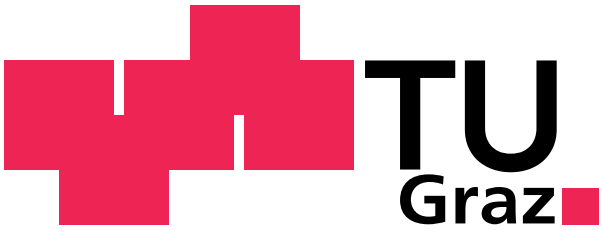

Institut für Health Care Engineering mit
Europaprüfstelle für Medizinprodukte
Technische Universität Graz
8010 Graz, Stremayrgasse 16, 2.Stock
Tel.: 0316/873-7378 Fax.: 0316/873-107378

Masterarbeit

Cybersecurity in der Medizintechnik

zum Erlangen des Grades eines
Diplom Ingenieur

Author: Alisia Fladerer BSc.

Betreuer: Assoc.Prof. Dipl.-Ing. Dr.techn. Jörg Schröttner

Head of Institute: Univ.-Prof. Dr. Christian Baumgartner

29. Januar 2025

Zusammenfassung

Diese Masterarbeit untersucht die Cybersicherheitsanforderungen für Medizingeräte und beleuchtet die speziellen Herausforderungen, die mit der zunehmenden Vernetzung und Digitalisierung im Gesundheitssektor einhergehen. Zu Beginn wird ein umfassender Überblick über die regulatorischen Anforderungen, Normen und Leitlinien gegeben, die für die Sicherheit vernetzter Medizinprodukte maßgeblich sind, darunter die EU-MDR (Medical Device Regulation) und die einschlägigen ISO/IEC-Standards. Basierend auf einer fundierten Literaturrecherche und der Analyse verschiedener Standards und Empfehlungen wurde eine Methode zur Bewertung der Cybersicherheit von Medizinprodukten entwickelt.

Die Literaturrecherche hat eine Vielzahl an Normen ergeben, die sich mit dem Thema Cybersecurity beschäftigen. Neben den harmonisierten Normen, sind die EN ISO/IEC 27002, die EN IEC 62443-4-1, die EN IEC 81001-5-1, ISO/IEC 15408-2 und die EN 82304 für den Hersteller zu empfehlen. Zusätzlich wird die Anwendbarkeit der Methode anhand von zwei Beispielen überprüft. Das Temperaturmesssystem und das Vorhersagemodell erfüllen wesentliche Cybersicherheitsanforderungen durch Verschlüsselung, Authentifizierung und Risikomanagementprozesse, weisen jedoch spezifische Schwächen auf. Während beim Temperaturmesssystem insbesondere die Authentifizierung und Echtzeit-Überwachung ausgebaut werden sollten, fehlen beim Vorhersagemodell klare Coding-Guidelines und kontinuierliche Überwachung. Beide Produkte erfüllen ihre jeweiligen Security Levels (2 bzw. 3), haben aber noch Potenzial für Verbesserungen, um die Sicherheit weiter zu stärken.

Die Arbeit liefert somit nicht nur eine fundierte Analyse des regulatorischen Rahmens, sondern zeigt auch praxisnahe Verbesserungsmöglichkeiten auf, die Herstellern dabei helfen können, die Sicherheit und Resilienz vernetzter Medizingeräte zu erhöhen.

Schlüsselwörter: Cybersicherheit, Medizingeräte, Sicherheitsnormen, Bedrohung, Sicherheitslücken

Abstract

This Master's thesis examines the cybersecurity requirements for medical devices, highlighting the specific challenges associated with increasing connectivity and digitisation in the healthcare sector. It begins with a comprehensive overview of the regulatory requirements, standards and guidelines that are critical to the security of connected medical devices, including the EU Medical Device Regulation (EU-MDR) and relevant ISO/IEC standards. A methodology for evaluating the cybersecurity of medical devices was developed based on a thorough literature review and analysis of various standards and recommendations.

The literature review identified numerous standards that address cybersecurity. In addition to harmonised standards, EN ISO/IEC 27002, EN IEC 62443-4-1, EN IEC 81001-5-1, ISO/IEC 15408-2 and EN 82304 are recommended for manufacturers. In addition, the applicability of the methodology was verified using two case studies: a temperature monitoring system and a predictive model. While both meet basic cybersecurity requirements through encryption, authentication and risk management processes, specific weaknesses were identified. The temperature monitoring system requires enhanced authentication and real-time monitoring, while the predictive model lacks clear coding guidelines and continuous monitoring. Both products meet their respective security levels (2 and 3) but have room for improvement to further enhance their security.

This thesis provides a comprehensive analysis of the regulatory framework and practical recommendations to help manufacturers improve the security and resilience of connected medical devices.

Key Words: Cybersecurity, Medical Device, Threat, Safety standards, Vulnerabilities

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Medizingeräte sind ein wesentlicher Bestandteil der modernen Gesundheitsversorgung, da sie zur Diagnose, Überwachung und Behandlung von Krankheiten eingesetzt werden. Diese Geräte reichen von einfacheren externen Geräten, wie Blutzuckermessgeräten oder Blutdruckmonitoren, bis hin zu komplexeren, implantierbaren Geräten wie Herzschrittmachern und Insulinpumpen. Mit der Weiterentwicklung der Technologie und der zunehmenden Vernetzung der Medizingeräte haben sich jedoch auch neue Herausforderungen und Risiken ergeben, insbesondere in Bezug auf die Cybersicherheit. Die zunehmende Integration von Software in medizinische Geräte und deren Anbindung an Netzwerke birgt erhebliche Cybersicherheitsrisiken. Eine der größten Gefahren besteht darin, dass Angreifer auf diese vernetzten Geräte zugreifen und deren Funktion manipulieren können. Dies könnte zu gravierenden Auswirkungen auf die Patientensicherheit führen, da die Geräte lebenswichtige Funktionen erfüllen, wie etwa die Regulierung des Herzrhythmus bei Herzschrittmachern oder die Dosierung von Insulin bei Diabetikern. Selbst theoretische Angriffe auf diese Systeme haben gezeigt, dass es möglich ist, auf diese Geräte zuzugreifen und ihre Funktion zu verändern, was potenziell gefährliche Konsequenzen für die Gesundheit und das Leben der Patienten haben könnte. [3] [72]

Die potenziellen Schwachstellen betreffen nicht nur die Integrität der Daten, die von den Geräten gesammelt werden, sondern auch ihre Verfügbarkeit und Funktionalität. Zudem besteht die Gefahr, dass Hacker auf sensible Gesundheitsdaten zugreifen und diese für böswillige Zwecke missbrauchen. [6] [17] [77]

Diese Entwicklungen verdeutlichen die dringende Notwendigkeit, nicht nur die Funktionalität, sondern auch die Sicherheit von Medizingeräten zu gewährleisten. Da diese Geräte zunehmend vernetzt sind und eine zentrale Rolle im Gesundheitswesen spielen, müssen robuste Sicherheitsmaßnahmen entwickelt und implementiert werden, um sowohl die Patientensicherheit als auch den Datenschutz zu gewährleisten. [72] [17]

1.1 Schutzziele bei Medizingeräten

1.1.1 Vertraulichkeit

Vertraulichkeit bedeutet im Kontext der Medizintechnik, dass sensible Informationen, wie persönliche und medizinische Patientendaten, nur für berechtigte Nutzer und Systeme zugänglich sind. Bei vernetzten Medizingeräten, die Patientendaten in Echtzeit verarbeiten und senden, umfasst Vertraulichkeit den Schutz der Daten vor Abhören, Diebstahl und unautorisiertem Zugriff. Besonders bei implantierbaren und tragbaren Geräten, die mit anderen Krankenhaus- und Patientensystemen verbunden sind, ist es wichtig, dass diese Verbindungen abgesichert und verschlüsselt sind. [84] [78]

Bei einer Verletzung der Vertraulichkeit könnten vertrauliche Patientendaten (etwa Diagnosen, Medikation oder Behandlungsverlauf) in die falschen Hände geraten. Bei

medizinischen Geräten, die über drahtlose Netzwerke kommunizieren, kann ein Angreifer unter Ausnutzung von Schwachstellen sensible Informationen abfangen und zur Erpressung nutzen oder manipulieren. Besonders bei Geräten wie Infusionspumpen oder Herzschrittmachern könnte dies die Sicherheit der Patienten gefährden, indem sensible Parameter unbemerkt verändert werden. [84] [78]

1.1.2 Integrität

Integrität bedeutet, dass alle medizinischen Daten und Systeme unverändert und vollständig sind und dass jede Änderung nur von berechtigten Personen vorgenommen wird. Für Medizingeräte bedeutet dies, dass sowohl die gesendeten und empfangenen Daten als auch die Gerätekonfiguration vor Manipulation geschützt sind. Die Integrität umfasst neben den Patientendaten auch die Einstellungen und Steuerungsparameter des Geräts, wie die Dosierung bei Infusionspumpen oder die Stimulation bei Herzschrittmachern. [59] [78]

