werden. Die existierenden Umsetzungsbeschreibungen müssen zudem in einem kontinuierlichen Zyklus auf die Aktualität in Verbindung mit dem „Stand der Technik“ überprüft und gegebenenfalls erweitert werden.

Zusätzlich fehlt eine Zuordnung der verschiedenen SRs zu den technischen und organisatorischen Maßnahmen der Kataloge. Dies würde die Arbeit mit dem Umsetzungsleitfaden ebenfalls erleichtern, da bei einem SL-T bzw. SL-C, das erreicht werden soll, die entsprechenden SRs welche benötigten werden, anhand der Sicherheitsmaßnahmen der Kataloge ausgewählt werden können.

Als weitere zukünftige Arbeit in Verbindung mit dieser Master-Thesis könnte der gesamte Umsetzungsleitfaden, in Form eines Programmes, teilautomatisiert werden. Dadurch kann der bisherige hohe manuelle Dokumentationsaufwand stark minimiert werden.

V. Literaturverzeichnis

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI), „Die Lage der IT-Sicherheit in Deutschland 2023," Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 2023.

[2] Bundesamt für Sicherheit in der Informationstechnik, „Branchenlagebild Automotive. Cyber-Sicherheit in der Automobilbranche 2022/2023," Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2023.

[3] Bundeskriminalamt, „Cybercrime. Bundeslagebild 2023," Bundeskriminalamt, Wiesbaden, 2023.

[4] Bitkom e.V., „Bitkom zum Bundeslagebild Cybercrime," Bitkom e.V., 13 Mai 2024. [Online]. Available: https://www.bitkom.org/Presse/Presseinformation/Statement-Bundeslagebild-Cybercrime. [Zugriff am 16 August 2024].

[5] N. Pohlmann, Cyber-Sicherheit. Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung, 2. Auflage, Wiesbaden: Springer Vieweg, 2022.

[6] S. Luber, „Was ist DarkBart?," Security Insider, 6 Mai 2024. [Online]. Available: https://www.security-insider.de/was-ist-darkbart-a-4b2b436e3b04490f0b79fe5f9f0b0faf/?cflt=rel. [Zugriff am 16 August 2024].

[7] S. Luber, „Was ist FraudGPT," Security Insider, 30 April 2024. [Online]. Available: https://www.security-insider.de/was-ist-fraudgpt-a-f39f3d518d190218a37849140ae6bd63/?cflt=rel. [Zugriff am 16 August 2024].

[8] S. Luber, „Was ist WormGPT," Security Insider, 2 Mai 2024. [Online]. Available: https://www.security-insider.de/was-ist-wormgpt-a-5796962f97df6867e00e100c889e73bc/?cflt=rel. [Zugriff am 16 August 2024].

[9] European Commission, „Cybersecurity Policies," European Union, [Online]. Available: https://digital-strategy.ec.europa.eu/de/policies/cybersecurity-policies. [Zugriff am 19 August 2024].

[10] Computerwoche, „Mutation einer Geheimdienststelle. Sicherheitsdienste erobern neues Aufgabengebiet," Computerwoche, 23 März 1990. [Online]. Available: https://www.computerwoche.de/a/mutation-einer-geheimdienststelle. [Zugriff am 19 August 2024].

[11] Bundesamt für Sicherheit in der Informationstechnik, „Kurzprofil des BSI," Bundesamt für Sicherheit in der Informationstechnik, [Online]. Available: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/BSI-Kurzprofil/kurzprofil_node.html. [Zugriff am 19 August 2024].

[12] Bundesamt für Sicherheit in der Informationstechnik, „Auftrag," Bundesamt für Sicherheit in der Informationstechnik, [Online]. Available: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/auftrag_node.html. [Zugriff am 19 August 2024].

[13] Bundesamt für Sicherheit in der Informationstechnik, „Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)," Bundesamt für Sicherheit in der Informationstechnik, [Online]. Available: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html. [Zugriff am 19 August 2024].

[14] Bundesamt für Sicherheit in der Informationstechnik, „EU-Richtlinien zur Netzwerk- und Informationssicherheit," Bundesamt für Sicherheit in der

Informationstechnik, [Online]. Available: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/NIS-Richtlinien/nis-richtlinie_node.html. [Zugriff am 19 August 2024].

[15] European Commission, „The EU Cybersecurity Act,“ European Union, [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act. [Zugriff am 19 August 2024].

[16] European Commission, „The EU cybersecurity certification framework,“ European Union, [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework. [Zugriff am 19 August 2024].

[17] OpenKRITIS, „NIS2 Umsetzungsgesetz,“ OpenKRITIS, [Online]. Available: https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html. [Zugriff am 19 August 2024].

[18] S. Zimmermann, „NIS2UmsuCG - VDMA-Stellungnahme zum Diskussionspaper des BMI zur Umsetzung der NIS2-Richlinie in Deutschland,“ 2023. [Online]. Available: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/nis2umsucg.html. [Zugriff am 19 August 2024].

[19] Europäische Kommission, *Empfehlung der Kommision vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen,* Europäische Union, 2003.

[20] Bundesministerium des Innern und für Heimat, „Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung,“ 22 Juli 2024. [Online]. Available: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/nis2u

msucg.html. [Zugriff am 19 August 2024].

[21] M.-F. Beck, „Leitfaden zur Erhöhung der Security von Maschinen,“ [Online]. Available: https://umsetzungsleitfaden.gitbook.io/leitfaden-zur-erhohung-der-security-von-maschinen/.

[22] European Commission, „EU Cyber Resilience Act,“ European Commission, 8 Juli 2024. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act. [Zugriff am 5 September 2024].

[23] Europäische Kommission, *Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020,* Brüssel: Europäische Union, 2022.

[24] Deutsche Industrie und Handelskammer, „Cyber Resilience Act (CRA),“ Deutsche Industrie und Handelskammer, [Online]. Available: https://www.dihk.de/de/themen-und-positionen/wirtschaft-digital/dihk-durchblick-digital/cyber-resilience-act-cra--90956. [Zugriff am 19 August 2024].

[25] Europäische Union, *VERORDNUNG (EU) 2023/1230 DES EUROPÄISCHEN PARLAMENTS UND DES 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,* Brüssel: Europäische Union, 2023.

[26] V. Nicaise, „Stuxnet, welche Lehren lassen sich zwölf Jahre später ziehen?,“ Stromshield, 4 Juli 2022. [Online]. Available: https://www.stormshield.com/de/news/stuxnet-welche-lehren-lassen-sich-zwoelf-jahre-spaeter-ziehen/. [Zugriff am 5 September 2024].

[27] International Society of Automation, *ANSI/ISA-62443-1-1 (99.01.01)-2007. Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models,* Durham NC: International Society of Automation, 2007.

[28] International Society of Automation, *ANSI/ISA-62443-3-3 (99.03.03)-2013 Security for industrial automation and control systems Part 3-3: System security requirements and security levels,* Durham NC: International Society of Automation, 2013.

[29] International Society of Automation, *ANSI/ISA-62443-2-4-2018 / IEC 62443-2-4:2015+AMD1:2017 CSV, Security for industrial automation and control systems, Part 2-4: Security program requirements for IACS service providers (IEC 62443-2-4:2015+AMD1:2017 CSV, IDT),* Durham NC: International Society of Automation, 2018.

[30] International Society of Automation, *ANSI/ISA-62443-4-2-2018 Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components,* Durham NC: International Society of Automation, 2018.

[31] International Society of Automation, *ANSI/ISA-62443-2-1 (99.02.01)-2009 Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program,* Durham NC: International Society of Automation, 2009.

[32] International Society of Automation, *Using the ISA/IEC 62443 Standard to Secure Your Control Systems; IC32 Version 4.2.1 - Europe Edition,* International Society of Automation.

[33] Bundesamt für Sicherheit in der Informationstechnik, „Arbeitsbeispiel RECPLAST GmbH," Bundesamt für Sicherheit in der Informationstechnik, [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-

Grundschutz-Kompendium/Hilfsmittel-und-Anwenderbeitraege/Recplast/recplast_node.html. [Zugriff am 18 August 2024].

[34] The MITRE Corporation, „ICS Matrix,“ The MITRE Corporation, [Online]. Available: https://attack.mitre.org/matrices/ics/. [Zugriff am 18 August 2024].

[35] International Society of Automation, *ANSI/ISA-62443-3-2-2020 Security for industrial automation and control systems, Part 3-2: Security risk assessment for system design,* Durham NC: International Society of Automation, 2020.

[36] International Society of Automation, *ANSI/ISA-62443-4-1-2018 Security for industrial automation and control systems Part 4-1: Product security development life-cycle requirements,* Durham NC: International Society of Automation, 2018.

[37] Nationaal Cyber Security Centrum, „Inschalingsmatrix,“ Ministerie van Justitie en Veiligheid, 1 Januar 2017. [Online]. Available: https://www.ncsc.nl/documenten/publicaties/2019/juli/02/inschalingsmatrix. [Zugriff am 2024 September 10].

[38] C. Haas, Interviewee, *Interview zur IEC-62443.* [Interview]. 6 September 2024.