Werden Patientendaten unbemerkt manipuliert, kann dies zu falschen Diagnosen oder unpassenden Behandlungen führen. Beispielsweise könnte eine fehlerhafte Anzeige des Blutzuckerspiegels eines Diabetikers zu einer fehlerhaften Insulindosierung führen. Bei Geräten, die drahtlos konfiguriert werden, wie Herzschrittmachern oder Insulinpumpen, kann ein Verlust der Integrität dazu führen, dass die Konfiguration des Geräts geändert und für den Patienten schädliche Parameter eingestellt werden. Ein Angreifer könnte z.B. die Dosis einer Medikamentenpumpe erhöhen, was zu einer lebensbedrohlichen Überdosierung führt, oder Alarme manipulieren, sodass medizinisches Personal nicht auf kritische Zustände aufmerksam gemacht wird. Wenn die Integrität von Software oder Firmware eines Geräts durch fehlerhafte Updates oder gezielte Angriffe verletzt wird, kann das Gerät seine normale Funktion nicht mehr sicherstellen. So könnten Fehlfunktionen oder Manipulationen zu fehlerhaften Messwerten führen, die für die Patientenversorgung genutzt werden und so unmittelbare Konsequenzen für die Patientensicherheit haben. [59] [78]

1.1.3 Verfügbarkeit

Verfügbarkeit bedeutet, dass Medizingeräte und die dazugehörigen Daten in kritischen Momenten stets zugänglich und funktionsfähig sind. Bei Medizingeräten, die für Diagnosen oder therapeutische Maßnahmen notwendig sind, wie z.B. Beatmungsgeräte oder Herzmonitore, ist die kontinuierliche Verfügbarkeit essenziell für eine stabile Patientenversorgung. In Notfallsituationen hängt die Patientensicherheit davon ab, dass diese Geräte unmittelbar bereitstehen und einsatzfähig sind. [34] [67]

Wenn durch Angriffe wie Ransomware oder DoS (Denial-of-Service) der Zugriff auf kritische Geräte blockiert wird, sind Ärzte und Pflegepersonal nicht in der Lage, rechtzeitig auf lebensrettende Daten zuzugreifen. Medizingeräte, die in Echtzeit arbeiten

und miteinander vernetzt sind, wie etwa computergestützte Katheterisierungslabore oder Radiologie-Systeme, müssen ständig verfügbar sein. Ein Malware-Angriff oder ein Systemfehler, der die Funktionalität dieser Geräte beeinträchtigt, kann dazu führen, dass elektive Operationen verschoben oder zeitkritische Eingriffe unterbrochen werden müssen. Die daraus resultierende Verzögerung in der Behandlung gefährdet die Patientensicherheit erheblich. [34] [67]

1.2 Aktuelle Bedrohung im Zusammenhang mit Cybersecurity in der Medizintechnik

Technologische Entwicklung und Vernetzung

Die fortschreitende Integration von medizinischen Geräten in IT-Infrastrukturen, oft über das Internet oder drahtlose Netzwerke, schafft neue Angriffsvektoren. Medizinische Geräte, die früher isoliert arbeiteten, sind zunehmend vernetzt, was zu einer erhöhten Anfälligkeit für Cyberangriffe führt. Dies gilt insbesondere für tragbare Geräte und implantierte Systeme wie Herzschrittmacher und Insulinpumpen, die oft drahtlos kommunizieren. [4] [85]

Die Angriffe auf diese Geräte können nicht nur zum Datendiebstahl führen, sondern auch die Funktionsweise der Geräte manipulieren, was die Patientensicherheit gefährdet [59] [84] [78]. Ein stark vernetztes Gesundheitsnetzwerk erhöht das Risiko, dass ein Angriff auf ein einzelnes Gerät das gesamte Netzwerk gefährden kann [86] [84].

Medizinische Bildgebungsgeräte wie Computertomographen (CT) und Magnetresonanztomographen (MRT) sind ebenfalls stark gefährdet. Sie sind integrale Bestandteile moderner Krankenhäuser, aber ihre zunehmende Vernetzung macht sie anfällig für gezielte Cyber-Angriffe. Angreifer können nicht nur den Betrieb der Geräte stören, sondern auch die Strahlenbelastung oder andere Parameter manipulieren, was potenziell schwerwiegende Folgen für die Patienten haben kann. [58] [57]

Besonders kritisch sind implantierbare medizinische Geräte, wie Herzschrittmacher oder Neurostimulatoren, da sie nicht nur sensible Daten übertragen, sondern auch direkt die Gesundheit der Patienten beeinflussen. Sicherheitslücken in diesen Geräten können nicht nur zur Offenlegung von Patientendaten führen, sondern auch deren Funktion beeinträchtigen. [38] [1]

Veraltete Software und begrenzte Sicherheitsmaßnahmen

Viele medizinische Geräte verwenden veraltete Software, die oft nicht mehr unterstützt wird und für Sicherheitsupdates schwer zugänglich ist. Es gibt zahlreiche Beispiele, in denen Malware wie der Conficker-Wurm Geräte wie Röntgengeräte oder Herzmonitore infiziert hat, was zu Ausfällen und Verzögerungen in der Patientenversorgung führte. Veraltete Software und fehlende Sicherheitsupdates stellen ein erhebliches Risiko dar, da

viele Hersteller keine effektiven Mechanismen zur Verfügung stellen, um ältere Geräte auf den neuesten Stand zu bringen. [34] [67]

Es fehlt oft an regelmäßigen Software-Updates und - Patches, was dazu führt, dass Geräte anfällig für bekannte Sicherheitslücken bleiben. Diese Schwachstellen betreffen sowohl die Funktionsfähigkeit der Geräte als auch den Schutz der Patientendaten, die durch die Geräte gesammelt und übertragen werden. [84] [15] [71]

Die begrenzte Rechenleistung und der Speicherplatz solcher Geräte erschweren es, Sicherheitssoftware wie Antivirusprogramme effektiv zu betreiben [85].

Implantierbare medizinische Geräte wie Kardioverter-Defibrillatoren (ICDs) und Herzschrittmacher sind besonders gefährdet. In mehreren Fällen wurden Schwachstellen in diesen Geräten entdeckt, die es Angreifern ermöglichten, ihre Funktionsweise zu manipulieren oder sogar die Batterie vorzeitig zu entladen. Diese Sicherheitslücken, die oft durch unzureichende Firmware-Updates verursacht werden, können zu unangemessenen elektrischen Schocks oder Fehlfunktionen führen. [3] [69]

Die Zeit, die zwischen der Entdeckung einer Schwachstelle und ihrer Behebung durch Updates oder Patches vergeht, ist oft zu lang. Studien zeigen, dass medizinische Geräte im Durchschnitt 3,2 Jahre anfällig bleiben, bevor Schwachstellen durch Patches behoben werden. Dies bedeutet, dass viele Geräte während dieser Zeit einem erhöhten Risiko ausgesetzt sind. Insbesondere ältere oder „Legacy"− Geräte, die nicht regelmäßig aktualisiert werden, sind anfällig für Angriffe und stellen eine Bedrohung dar. [6]

Komplexität und Langlebigkeit von Geräten

Die langen Lebenszyklen von medizinischen Geräten bedeuten, dass viele dieser Geräte über Jahre oder sogar Jahrzehnte mit älteren Betriebssystemen im Einsatz bleiben. Die Betriebssysteme der älteren Generation werden zum Teil nicht mehr unterstützt oder aktualisiert. Diese Komplexität führt zu Schwierigkeiten bei der Implementierung von Sicherheitsmaßnahmen, da Geräte oft individuell konfiguriert sind und Änderungen nur durch die Hersteller durchgeführt werden können. [85] [78]

Angriffsmethoden und Bedrohungen

Medizinische Geräte sind sowohl aktiven als auch passiven Cyberbedrohungen ausgesetzt. Aktive Bedrohungen umfassen direkte Angriffe wie das Abfangen von Daten oder die Manipulation von Gerätekonfigurationen. Passiv können Angreifer Kommunikation überwachen oder Netzwerkdaten abfangen. [67]

Die Abbildung 1 bietet einen Überblick über die Hauptbedrohungen im Zeitraum von Januar 2021 bis März 2023. Hierbei dominieren Ransomware und datenbezogene Bedrohungen, wobei verschiedene Angriffsmuster kombiniert auftreten können.