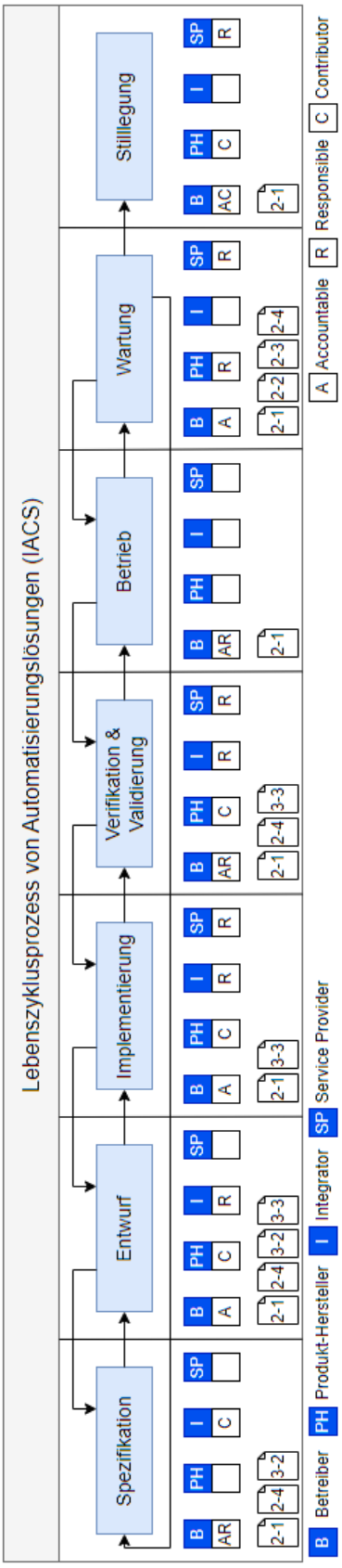
[39] International Society of Automation, *Using the ISA/IEC 62443 Standard to Secure Your Control Systems; IC32 Verson 4.2.1 - Europe Edition,* Durham NC: International Society of Automation, 2023.

VI. Bilderverzeichnis

VII. Tabellenverzeichnis

VIII. Anhangsverzeichnis und Anlagen

Anhang 1: Lebenszyklusprozess von IACS



Quelle: Eigene Darstellung nach [32]

Anhang 2: Sicherheitsanforderungen an Produkte mit digitalen Elementen

Produkte mit digitalen Elementen müssen, gemäß Anhang 1 Abschnitt 1 CRA [23]:

- Mit einer sicheren Standardkonfiguration ausgeliefert werden und die Möglichkeit bieten, das Produkt in seinen ursprünglichen Zustand zurückzusetzen
- Durch geeignete Kontrollmechanismen Schutz vor unbefugtem Zugriff bieten, darunter u. a. zumindest Authentifizierungs-, Identitäts- oder Zugangsverwaltungssysteme
- Die Vertraulichkeit gespeicherter, übermittelter oder anderweitig verarbeiteter personenbezogener oder sonstiger Daten schützen, z.B. durch Verschlüsselung relevanter Daten, die gespeichert sind oder gerade verwendet oder übermittelt werden, durch modernste Mechanismen
- Die Integrität gespeicherter, übermittelter oder anderweitig verarbeiteter personenbezogener oder sonstiger Daten, Befehle, Programme und Konfigurationen vor einer vom Nutzer nicht genehmigten Manipulation oder Veränderung schützen sowie deren Beschädigung melden
- Die Verarbeitung personenbezogener oder sonstiger Daten auf solche, die angemessen und relevant sind, und auf das für die bestimmungsgemäße Verwendung des Produkts erforderliche Maß beschränken („Datenminimierung“)
- Die Verfügbarkeit wesentlicher Funktionen, einschließlich der Abwehrfähigkeit gegen Überlastungsangriffe auf Server (Denial-of-Service-Angriffe) und deren Eindämmung gewährleisten
- Ihre eigenen negativen Auswirkungen auf die Verfügbarkeit der von anderen Geräten oder Netzen bereitgestellten Diensten minimieren
- So konzipiert, entwickelt und hergestellt werden, dass die Auswirkungen eines Vorfalls durch geeignete Mechanismen und Techniken zur Minderung der möglichen Ausnutzung verringert werden
- Sicherheitsbezogene Informationen durch Aufzeichnung und/oder Überwachung einschlägiger interner Vorgänge wie Zugang zu Daten, Diensten oder Funktionen und Änderungen daran bereitstellen