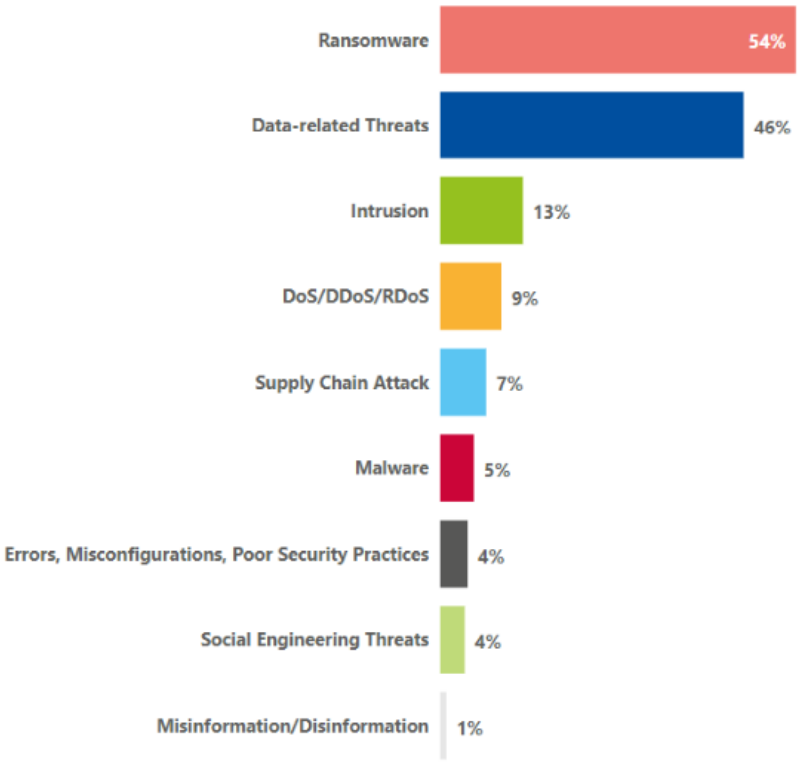

Abbildung 1: Prozentsätze gemeldeter Vorfälle für Bedrohungen im Gesundheitssektor.[76]

a) Ransomware

Ransomware ist eine Form von Schadsoftware, bei der Angreifer Daten verschlüsseln und nur gegen Lösegeldzahlung freigeben. Diese Angriffe zielen besonders auf Gesundheitsdaten, da diese für die Erpresser von hoher Bedeutung sind. Ransomware-Angriffe nehmen seit 2021 im Gesundheitssektor zu. Mehrere Vorfälle führten zur Beeinträchtigung von Patientenversorgung, wie etwa der Schließung von Notfallabteilungen und der Verschiebung wichtiger Behandlungen. Der Anstieg setzt sich fort, da 2023 bereits mehrere Ransomware-Angriffe gemeldet wurden. Die Tendenz zeigt, dass die Gesundheitsdaten weiterhin im Visier der Angreifer bleiben werden. [78] [76] [67]

b) Data-related Threats (Datenbedrohungen)

Diese Bedrohungen umfassen den unautorisierten Zugriff auf Daten, Manipulation und Diebstahl. Die Daten im Gesundheitssektor sind durch ihre persönliche und sensible Natur besonders wertvoll. Bedrohungen gegen Daten nehmen zu, besonders durch den Anstieg von Cyberangriffen und Sicherheitsverletzungen in der Pandemie. [76] [67]

c) Denial of Service (DoS) Angriffe

DoS-Angriffe zielen darauf ab, Dienste durch Überlastung des Netzwerks oder der Server unzugänglich zu machen. Diese Angriffe beeinflussen die Verfügbarkeit der IT-Systeme. DoS-Angriffe nehmen zu, insbesondere durch geopolitisch motivierte Gruppen. Die Verfügbarkeit von Gesundheitsdiensten wird dadurch beeinträchtigt, was die Funktionsfähigkeit im Gesundheitssektor gefährden kann. [76] [67]

d) Malware (Schadsoftware)

Malware bezeichnet jede Software, die zum unautorisierten Zugriff, zur Manipulation oder um Systemen zu schaden eingesetzt wird. Beispiele sind Computer-Viren, Würmer und Trojaner. Malware-Angriffe machen etwa 5 % der gemeldeten Vorfälle aus. Es wird erwartet, dass sich die Malware-Bedrohung weiterentwickelt, oft in Kombination mit Social Engineering. [76]

e) Supply-Chain Attacks (Angriffe auf die Lieferkette)

Lieferkettenangriffe zielen auf die Beziehung zwischen Organisationen und ihren Dienstleistern ab und nutzen Schwachstellen in diesen Verbindungen. Diese Bedrohung nimmt zu, besonders in Bezug auf Software und Cloud-Anwendungen, da die Abhängigkeit von externen Dienstleistern steigt. [76]

f) Social Engineering Threats (Soziale Bedrohungen)

Social Engineering umfasst Angriffe, die menschliche Schwächen ausnutzen, um unbefugten Zugang zu Informationen oder Systemen zu erhalten. Taktiken sind Phishing und Spear-Phishing. Diese Bedrohung ist ein konstantes Risiko, das sich oft in Kombination mit anderen Angriffen zeigt. Erhöhte Schulungen zum Sicherheitsbewusstsein sind dringend notwendig. [76] [67]

g) Intrusion (Einbrüche)

Einbrüche (Intrusionen) beziehen sich auf Vorfälle, bei denen Angreifer unerlaubt Zugang zu Systemen erlangen, ohne dass die genauen Einzelheiten des Zugangs bekannt sind [76].

h) Desinformation/Misinformation

Im Jahr 2021 stellte Desinformation ein erhebliches Problem dar. Anfang Januar 2021 teilte die Europäische Arzneimittel-Agentur (EMA) mit, dass einige der im Dezember 2020 gestohlenen Daten zum Impfstoffkandidaten von Pfizer/BioNTech von Bedrohungsakteuren manipuliert wurden, bevor sie online veröffentlicht wurden. Ziel dieser Manipulation war es, das Vertrauen der Öffentlichkeit in die COVID-19-Impfstoffe zu schwächen. Auch wenn die direkte Bedrohung für Gesundheitsorganisationen durch Desinformation begrenzt war, wurde die Bedeutung dieser Bedrohung durch die Manipulation der öffentlichen Meinung und durch Angriffe auf Gesundheitsbehörden deutlich. [76]

i) Errors, Misconfiguration and poor security practices (Fehler, Fehlkonfigurationen und schlechte Sicherheitspraktiken)

Die Bedrohung entsteht durch menschliche Fehler, fehlerhafte Konfigurationen und unzureichende Sicherheitsmaßnahmen. Beispiele sind ungeschützte Datenbanken, unzureichend gepatchte Software und Sicherheitslücken in medizinischen Geräten. Diese Probleme können zu Datenlecks, Betriebsunterbrechungen und Risiken für die Patientensicherheit führen. [76]

Menschliche Faktoren und organisatorische Herausforderungen

Ein erheblicher Teil der Bedrohungen in der Medizintechnik resultiert aus menschlichen Fehlern, wie dem Klicken auf Phishing-Links oder dem Missbrauch von Zugangsdaten. Organisatorische Schwächen und das mangelnde Bewusstsein für Cyberrisiken verschärfen diese Bedrohungen. Schulungsprogramme zur Sensibilisierung für Cybersicherheit sind daher unerlässlich, um das menschliche Verhalten zu verbessern und die Verteidigungsfähigkeit gegenüber Angriffen zu stärken. [64]

Insider-Bedrohungen, sei es durch böswillige Absicht oder durch unbeabsichtigte Fehler, stellen eine weitere signifikante Gefahr dar. Sie sind schwerer zu erkennen und zu verhindern sind, da Insider oft legitimen Zugang zu sensiblen Systemen und Daten haben. [38] [76] [13]

Die Zusammenarbeit zwischen verschiedenen Abteilungen und externen Partnern ist ein weiterer wichtiger organisatorischer Faktor. Eine mangelnde Kommunikation zwischen IT-Sicherheitsteams, medizinischem Personal und externen Dienstleistern kann zu Sicherheitslücken führen. [11]

Systemische und organisatorische Risiken

Organisationen im Gesundheitssektor sind oft nicht ausreichend auf Cybersicherheitsvorfälle vorbereitet, was sich in der unzureichenden Umsetzung von Sicherheitsmaßnahmen und Notfallplänen zeigt. Viele Krankenhäuser und Gesundheitseinrichtungen verfügen über keine klaren Strategien zur Risikobewertung und Reaktion auf Cyberangriffe. Die Auswirkungen solcher Angriffe können enorm sein, wie zahlreiche Vorfälle in den letzten Jahren gezeigt haben, bei denen Gesundheitsdienste durch Ransomware-Angriffe lahmgelegt wurden. [16]

Neue Ansätze und Technologietrends

Die Einführung von Cloud-Diensten, Big Data und dem Internet of Things (IoT) bietet nicht nur Vorteile, sondern auch neue Risiken, insbesondere durch Hyperkonnektivität [67].

Die Integration von KI und maschinellem Lernen in medizinische Geräte bietet sowohl Chancen als auch Risiken. Die Technologien können zur Verbesserung der Diagnosegenauigkeit und der Patientenversorgung beitragen, gleichzeitig jedoch neue Angriffsvektoren eröffnen, die gezielt durch fortschrittliche Cyberangriffe ausgenutzt werden können. [13] [77]

1.3 IT-Sicherheit vs. Betriebssicherheit vs. Informationssicherheit

Die Begriffe IT-Sicherheit, Betriebssicherheit und Informationssicherheit spielen in der Medizintechnik eine zentrale Rolle, da sie unterschiedliche, aber miteinander verbundene Aspekte der Sicherheit abdecken.

IT-Sicherheit

IT-Sicherheit befasst sich mit dem Schutz von Computersystemen, Netzwerken und Daten vor unbefugtem Zugriff, Manipulation oder Zerstörung. In der Medizintechnik bedeutet dies den Schutz von vernetzten medizinischen Geräten, die in IT-Systeme eingebunden sind. Diese Geräte müssen gegen potenzielle Angriffe geschützt werden, während gleichzeitig ihre Funktionalität aufrechterhalten bleibt. Besonders wichtig ist es, sicherzustellen, dass IT-Sicherheitsmaßnahmen wie Authentifizierungssysteme, Zugriffskontrollen und Verschlüsselung integriert sind, um den Schutz der Daten und Systeme zu gewährleisten. Dies gilt während des gesamten Lebenszyklus der Geräte, von der Entwicklung bis zum Einsatz im Gesundheitswesen. [40] [60]

Betriebssicherheit

Betriebssicherheit bezieht sich auf die Fähigkeit eines Systems, sicher und zuverlässig zu arbeiten, auch unter unerwarteten oder herausfordernden Bedingungen. In der Medizintechnik ist es entscheidend, dass die wesentlichen Funktionen eines Geräts auch dann aufrechterhalten werden, wenn es Angriffen ausgesetzt ist. Wenn beispielsweise restriktive Sicherheitsmaßnahmen die Arbeit des medizinischen Personals behindern, kann dies die Sicherheit der Patienten gefährden. Ein sorgfältiges Gleichgewicht zwischen Sicherheit und betrieblicher Effizienz ist daher unerlässlich. Es ist wichtig, dass medizinische Geräte so konzipiert sind, dass sie auch unter Stressbedingungen ihre Funktionen beibehalten und Notfallzugriffe ermöglichen, falls es erforderlich ist. [40] [60]

Informationssicherheit

Informationssicherheit konzentriert sich auf den Schutz von Daten vor unbefugtem Zugriff, Veränderung oder Verlust. Besonders im Gesundheitswesen, wo medizinische Geräte hochsensible Patientendaten verarbeiten und übertragen, ist der Schutz dieser Informationen von zentraler Bedeutung. Die Vertraulichkeit, Integrität und Verfügbarkeit der Daten müssen gewährleistet sein, um das Vertrauen der Patienten in das Gesundheitssystem zu sichern und den gesetzlichen Anforderungen zu entsprechen. Der Verlust oder die Manipulation von Patientendaten kann nicht nur rechtliche Folgen nach sich ziehen, sondern auch die medizinische Versorgung gefährden. Daher sind umfassende Maßnahmen zur Sicherstellung der Informationssicherheit notwendig, die in alle relevanten Prozesse integriert werden. [84] [31]

Die Interaktion zwischen IT-Sicherheit, Betriebssicherheit und Informationssicherheit ist entscheidend für die Cybersicherheit in der Medizintechnik. IT-Sicherheitsmaßnahmen wie Firewalls oder Zugangskontrollen dürfen nicht so streng sein, dass sie die Betriebssicherheit beeinträchtigen. Ebenso müssen alle Schutzmaßnahmen die Informationssicherheit

gewährleisten, ohne die Funktionalität der Geräte zu gefährden. Eine übergreifende Sicherheitsstrategie, die alle drei Bereiche abdeckt, ist erforderlich, um die Patientensicherheit zu garantieren. Dies erfordert den Einsatz standardisierter Sicherheitsrahmenwerke, die die besonderen Bedürfnisse des Gesundheitssektors berücksichtigen. [40] [60] [31]

Insgesamt ist eine enge Verzahnung der IT-Sicherheit, Betriebssicherheit und Informationssicherheit notwendig, um sowohl den Schutz der medizinischen Geräte als auch der darin verarbeiteten Daten zu gewährleisten. Alle drei Sicherheitsdimensionen müssen sorgfältig berücksichtigt werden, um die Risiken zu minimieren und die Funktionsfähigkeit der Systeme sicherzustellen. [84] [64] [40] [60] [31]

1.4 Regulatorische Herausforderungen

Die regulatorischen Anforderungen an die IT-Sicherheit von medizinischen Geräten sind einerseits komplex, aber auch oft unzureichend. Die langsame Reaktion auf neue Bedrohungen und die mangelnde Implementierung von Sicherheitsstandards in vernetzten Geräten machen es schwierig, ein einheitliches Sicherheitsniveau zu gewährleisten. Unterschiedliche Standards und Vorschriften erschweren die Implementierung einheitlicher Sicherheitsmaßnahmen. Häufig sind die existierenden Leitlinien unzureichend auf die spezifischen Cybersicherheitsanforderungen von Medizinprodukten abgestimmt, was zu Unsicherheiten und Umsetzungsproblemen führt. [15] [71] [10]

Diese Arbeit wird zu einem besseren Verständnis der Anwendbarkeit und Wirksamkeit bestehender Cybersicherheitsnormen im Bereich der Medizingeräte beitragen. Durch die umfassende Zusammenstellung und Analyse relevanter Normen sowie die kritische Bewertung ihrer Umsetzungspotenziale wird ein Überblick darüber geschaffen, welche Standards für die besonderen Anforderungen vernetzter Medizingeräte geeignet sind und wo möglicherweise noch Lücken bestehen. Darüber hinaus werden zwei ausgewählte Medizingeräte hinsichtlich ihrer Cybersicherheitsmaßnahmen analysiert, was die praxisbezogenen Herausforderungen und Sicherheitsanforderungen in der Anwendung verdeutlicht.

2 Methoden und Zielsetzung

2.1 Zielsetzung

Das Ziel dieser Masterarbeit ist es, die Bedeutung von Cybersecurity für die Medizinproduktsicherheit zu analysieren und die damit verbundenen Maßnahmen auf Basis der regulatorischen Anforderungen zu diskutieren. Anhand zweier exemplarischer Medizinprodukte sollen schließlich Aspekte der Cybersecurity analysiert und bewertet werden. Die Arbeit soll einen Beitrag dazu leisten, die Bedeutung von Cybersecurity bei Medizinprodukten sowie die dazu erforderlichen regulatorischen Anforderungen für Medizinprodukthersteller hervorzuheben.

2.2 Literaturrecherche

Die Literaturrecherche stellt die erste methodische Grundlage dieser Arbeit dar. Der Ablauf der Literaturrecherche war in mehreren Schritten organisiert:

- **Rechercheansatz:** Es wurde eine systematische Suche nach wissenschaftlichen Artikeln, regulatorischen Dokumenten, Normen und Leitlinien durchgeführt. Dabei lag der Fokus auf internationalen und nationalen Richtlinien zur Cybersicherheit von Medizinprodukten mit dem Schwerpunkt auf Europa, wissenschaftlichen Publikationen über Sicherheitslücken und Angriffsvektoren bei vernetzten medizinischen Geräten sowie Best-Practice-Ansätzen in der IT-Sicherheit.
- **Datenquellen:** Die Recherche umfasste sowohl akademische als auch behördliche Quellen. Wichtige wissenschaftliche Datenbanken wie Google Scholar, PubMed, IEEE Xplore und spezifische regulatorische Plattformen wie Eur-Lex (für europäische Regulierungen wie die MDR und IVDR) wurden genutzt. Suchmaschinen und Datenbanken wurden mit Schlüsselwörtern wie „Cybersicherheit“, „Medizinprodukte“, „Sicherheitsanforderungen“, „Regulatorische Compliance“, „Verantwortlichkeit", „Sicherheitslücken in medizinischen Geräten", „Einflussfaktoren", „Software als Medizinprodukt (SaMD)“ durchsucht.
- **Kriterien für die Auswahl der Literatur:** Die Auswahl der Literatur erfolgte nach festgelegten Kriterien, darunter Aktualität (Fokus auf Veröffentlichungen der letzten 10 Jahre), Relevanz (Publikationen, die direkte Verbindungen zur Cybersicherheit von Medizinprodukten aufweisen) und Qualität (wissenschaftliche Peer-Reviewed-Artikel, regulatorische Dokumente, Normen und Leitfäden von Behörden und Fachgremien). Studien und Berichte, die praxisorientierte Bewertungen oder Analysen von Sicherheitsvorkehrungen bei Medizinprodukten enthielten, wurden bevorzugt.

- **Analyse und Zusammenfassung:** Nach der Recherche wurden die relevanten Dokumente inhaltlich analysiert, kategorisiert und in einem strukturierten Überblick zusammengefasst.