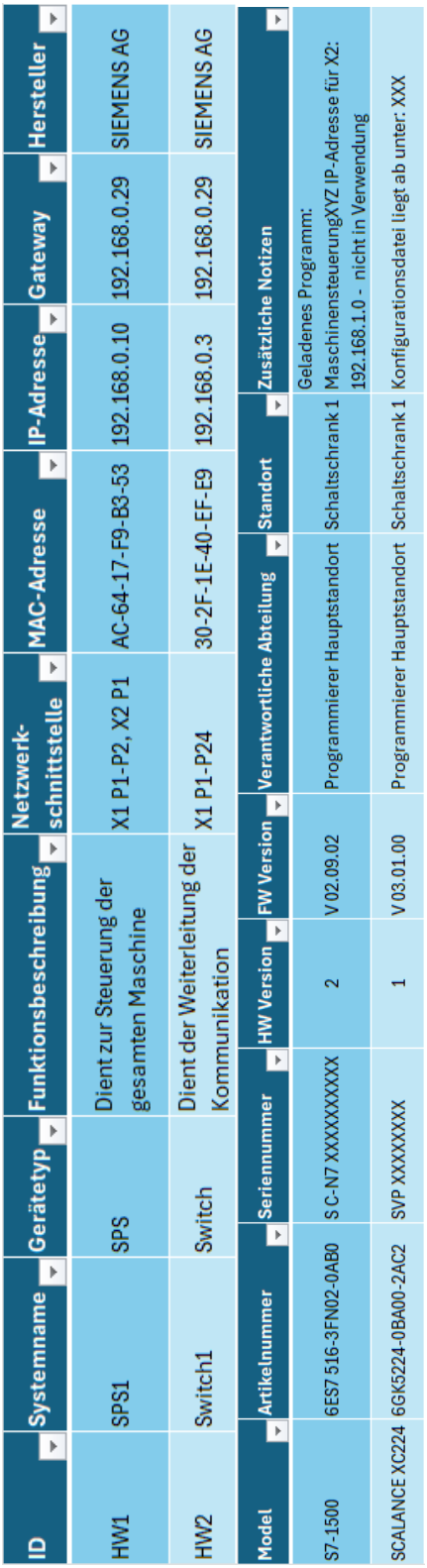
- Sicherstellen, dass Schwachstellen durch Sicherheitsaktualisierungen behoben werden können, gegebenenfalls auch durch automatische Aktualisierungen und die Benachrichtigung der Nutzer über verfügbare Aktualisierungen.

Anhang 3: Risikomatrix

							Eintrittswahrscheinlichkeit →				
					Wahrschein-lichkeit	Wahrschein-lichkeit	Praktisch unwahrscheinlich und unrealistisch	Denkbar möglich, aber sehr unwahrscheinlich	Ungewöhnlich, aber möglich	Durchaus möglich oder nicht ungewöhnlich	Tritt wahrscheinlich auf
					Häufigkeit	Häufigkeit	Das Ereignis könnte zu einem späteren Zeitpunkt als 10 Jahre eintreten	Das Ereignis könnte in 5 bis 10 Jahren eintreten	Ist aufgetreten oder wird voraussichtlich in 2 bis 5 Jahren auftreten	Ist aufgetreten oder wird voraussichtlich in 1 bis 2 Jahren auftreten	Wird voraussichtlich mehr als einmal im Jahr auftreten
	Gesund-heitliche Schäden	**Umwelt-einflüsse**	**Finanzielle Schäden**	**Ansehen / Reputation**			**Unwahr-scheinlich**	**Selten**	**Möglich**	**Wahrscheinlich**	**Definitiv**
							1	**2**	**3**	**4**	**5**
Auswirkungen	Leichte Auswirkung, Verletzung ohne krankheits-bedingter Abwesenheit	Keine bis geringe Umwelt-auswirkungen	Möglicher Geräte- oder Vermögensschaden oder finanzieller Verlust < 10K €	Kein Schaden oder nur leichte Bedenken des Kunden	**Trivial**	**1**	1	2	3	4	5
	Normale Auswirkung, Verletzung mit krankheits-bedingter Abwesenheit	Vorübergehende Umwelt-auswirkungen vor Ort, ungiftige Gerüche	Möglicher Geräte- oder Vermögensschaden oder finanzieller Verlust zwischen 10K € und 50K €	Geringfügiger Schaden für den öffentlichen Ruf, Bedenken des Kunden	**Gering**	**2**	2	4	6	8	10
	Schwere Auswirkungen, bleibende Verletzung mit Abwesenheit	Geringe Umwelt-auswirkungen vor Ort, Aufräumarbeiten erforderlich	Schäden/Verlust in Höhe von 50K € bis 100K €	Schädigung des lokalen Rufs, mehrere Kunden-beschwerden	**Mäßig**	**3**	3	6	9	12	15
	Sehr schwere Auswirkung, tödlicher Unfall	Große Umwelt-auswirkungen vor Ort, gelangt in die Umwelt	Schäden/Verlust in Höhe von 100K € bis 500K €	Schädigung des regionalen Rufs, Verlust von Kundenaufträgen, Ansprüche von Kunden	**Bedeutend**	**4**	4	8	12	16	20
	Katastrophale Auswirkung, mehrere Todesopfer	Katastrophale Umwelt-auswirkungen in der Region	Schäden/Verlust in Höher > 500K €	Schädigung des internationalen Rufs, Verlust mehrerer Kunden	**Kritisch**	**5**	5	10	15	20	25

Quelle: Eigene Darstellung nach [32]

Anhang 4: Manuell erstellte Inventarisierungsliste

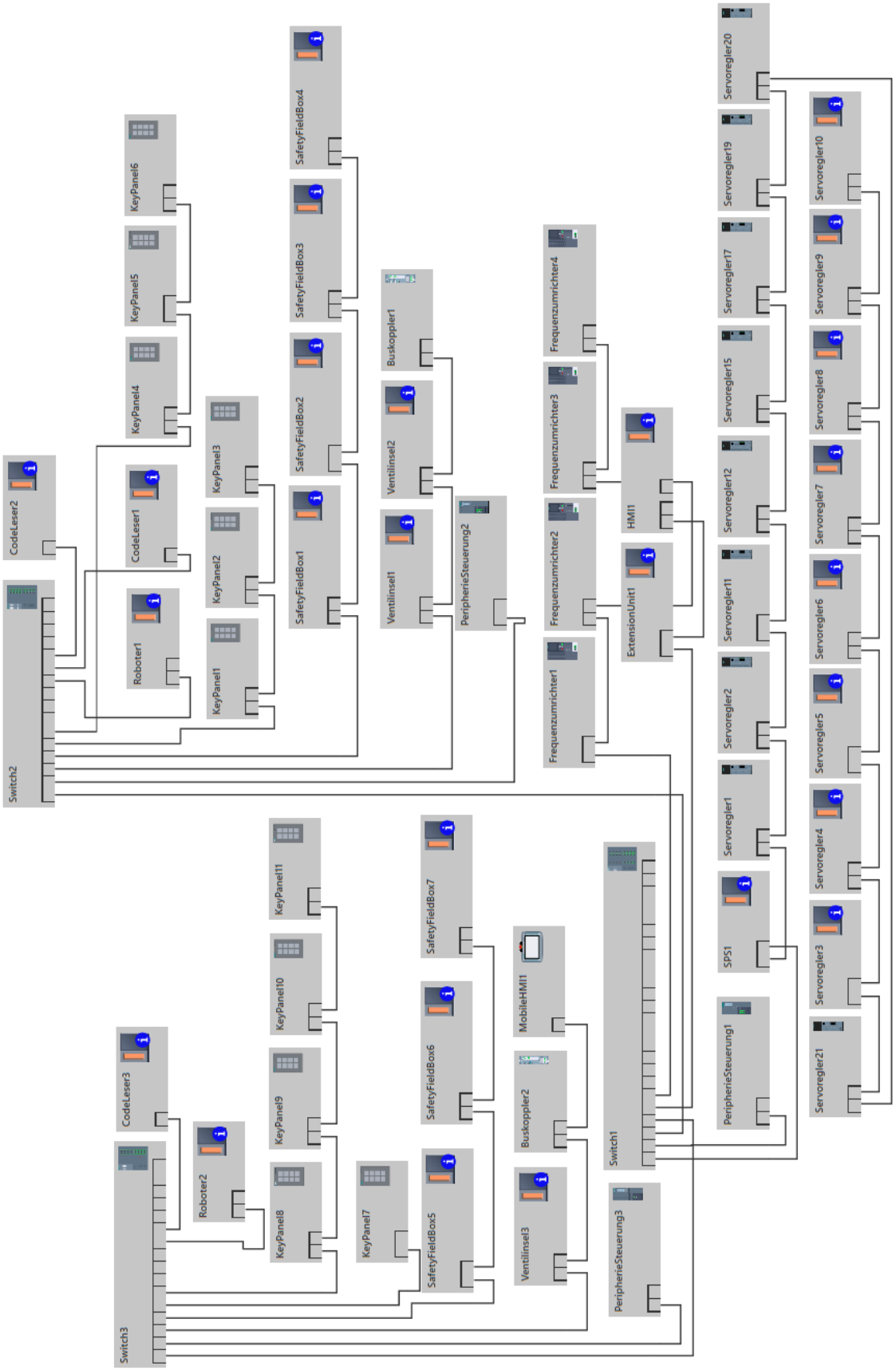


ID	Systemname	Gerätetyp	Funktionsbeschreibung	Netzwerk-schnittstelle	MAC-Adresse	IP-Adresse	Gateway	Hersteller
HW1	SPS1	SPS	Dient zur Steuerung der gesamten Maschine	X1 P1-P2, X2 P1	AC-64-17-F9-B3-53	192.168.0.10	192.168.0.29	SIEMENS AG
HW2	Switch1	Switch	Dient der Weiterleitung der Kommunikation	X1 P1-P24	30-2F-1E-40-EF-E9	192.168.0.3	192.168.0.29	SIEMENS AG