2.3 Zusammenfassung von regulatorischen Anforderungen und Empfehlungen

Im zweiten Schritt wurden die in der Literaturrecherche gesammelten regulatorischen Anforderungen und Empfehlungen zusammengefasst und hinsichtlich ihrer Anwendbarkeit auf Medizinprodukte analysiert. Dieser Prozess beinhaltete die Konsolidierung relevanter Verordnungen, Normen und Leitfäden und die Erstellung einer Checkliste zur systematischen Bewertung von Cybersicherheitsmaßnahmen.

Zusammenfassung von Verordnungen, Normen und Guidance Dokumenten: Die Verordnungen sowie ISO/IEC-Normen und andere relevante Leitfäden wurden analysiert und ihre spezifischen Anforderungen an die Cybersicherheit hervorgehoben. Diese Anforderungen wurden im Hinblick auf ihre Anwendbarkeit auf Medizinprodukte diskutiert, um sicherzustellen, dass sie praxisnah und umsetzbar sind.

Erstellung der Checkliste: Die Checkliste basiert auf dem Leitfaden des Johner Instituts [54], der bereits etablierte Anforderungen und Best Practices für die Bewertung der Cybersicherheit von Medizinprodukten enthält. Zusätzlich wurden Anforderungen, die in der Literatur gefunden wurden und im Johner Leitfaden nicht abgedeckt waren, in die Checkliste integriert.

Organisation der Checkliste in Excel: Die Checkliste wurde in einem Excel-Dokument erstellt, das eine systematische Bewertung der Cybersicherheitsanforderungen ermöglicht. Zu jeder Anforderung wurden die zugehörigen Normen und regulatorischen Vorgaben vermerkt. Außerdem wurde für jede Anforderung ein Security Level bestimmt.

Security Levels: Für die Bewertung der Cybersicherheit von Medizingeräten wurden Sicherheitsstufen (Security Levels) verwendet, um das Schutzniveau zu klassifizieren, das erforderlich ist, um die Integrität, Vertraulichkeit und Verfügbarkeit der Geräte und ihrer Daten zu gewährleisten. Das Security Level eines Medizinprodukts wird basierend auf seiner Zweckbestimmung festgelegt. Die Definition der unterschiedlichen Security Levels basiert auf den Normen EN IEC 62443-4-2 [26], EN 62304 [21], IEC TR 60601-4-5 [40], ISO/TR 24971 [53] und dem Leitfaden des Johner Instituts [54].

- **Security Level 1 Basis-Sicherheitsanforderungen:** Grundlegendes Sicherheitsniveau für Produkte mit minimalem Risiko. Es umfasst grundlegende Sicherheitsmechanismen wie Passwortschutz und physische Sicherung des Geräts. *Beispiel:* Einfache tragbare Geräte, die keine kritischen medizinischen Funktionen ausführen, z. B. Fitness-Tracker.

- **Security Level 2 Erhöhtes Sicherheitsniveau:** Für Produkte, die personenbezogene Daten verarbeiten, aber keine lebenswichtigen Funktionen steuern. Es werden zusätzliche Sicherheitsmaßnahmen implementiert, um gegen gezielte Angriffe zu schützen. *Beispiel: Geräte, die Gesundheitsdaten sammeln und speichern, wie z. B. tragbare Blutzuckermessgeräte.*
- **Security Level 3 Hohes Sicherheitsniveau:** Für Produkte mit direkter Auswirkung auf die Patientensicherheit, bei denen fortschrittliche Sicherheitsmaßnahmen erforderlich sind. *Beispiel: Implantierbare medizinische Geräte wie Herzschrittmacher, die in Echtzeit arbeiten und bei denen Manipulationen lebensgefährliche Folgen haben könnten.*
- **Security Level 4 Maximaler Schutz:** Höchste Sicherheitsstufe für Produkte mit den kritischsten Funktionen und höchsten Risiken. *Beispiel: Geräte für die Intensivpflege, wie Beatmungsgeräte oder Infusionspumpen, die in einer hochsensiblen Umgebung arbeiten*

Ziel der Checkliste: Die Checkliste dient als Werkzeug für Hersteller, um die Erfüllung der Cybersicherheitsanforderungen ihrer Produkte zu überprüfen. Hersteller können auf Basis der erfüllten Anforderungen ein Security Level bestimmen, das den Sicherheitsstatus ihrer Geräte widerspiegelt.

2.4 Anwendung der Ergebnisse auf ausgewählte Medizinprodukte

Die entwickelte Checkliste und die zugehörigen Beurteilungskriterien wurden auf zwei ausgewählte Medizinprodukte angewendet, um deren Cybersicherheit zu bewerten und deren Security Level zu bestimmen. Dieser Teil der Methodik lässt sich in folgende Schritte unterteilen:

Auswahl der Produkte: Die Auswahl der Medizinprodukte erfolgte auf der Grundlage ihrer Relevanz für die Cybersicherheit und ihrer Vernetzungsfähigkeit.

- **Temperaturmesssystem:** Das Produkt ist ein Thermometer, das dazu bestimmt ist, die Körpertemperatur kontinuierlich im Bereich der Achselhöhle zu messen und medizinischem Fachpersonal relative Temperaturänderungen des Patienten anzuzeigen. Das System besteht aus einem Sensor und einer unterstützenden Softwareanwendung. Die vom Sensor gemessenen Temperaturdaten werden drahtlos übertragen und können mithilfe der Software in ein Krankenhausinformationssystem (KIS) integriert werden.
- **Vorhersagemodell:** Das Produkt ermöglicht eine automatisierte Risikobewertung, indem es vorhandene Daten aus elektronischen Gesundheitsakten analysiert, wie z. B. Laborwerte, Medikation und Pflegedokumentation, um personalisierte Risikoeinschätzungen zu erstellen.

Bewertung der Produkte: Beide Produkte wurden systematisch anhand der Checkliste bewertet. Der Fokus lag darauf, die implementierten Cybersicherheitsmaßnahmen zu analysieren und Schwachstellen zu identifizieren

Bestimmung des Security Levels: Die Bestimmung des Security Levels für jedes Produkt wurde durch eine strukturierte Bewertung mithilfe der entwickelten Checkliste vorgenommen. In dieser Checkliste ist für jede Sicherheitsanforderung ein spezifisches Security Level zugeordnet. Für die Bewertung wurden die Security Levels aller erfüllten Anforderungen herangezogen und deren Mittelwert berechnet. Dieser Mittelwert repräsentiert das durchschnittliche Sicherheitsniveau des Produkts.

Im nächsten Schritt wurde das berechnete Security Level in Relation zur Zweckbestimmung des Produkts gesetzt. Dabei wurde überprüft, ob das ermittelte Sicherheitsniveau die Anforderungen des Produkts ausreichend abdeckt.

Ermittlung von Verbesserungsmöglichkeiten: Basierend auf den Ergebnissen der Analyse wurden konkrete Empfehlungen zur Verbesserung der Cybersicherheitsmaßnahmen der Produkte formuliert.

3 Ergebnisse

3.1 Aktuelle Bedrohungen und Sicherheitslücken

3.1.1 Beispiele von Cyberangriffen

Ransomware-Angriffe stellen die größte Bedrohung dar und machen etwa 54 % der Vorfälle aus. Diese Angriffe führen häufig zu Datenverlust und Störungen medizinischer Dienste, die lebensbedrohliche Folgen für Patienten haben können. Fast die Hälfte der Vorfälle (46 %) betrifft Datenverletzungen, die durch Fehlkonfigurationen oder Schwachstellen verursacht werden. Während der Pandemie wurden mehrfach Patientendaten unabsichtlich veröffentlicht, was die Dringlichkeit sicherheitsbewusster Praktiken verdeutlicht. Ein weiterer Trend sind DoS-Angriffe (Denial of Service), die vermehrt in Verbindung mit geopolitischen Entwicklungen durch hacktivistische Gruppen auftreten, insbesondere durch pro-russische Gruppen im Jahr 2023. Obwohl die tatsächlichen Auswirkungen dieser Angriffe oft gering sind, betonen sie die Bedrohungslage. [76]

Der WannaCry-Ransomware-Angriff, 2017, hat große Teile des National Health Service (NHS) in Großbritannien lahmgelegt. Mehrere Krankenhäuser waren gezwungen, Operationen und Termine abzusagen, da sie keinen Zugang zu Patientendaten hatten. Der Angriff nutzte Schwachstellen in veralteten Windows-Systemen aus und zeigte, wie gefährlich veraltete Software für kritische Infrastrukturen sein kann. Der Angriff wurde teilweise durch Schwachstellen in vernetzten medizinischen Geräten verstärkt, die oft nicht rechtzeitig aktualisiert werden. [16] [58]