Model	Artikelnummer	Seriennummer	HW Version	FW Version	Verantwortliche Abteilung	Standort	Zusätzliche Notizen
S7-1500	6ES7 516-3FN02-0AB0	S C-N7 XXXXXXXXX	2	V 02.09.02	Programmierer Hauptstandort	Schaltschrank 1	Geladenes Programm: MaschinensteuerungXYZ IP-Adresse für X2: 192.168.1.0 - nicht in Verwendung
SCALANCE XC224	6GK5224-0BA00-2AC2	SVP XXXXXXXX	1	V 03.01.00	Programmierer Hauptstandort	Schaltschrank 1	Konfigurationsdatei liegt ab unter: XXX

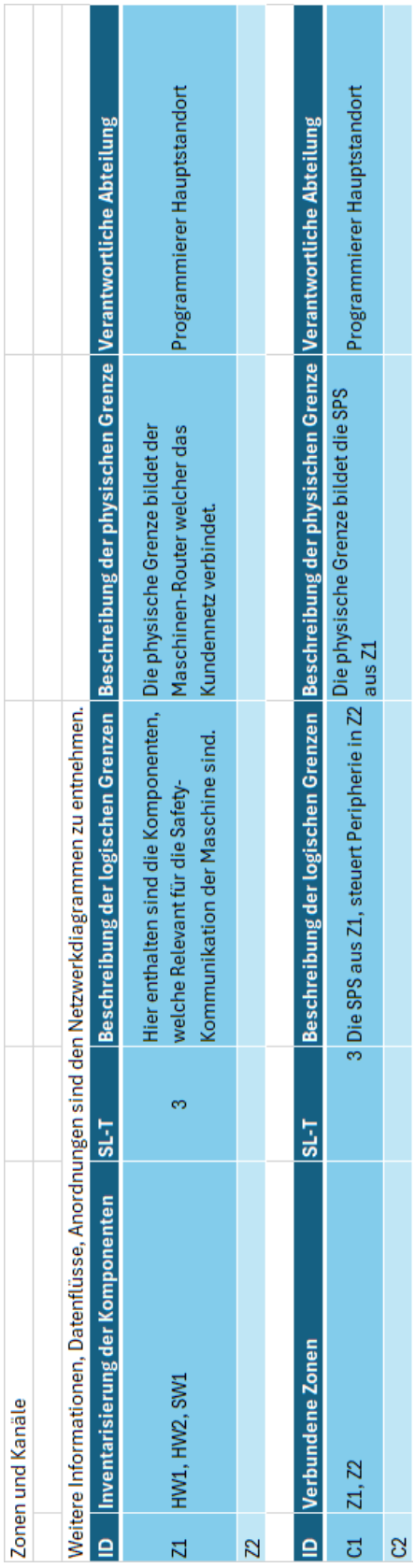
Quelle: Eigene Darstellung

Anhang 5: Netzwerkdiagramm aus SINETPLAN



Quelle: Selbst generiert mit SINETPLAN

Anhang 6: Beschreibung der Zonen und Kanäle



Zonen und Kanäle

Weitere Informationen, Datenflüsse, Anordnungen sind den Netzwerkdiagrammen zu entnehmen.

ID	Inventarisierung der Komponenten	SL-T	Beschreibung der logischen Grenzen	Beschreibung der physischen Grenze	Verantwortliche Abteilung
Z1	HW1, HW2, SW1	3	Hier enthalten sind die Komponenten, welche Relevant für die Safety-Kommunikation der Maschine sind.	Die physische Grenze bildet der Maschinen-Router welcher das Kundennetz verbindet.	Programmierer Hauptstandort
Z2					

ID	Verbundene Zonen	SL-T	Beschreibung der logischen Grenzen	Beschreibung der physischen Grenze	Verantwortliche Abteilung
C1	Z1, Z2	3	Die SPS aus Z1, steuert Peripherie in Z2	Die physische Grenze bildet die SPS aus Z1	Programmierer Hauptstandort
C2					

Quelle: Eigene Darstellung

Anhang 7: Tolerierbare Risikotabelle

Tolerierbares Risiko = 8	
Risiko	SL-T
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1
12	1
13	1
14	1
15	2
16	2
17	2
18	2
19	2
20	2
21	3
22	3
23	3
24	3
25	3
Max_Initiales Risiko = 15	
Detaillierte Cyber Security Risikobewertung nötig?	
JA	Nein

Quelle: Eigene Darstellung nach [32]

Anhang 8: Bedrohungsanalyse

ID	Name
B1	Ausnutzung von Fernwartungszugängen

Beschreibung der Bedrohungsquelle
Angreifer nutzen oftmals Schwachstellen in entfernten Geräten wie bspw. Routern, Jump Hosts, Anwendungsservern oder VPN-Servern aus, um dadurch Zugriff auf verbundene Geräte wie SPSen oder Netzwerkgeräte zu erlangen.