Der Conficker-Wurm infizierte zahlreiche medizinische Geräte, darunter Röntgen- und Laborausrüstungen, in verschiedenen Gesundheitseinrichtungen. Aufgrund veralteter Betriebssysteme und fehlender Sicherheitsupdates konnten die Geräte nicht vor dieser bekannten Malware geschützt werden. Die Infektion beeinträchtigte die Funktion der betroffenen Geräte erheblich und führte zu Verzögerungen in der Patientenversorgung. [34]

Im Medtronic CareLink Vorfall 2018 wurden Sicherheitslücken in Medtronic-Geräten aufgedeckt, die über das CareLink-System überwacht wurden. Aufgrund fehlender Verschlüsselung und mangelnder Authentifizierung konnten potenzielle Angreifer die Kommunikation mit den Geräten abfangen und manipulieren. In Reaktion darauf gab die US-amerikanische FDA Sicherheitswarnungen heraus und forderte erweiterte Maßnahmen zur Risikominderung. [17]

Der Abbott (St. Jude Medical) Vorfall 2016 betraf eine Schwachstelle in Merlin-Geräten, die es Angreifern ermöglichte, die Batterieleistung zu manipulieren oder die Kommunikation der Geräte zu stören. Diese Schwachstelle führte zu einer erhöhten Anfälligkeit für Cyberangriffe und resultierte in einer Rückrufaktion durch die FDA. Der Hersteller reagierte mit einem Firmware-Update, um die Sicherheit der Geräte zu gewährleisten. [17] [67]

3.1.2 Beispiele für Sicherheitslücken in Medizingeräten

Die aktuellen Sicherheitsinformationen zu verschiedenen Medizingeräten weisen auf bedeutende Cybersicherheitsrisiken hin, die insbesondere die Kontrolle und Sicherheit von Insulinpumpen, Beatmungsgeräten und Lasersystemen betreffen. Die Medtronic MiniMed™ 508 und Paradigm™ Insulinpumpen sind aufgrund ihrer drahtlosen Kommunikation anfällig für Cyberangriffe, die unbefugten Zugriff auf die Insulinabgabe ermöglichen könnten. Anwender sollten ihre Geräte stets unter Kontrolle halten, verdächtige Insulinabgaben abbrechen und keine unbekannten USB-Geräte anschließen, um das Risiko von Manipulationen zu minimieren. [61]

Die Dräger Beatmungsgeräte der Serien Evita V500/V300 und Babylog VN500 nutzen ältere Betriebssysteme, die nicht mehr aktualisiert werden und daher Schwachstellen aufweisen könnten. Da jedoch die meisten Geräte über serielle Verbindungen angeschlossen sind, ist die Anfälligkeit für Cyberangriffe relativ gering. Dräger empfiehlt, den physischen Zugang zu den Geräten zu kontrollieren und ungenutzte Schnittstellen zu verschließen. Auf Anfrage stellt Dräger kostenloses Material zum Abdecken dieser Anschlüsse bereit, um die Sicherheit zusätzlich zu gewährleisten. [20]

Die DANA Diabecare RS Insulinpumpe wurde ebenfalls als potenziell gefährdet eingestuft, insbesondere bei älteren Firmware-Versionen unter 3.0. Anwender können durch ein Firmware-Update und die Aktivierung des Flugmodus vorübergehend Schutz erhalten, falls sie Bedenken hinsichtlich eines unbefugten Zugriffs haben. Die neue Firmware erhöht die Cybersicherheit und verringert das Risiko unautorisierter Änderungen an der Pumpensteuerung. [73]

Auch das Johnson & Johnson Vision iDESIGN® Refractive Studio und das CATALYS™ Precision Laser System nutzen Betriebssysteme, die Schwachstellen im Druckspoolerdienst aufweisen, was Remotecodeausführungen ermöglichen könnte. Ein potenzieller Angriff könnte Angreifern den Zugriff auf Systemdaten oder die Steuerung von Geräten gewähren. Johnson & Johnson Vision stellt hierfür ein Software-Update bereit und nimmt direkten Kontakt mit den betroffenen Nutzern auf, um das Update zu implementieren. Anwender werden bis zur Aktualisierung angewiesen, zusätzliche Sicherheitsprüfungen vorzunehmen. [55]

3.2 Bedeutung für die Patientensicherheit

Die Cybersicherheitsbedrohungen, die medizinische Geräte betreffen, haben direkte und potenziell schwerwiegende Auswirkungen auf die Patientensicherheit. In einer zunehmend digitalisierten und vernetzten Gesundheitsumgebung sind die Risiken komplexer und vielfältiger geworden, was die Bedeutung von Cybersicherheitsmaßnahmen zur Gewährleistung der Patientensicherheit hervorhebt.

Unterbrechung kritischer Geräte und Auswirkungen auf Patientenversorgung

Eine der gravierendsten Auswirkungen von Cyberangriffen auf medizinische Geräte ist die direkte Unterbrechung kritischer medizinischer Versorgung. Angriffe auf Geräte wie Infusionspumpen oder Beatmungsgeräte können schwerwiegende Folgen für die betroffenen Patienten haben. Wenn solche Geräte nicht ordnungsgemäß funktionieren, kann dies zu einer Unterbrechung der lebensrettenden Versorgung führen. Angreifer könnten beispielsweise gezielte Denial-of-Service (DoS)-Angriffe durchführen, um die Funktion dieser Geräte zu blockieren, was unmittelbar das Leben der Patienten gefährdet. [4] [76]

Auch im Falle eines Ransomware-Angriffs können Geräte, die für diagnostische und therapeutische Zwecke notwendig sind, für eine längere Zeit außer Betrieb gesetzt werden. Dies betrifft nicht nur den stationären Betrieb in Krankenhäusern, sondern auch ambulante Geräte, die zur Langzeitüberwachung von Patienten eingesetzt werden, wie etwa tragbare Insulinpumpen oder Herzmonitore. Wenn ein Gerät aufgrund eines Cyberangriffs außer Betrieb gesetzt wird, besteht das Risiko, dass schwerwiegende Gesundheitskomplikationen nicht rechtzeitig erkannt oder behandelt werden. [16] [67]

Manipulation von Diagnosedaten und Therapieentscheidungen

Ein weiteres erhebliches Risiko für die Patientensicherheit besteht in der Manipulation von Diagnosedaten. Viele vernetzte medizinische Geräte sammeln und analysieren Daten, die dann zur Diagnosestellung oder zur Steuerung von Behandlungen verwendet werden. Wenn Angreifer diese Daten ändern oder verfälschen, können Ärzte falsche Diagnosen stellen oder fehlerhafte Behandlungsentscheidungen treffen. Es ist möglich, dass Cyberangriffe auf Geräte, die bildgebende Verfahren oder Laboranalysen unterstützen, die Qualität und Genauigkeit der diagnostischen Informationen verändern. [34]

Eine solche Datenmanipulation kann potenziell tödliche Folgen haben, wenn beispielsweise falsche Medikamentendosierungen verordnet oder lebenswichtige Parameter wie die Herzfrequenz falsch gemessen werden [77].

Auch die Integrität der Patientendaten spielt hierbei eine entscheidende Rolle. Wenn die Datenintegrität durch Malware oder andere Cyberangriffe verletzt wird, besteht das Risiko, dass Änderungen an Gesundheitsdaten unbemerkt bleiben und falsche Informationen die Behandlung negativ beeinflussen. Insbesondere bei der elektronischen Gesundheitsakte (EHR) ist das kritisch, da ein Angriff auf diese Daten zu Fehlinformationen über Medikationen, Allergien oder vergangene Eingriffe führen könnte. [12] [16]

Schwachstellen in implantierbaren Geräten und potenzielle Folgen

Implantierbare medizinische Geräte (IMDs) wie Herzschrittmacher, Insulinpumpen und Neurostimulatoren sind besonders gefährdet, da sie oft drahtlos gesteuert und überwacht werden. Angreifer könnten über Funkfrequenzverbindungen oder ungesicherte Netzwerke auf diese Geräte zugreifen, um ihre Funktion zu manipulieren. [38]

Diese Geräte sind ebenfalls häufig anfällig für Cyberangriffe, da sie drahtlose Kommunikationsschnittstellen verwenden, die von Angreifern aus der Ferne manipuliert werden können. Ein erfolgreicher Angriff auf ein IMD könnte den Patienten schaden, indem der Herzschlag manipuliert oder eine lebenswichtige Insulindosis verändert wird oder falsche Signale senden oder ganz ausfällt. [78] [38]

Ransomware und die Verfügbarkeit kritischer Ressourcen

Ransomware-Angriffe verschlüsseln im Gesundheitswesen nicht nur den Zugang zu Gesundheitsdaten, sondern können auch medizinische Geräte lahmlegen. Dies hat erhebliche Auswirkungen auf die Patientensicherheit, insbesondere bei Notfällen. Wenn lebenswichtige Geräte während eines Ransomware-Angriffs nicht zugänglich sind, könnte dies zu Verzögerungen bei der Behandlung oder sogar zum Tod von Patienten führen. Ransomware-Angriffe können auch die gesamte Krankenhausinfrastruktur beeinträchtigen, indem sie die Kommunikation zwischen Geräten stören. In Situationen, in denen die schnelle Reaktion auf Notfälle von entscheidender Bedeutung ist, könnte die Unfähigkeit, auf Diagnosedaten oder Gerätefunktionen zuzugreifen, eine erhebliche Gefahr darstellen. Wenn Krankenhäuser während eines Angriffs keinen Zugang zu Patientendaten, wie medizinischen Vorgeschichten oder aktuellen Medikationsplänen, haben, kann dies ebenfalls zu schwerwiegenden Behandlungsfehlern führen. Patienten, die auf kontinuierliche Behandlung angewiesen sind, wie Dialysepatienten oder solche, die eine intensive Überwachung benötigen, sind durch solche Angriffe besonders gefährdet. In diesen Fällen kann ein kurzer Ausfall eines Geräts oder Systems die Situation eines Patienten erheblich verschlechtern. [12] [71] [67] [57]

3.3 Verknüpfung von regulatorischen Anforderungen mit Best Practice Beispielen und Empfehlungen

3.3.1 Europäische Regulierung und Standards

Die regulatorischen Vorgaben zur Cybersecurity lassen sich in drei Kategorien einteilen:

- **Verordnungen:** Diese sind Gesetze oder bindende Regelungen, die von staatlichen Behörden oder Regulierungsagenturen erlassen werden und Gesetzeskraft besitzen. Sie sind national oder international gültig und legen spezifische Cybersicherheitsanforderungen fest, die verpflichtend einzuhalten sind. Ein Beispiel ist die EU-Medizinprodukteverordnung (MDR), die Anforderungen an die Cybersicherheit für medizinische Geräte definiert und somit eine gesetzliche Grundlage für die Sicherheit in der Medizintechnik schafft. [10]
- **Normen:** Diese Dokumente dienen als standardisierte „Stand der TechnikDokumente und werden oft durch Konsens von Normungsorganisationen entwickelt. Normen bieten detaillierte Sicherheitsanforderungen und technische Spezifikationen, die helfen, einheitliche Cybersicherheitsstandards umzusetzen. Ein Beispiel ist die ISO

27799, die Sicherheitsanforderungen für Informationssicherheit im Gesundheitswesen beschreibt. Normen sind keine gesetzlichen Vorschriften, können aber als Best-Practice-Richtlinien für Organisationen im Gesundheitswesen genutzt werden. [10]

- **Best Practices:** Diese sind Leitlinien, die sich auf bewährte Methoden zur Erreichung von Cybersicherheitszielen konzentrieren. Sie sind nicht bindend, sondern bieten Empfehlungen, die auf den praktischen Erfahrungen und Bedürfnissen der Branche basieren. Best Practices unterstützen die Umsetzung von Vorschriften und Normen, indem sie konkrete Vorgehensweisen und technische Maßnahmen empfehlen. So stellt beispielsweise die Medical Device Coordination Group (MDCG) Best-Practice-Richtlinien zur Cybersicherheit von Medizingeräten bereit, die den Herstellern helfen, regulatorische Anforderungen effizient umzusetzen. [10]

In der Europäischen Union sind die wichtigsten regulatorischen Rahmenwerke die Medical Device Regulation (MDR) und die NIS 2 Richtlinie. Die MDR legt fest, dass Medizinprodukte gemäß dem aktuellen Stand der Technik (State-of-the-Art) entwickelt werden müssen, einschließlich Anforderungen an die IT-Sicherheit. Dies betrifft sowohl Software in Medizinprodukten als auch den Schutz vor unbefugtem Zugriff und die Gewährleistung eines sicheren Betriebs. Die NIS 2 Richtlinie erweitert diese Anforderungen und fokussiert sich speziell auf die Cybersicherheit in essenziellen und wichtigen Einrichtungen, zu denen auch die Hersteller von Medizinprodukten gehören (siehe Abbildung 2).[5]

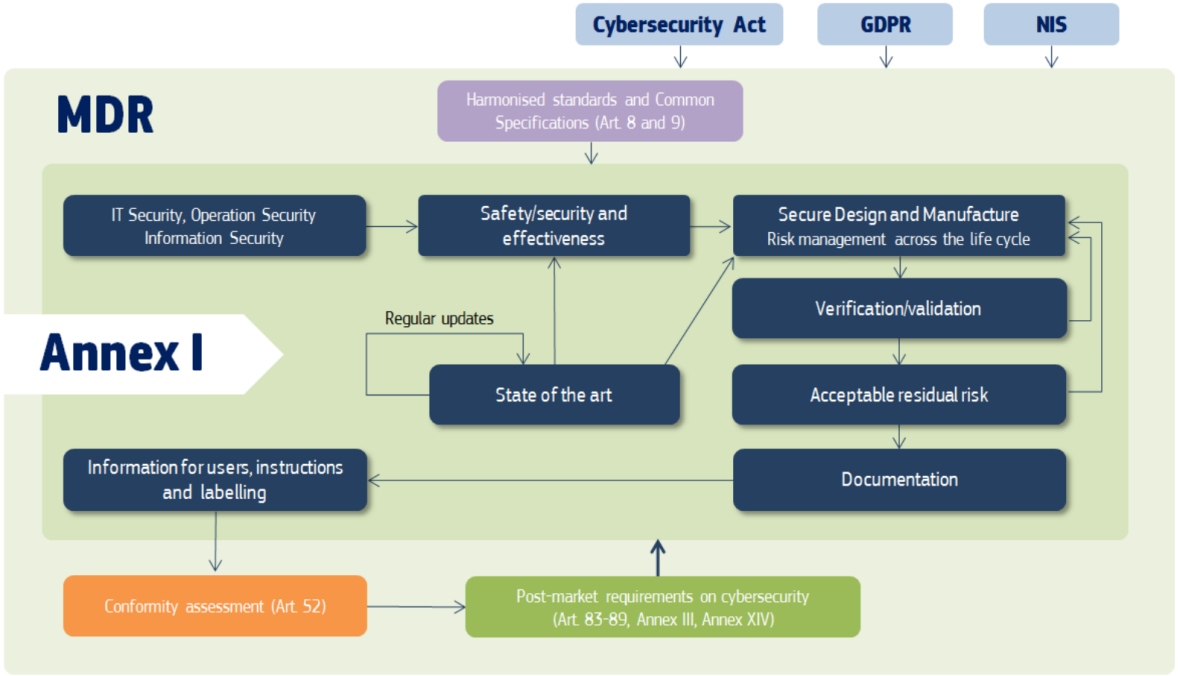

Abbildung 2: Anforderungen an die Cybersicherheit in der MDR [60]

Die ENISA (European Union Agency for Network and Information Security) ist eine zentrale Agentur der EU für Netz- und Informationssicherheit. Die ENISA-Verordnung unterstreicht die Notwendigkeit einer kohärenten und umfassenden Strategie zur Cybersicherheit, die sowohl technische als auch organisatorische Aspekte umfasst. Die Harmonisierung von Standards und die Vermeidung von Doppelarbeit sind entscheidende Schritte, um eine robuste Cybersicherheitsinfrastruktur in Europa zu schaffen. Ein besonderes Augenmerk liegt auf der Bedeutung eines proaktiven Risikomanagements und der Bedrohungsanalyse, um die Sicherheit von Informationssystemen und Netzwerken zu gewährleisten. Die Förderung einer engen Zusammenarbeit zwischen den verschiedenen Akteuren und die Nutzung bewährter Standards tragen dazu bei, die Widerstandsfähigkeit gegen Cyberangriffe zu erhöhen. [7]

Die NIST Special Publication 800-53, Revision 5, ist ein umfassender Katalog von Sicherheits- und Datenschutzkontrollen, die für Informationssysteme und Organisationen entwickelt wurden. Ziel ist es, Organisationen vor einer Vielzahl von Bedrohungen und Risiken zu schützen, einschließlich feindlicher Angriffe, menschlicher Fehler, Naturkatastrophen und Datenschutzrisiken. Diese Kontrollen sind flexibel und anpassbar, um den spezifischen Anforderungen verschiedener Organisationen und ihrer Systeme gerecht zu werden. Die NIST SP 800-53 Revision 5 betont die Notwendigkeit eines ganzheitlichen Ansatzes zur Cybersicherheit, der sowohl technische als auch organisatorische Maßnahmen umfasst. Besonders hervorzuheben ist der Fokus auf Risikomanagement und die Integration von Sicherheits- und Datenschutzkontrollen, die den Schutz von Systemen und die Privatsphäre der Nutzer sicherstellen sollen. Der umfassende Katalog an Kontrollen und die Flexibilität, die in der Implementierung dieser Kontrollen vorgesehen ist, ermöglichen es Organisationen, ihre spezifischen Bedürfnisse und Bedrohungen zu adressieren. Die Einführung von Kontrollen zur Sicherstellung der Cyberresilienz ist besonders relevant in einer Zeit, in der die Komplexität und Vernetzung von Systemen ständig zunimmt. [65]

Darüber hinaus hat die fragmentierte Natur der Cybersicherheitsregulierung zu Schwierigkeiten bei der Umsetzung geführt, da verschiedene Gesetze und Standards teilweise widersprüchlich oder schwer anwendbar sind [10].