Beschreibung des Fähigkeitsniveaus der Bedrohungsquelle
SL3, vorsätzlicher Missbrauch mit anspruchvollen Mitteln und moderaten Ressourcen, IACS-spezifischen Kenntnissen und moderater Motivation

Beschreibung möglicher Bedrohungsvektoren
Schwachstellen, Phishing von Fernwartungs-Login, Social Engineering, Brute-Force

Identifizierung möglicher betroffener Komponenten
Fernwartungs-Router, VPN-Server, Jump-Hosts, Switche, Edge-Devices, IIoT Geräte

Identifizierung möglicher betroffener Zonen und Kanäle
Z1, C1

Gegenmaßnahmen
Segmentierung, Härtung

Quelle: Eigene Darstellung

Anhang 9: Schwachstellenidentifikation

ID	Schwachstelle	Beschreibung der Schwachstelle	Gefunden durch	Gegenmaßnahmen	Betroffenes Komponenten	Betroffene Zonen und Kanäle
S1	Offene Telnet Ports	Unverschlüsselte Übertragung von Passwörtern	OpenVAS	Härtung	HW2	Z1, Z2, C1
S2	Veraltete FW	Sicherheitslücke in aktueller FW entdeckt	Datenbank abgleich	Patchen	HW1	Z1

Quelle: Eigene Darstellung

Anhang 10: Auswirkungsbestimmung

	Gesund-heitliche Schäden	Umwelt-einflüsse	Finanzielle Schäden	Ansehen / Reputation		
Auswirkungen	Leichte Auswirkung, Verletzung ohne krankheits-bedingter Abwesenheit	Keine bis geringe Umwelt-auswirkungen	Möglicher Geräte- oder Vermögensschaden oder finanzieller Verlust < 10K €	Kein Schaden oder nur leichte Bedenken des Kunden	**Trivial**	**1**
	Normale Auswirkung, Verletzung mit krankheits-bedingter Abwesenheit	Vorübergehende Umwelt-auswirkungen vor Ort, ungiftige Gerüche	Möglicher Geräte- oder Vermögensschaden oder finanzieller Verlust zwischen 10K € und 50K €	Geringfügiger Schaden für den öffentlichen Ruf, Bedenken des Kunden	**Gering**	**2**
	Schwere Auswirkungen, bleibende Verletzung mit Abwesenheit	Geringe Umwelt-auswirkungen vor Ort, Aufräumarbeiten erforderlich	Schäden/Verlust in Höhe von 50K € bis 100K €	Schädigung des lokalen Rufs, mehrere Kunden-beschwerden	**Mäßig**	**3**
	Sehr schwere Auswirkung, tödlicher Unfall	Große Umwelt-auswirkungen vor Ort, gelangt in die Umwelt	Schäden/Verlust in Höhe von 100K € bis 500K €	Schädigung des regionalen Rufs, Verlust von Kundenaufträgen, Ansprüche von Kunden	**Bedeutend**	**4**
	Katastrophale Auswirkung, mehrere Todesopfer	Katastrophale Umwelt-auswirkungen in der Region	Schäden/Verlust in Höher > 500K €	Schädigung des internationalen Rufs, Verlust mehrerer Kunden	**Kritisch**	**5**

ID	Name	GS	U	FS	A//R	MAX
B1	Ausnutzung von Fernwartungszugängen	1	2	3	1	3

Quelle: Eigene Darstellung nach [32]

Anhang 11: Inschalingsmatrix

Fragen	Option 1		Option 2		Option 3		Gewichtung	
Standardmäßige Sicherheitslücke vorhanden	Nein	1	Nicht sicher/Ja	3			0	⊗
Ist Code zum ausnutzen verfügbar	Nein	1	Konzepte	4	Ja	6	0	⊗
Sind technische Details verfügbar	Keine	1	Ein paar	2	Komplett	3	0	⊗
Erforderlicher Zugriff	Physisch	1	LAN	4	Internet	6	0	⊗
Benötigte Rechte	Admin	1	Benutzer	2	Keine	4	0	⊗
Komplexität der Ausnutzung	Komplex	1	Durchschnittlich	2	Leicht	3	0	⊗
Benutzer Interaction erforderlich	Komplex	1	Leicht	3	Keine	4	0	⊗
Wird die Sicherheitslücke ausgenutzt	Ja	1	Limitiert	2	Oft	3	0	⊗
Ist ein Exploit zu erwarten	Nein	1	Ja	3			0	⊗
Patchverfügbarkeit	> 2 Monate	1	<= 2 Monate	2	Keine	3	0	⊗
							0	
Diese Bewertung basiert auf der "Inschalingsmatrix" (Niederländisch für "Klassifizierungsmatrix") von dem niederländischem nationalen Cyber Security Institut: https://www.ncsc.nl					Selten			
					Eintrittswahrscheinlichkeit "unwahrscheinlich" ist kein mögliches Ergebenis. Bewertet werden theoretische Schwachstellen.			

Quelle: Eigene Darstellung nach [37]

Anhang 12: Rest-Risikobewertung

Betrachtete Zone/Kanal:	Z1	Auswirkung							3
Schwachstelle	**Konsequenzen Beschreibung**	**GS**	**U**	**FS**	**A/R**	**Max**	**UTL**	**Risiko**	**SL-T**
Offene USB-Ports in Systemen und an Servern	Verlust von Systemen, Verlust von Daten	4	4	2	3	4	3	12	1
Keine oder keine aktuellen Anti-Viren-Programme	Verlust von Systemen, Verlust von Daten	4	4	2	3	4	4	16	2
Produktions-PCs EOL	Unauthorisierte Zugriff auf Systeme, Möglichkeit auf Konfigurationsänderungen	4	4	5	5	5	5	25	3

Implementierte Sicherheitsmaßnahmen	**MTL**	**Mit. Risk**	**Empfehlungen**	**ATL**	**Risk**
Physische Segmentierung, Physische Schutzmaßnahmen	2	8	USB-Sperren, USB-Nutzungs-Richtlinien	1	4
	4	16	Aktualisierung der Anti-Viren-Programme	2	8
Sitzungssperre nach Inaktivität	4	20	Upgrade auf neustes Betriebssystem, USB-Sperren	1	5

Quelle: Eigene Darstellung nach [32]

IX. Verzeichnis der Abkürzungen

BGB	Bürgerliches Gesetzbuch
BSI	Bundesamt für Sicherheit in der Informationstechnik
CRA	Cyber Resilience Act
CRS	Cyber Security Requirements Specification
CSMS	Cyber Security Management System
ENISA	European Network and Information Security Agency
IACS	Industrial Automation and Control System
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
IPSec	Internet Protocol Security
IT-SiG 2.0	IT-Sicherheitsgesetz 2.0
ISA	International Society of Automation
ISO	International Organization for Standardization
KMU	Klein- und mittelständische Unternehmen
MVO	Maschinenverordnung
NIS2	Network and Information Security Directive 2.0
NIS2UmsuCG	NIS2 Umsetzungs- und Cybersicherheitsstärkungsgesetz
OT	Operational Technology
RE	Requirements Enhancement
SL-A / C / T	Security Level – Achieved / Capable / Target
SNMP	Simple Network Management Protocol
SR	System Requirement
TLS	Transport Layer Security Protocol
VDMA	Verein Deutscher Maschinen und Anlagenbauer

VLAN	Virtual Local Area Network
VM	Virtuelle Maschine
ZfCH	Zentralstelle für das Chiffrierwesen
ZSI	Zentralstelle für Sicherheit in der Informationstechnik

X. Thesen

Thema der Arbeit: „Erstellung eines Umsetzungsleitfadens informationstechnischer Sicherheitsmaßnahmen für Maschinen anhand der IEC-62443“

Bearbeiter: Max-Florian Beck

Thesen:

- Auf die Industrie kommen viele neue Herausforderungen in Bezug auf verschiedene Cyber-Security Gesetze zu.
- Der Bereich Maschinenbau ist besonders durch die neuen Gesetzgebungen betroffen.
- Der „Stand der Technik“ ist nicht klar definiert, wodurch zusätzliche Herausforderungen und Unklarheiten entstehen.
- Normen geben nur grobe Vorgaben und keine genauen Handlungsbeschreibungen.
- Ein Umsetzungsleitfaden erleichtert die Arbeit der Maschinenbauer, spart Ressourcen und sorgt für eine höhere Sicherheit von Maschinen.
- Das Abnahmeprotokoll bietet dem Kunden eine umfangreiche Information zur Sicherheit der erworbenen Maschine.

XI. Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe.

Die Stellen der Arbeit, die anderen Quellen im Wortlaut oder dem Sinn nach entnommen wurden, sind durch Angaben der Herkunft kenntlich gemacht. Dies gilt auch für Zeichnungen, Skizzen, bildliche Darstellungen sowie für Quellen aus dem Internet.

Ich erkläre ferner, dass ich die vorliegende Arbeit in keinem anderen Prüfungsverfahren als Prüfungsarbeit eingereicht habe oder einreichen werde.

Die eingereichte schriftliche Arbeit entspricht der elektronischen Fassung. Ich stimme zu, dass eine elektronische Kopie gefertigt und gespeichert werden darf, um eine Überprüfung mittels Anti-Plagiatssoftware zu ermöglichen.

Ort, Datum	Unterschrift