3.3.2 Richtlinien in den USA

In den USA hat die FDA mehrere Leitlinien zur Cybersicherheit für Medizinprodukte veröffentlicht. Dazu gehört das Dokument „Content of Premarket Submissions for Management of Cybersecurity in Medical Devices", das Herstellern hilft, Sicherheitsmaßnahmen für vernetzte Geräte umzusetzen. Die FDA verweist dabei auf den NIST Cybersecurity Framework, das als Grundlage für Cybersicherheitsaktivitäten dient. Auch der kanadische Markt hat nachgezogen, wobei Health Canada spezifische Anforderungen an die Cybersicherheit von Medizinprodukten formuliert hat. [75]

Die Leitlinien der FDA konzentrieren sich auf verschiedene Phasen des Produktlebenszyklus und spezielle Anforderungen an vernetzte medizinische Geräte. Sie umfassen

präventive Maßnahmen in der Entwicklungsphase, Empfehlungen zur Sicherstellung der Interoperabilität und Überwachungsmechanismen im Post-Market-Bereich. Die wichtigsten FDA-Leitlinien zu Cybersicherheitsanforderungen für Medizinprodukte sind:

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Dieses Dokument betont, wie wichtig es ist, Cybersicherheitsmaßnahmen in die frühe Entwicklungsphase von Medizinprodukten zu integrieren. Die FDA fordert Hersteller dazu auf, Sicherheitsbedrohungen frühzeitig zu identifizieren und Maßnahmen zur Risikominderung zu entwickeln, einschließlich Risikoanalysen und der Evaluierung von Schwachstellen. [14]

Postmarket Management of Cybersecurity in Medical Devices: Diese Leitlinie richtet sich an das Management von Cybersicherheitsrisiken nach dem Inverkehrbringen von Medizinprodukten. Es wird betont, dass Hersteller kontinuierlich Schwachstellen und Bedrohungen überwachen und Sicherheitsupdates bereitstellen müssen, um die Sicherheit von Produkten während ihres gesamten Lebenszyklus zu gewährleisten. [68]

Cybersecurity for Networked Medical Devices Containing Off-the-Shelf Software: Die FDA gibt spezifische Anweisungen für vernetzte medizinische Geräte, die Standardsoftware („Off-the-Shelf“, OTS) verwenden. Hier wird empfohlen, strenge Sicherheitsvorkehrungen für die Verwendung dieser OTS-Software zu implementieren, um die Kompatibilität und Sicherheit des Gesamtsystems sicherzustellen. [36]

Design Considerations and Premarket Submissions - Recommendations for Interoperable Medical Devices: Diese Leitlinie konzentriert sich auf die Interoperabilität von Medizinprodukten und enthält Cybersicherheitsüberlegungen. Es werden Vorschläge zur Gestaltung von Geräten gemacht, die sicher in verschiedenen Netzwerken und mit anderen Geräten kommunizieren können, ohne dass dabei Sicherheitsrisiken entstehen. [18]

Wireless Medical Telemetry Risks and Recommendations: Dieses Dokument gibt Empfehlungen für die sichere Implementierung von drahtloser Medizintechnik. Es betont die Risiken durch Interferenzen und potenzielle Sicherheitslücken bei der drahtlosen Übertragung von Daten und bietet Richtlinien zur Risikominderung und Absicherung dieser Systeme. [37]

Obwohl die FDA klare Vorgaben zur Überwachung und Pflege von Geräten nach der Markteinführung macht, sind einige Richtlinien wie die zur drahtlosen medizinischen Telemetrie eher veraltet. Sie basieren auf älteren Technologien und könnten in Bezug auf moderne Bedrohungen, wie Cyberangriffe, eine genauere Überarbeitung benötigen. Es wird die freiwillige Teilnahme an Informationsaustauschprogrammen (z.B. ISAO) empfohlen, um Cybersicherheitsinformationen zu teilen. Während dies den Ansatz der geteilten Verantwortung fördert, könnte es Hersteller geben, die weniger stark in diesen Austausch involviert sind, was zu Lücken in der Cybersicherheit führen könnte. Eine stärkere Betonung auf die Postmarket-Phase, ähnlich wie in der FDA-Guidance, könnte die Verwaltung von Cyberrisiken in Europa verbessern. Regelmäßige Updates, die proaktive

Überwachung und ein engmaschiger Informationsaustausch sind Maßnahmen, die stärker verankert werden könnten.

3.3.3 Verordnungen und Richtlinien für die Cybersicherheit von Medizinprodukten

Die Cybersicherheit von Medizinprodukten wird durch eine Vielzahl von regulatorischen Vorgaben sichergestellt. Diese Regelwerke bieten Herstellern einen klaren Rahmen, um die Sicherheit und den Schutz ihrer Produkte in einer zunehmend digitalisierten und vernetzten Umgebung zu gewährleisten. Im Folgenden werden die wichtigsten Richtlinien zusammengefasst, die für die Cybersicherheit von Medizinprodukten relevant sind:

Verordnung (EU) 2017/745 über Medizinprodukte (MDR)

Die Anforderungen der MDR [81] in Bezug auf die Cybersicherheit von Medizinprodukten sind oberflächlich in verschiedenen Artikeln und Anhängen geregelt. Zu den wesentlichen Anforderungen gehören das Risikomanagement, der Schutz der Datenintegrität, die Software-Sicherheit und die kontinuierliche Überwachung nach dem Inverkehrbringen. Hersteller sind verpflichtet, ein umfassendes Risikomanagementsystem zu implementieren, das Cybersicherheitsaspekte berücksichtigt, um potenzielle Bedrohungen und Schwachstellen zu identifizieren, zu bewerten und entsprechende Gegenmaßnahmen zu ergreifen. Dies ist in Anhang I, Kapitel I, Punkt 3 der MDR festgelegt, wobei die Cybersicherheit ein zentraler Bestandteil des Designs und der Produktion von Medizinprodukten ist, um deren sichere Funktion auch bei Cybersicherheitsvorfällen sicherzustellen. Darüber hinaus müssen Medizinprodukte, die personenbezogene Daten verarbeiten oder übertragen, gemäß Anhang I, Kapitel II, Punkt 17.4 Maßnahmen zum Schutz der Vertraulichkeit und Integrität dieser Daten implementieren. Hierzu zählen der Einsatz von Verschlüsselungstechnologien und Zugriffskontrollen, um unbefugten Zugriff oder Datenmanipulationen zu verhindern. Für softwarebasierte und vernetzte Medizinprodukte, wie solche, die über Bluetooth oder WLAN kommunizieren, sieht Anhang I, Kapitel II, Punkt 17.2 vor, dass diese so gestaltet sein müssen, dass Risiken im Zusammenhang mit ihrer Vernetzung minimiert werden. Besondere Sicherheitsanforderungen sind erforderlich, um Schutzmaßnahmen gegen potenzielle Cyberangriffe zu gewährleisten. Schließlich verpflichtet die MDR in Artikel 83 die Hersteller, ein System zur Überwachung nach dem Inverkehrbringen einzurichten, um kontinuierlich neue Cybersicherheitsrisiken zu bewerten und angemessene Sicherheitsmaßnahmen anzupassen. Das Risikomanagement muss regelmäßig aktualisiert werden, um neu auftretenden Bedrohungen Rechnung zu tragen.[81]

Obwohl die MDR die Notwendigkeit der Cybersicherheit in Medizinprodukten betont, fehlen klare und detaillierte spezifische Leitlinien, die die technischen und organisatorischen Sicherheitsanforderungen für Hersteller präzise festlegen. Der Verweis auf allgemeine Risikomanagementprinzipien kann zu Interpretationsspielräumen führen, was potenziell zu einer uneinheitlichen Umsetzung der Cybersicherheitsmaßnahmen durch verschiedene Hersteller führen könnte. Besonders für kleinere Unternehmen, die möglicherweise über

weniger Ressourcen für die Implementierung umfassender Sicherheitsmaßnahmen verfügen, kann dies eine Herausforderung darstellen. Ein weiteres Problem besteht in den möglichen Verzögerungen zwischen der Entdeckung neuer Cybersicherheitsbedrohungen und der Reaktion durch Hersteller und Regulierungsbehörden. Obwohl die MDR von Herstellern verlangt, Sicherheitsupdates bereitzustellen und Bedrohungen nach dem Inverkehrbringen zu überwachen, gibt es keine klaren Fristen oder Verfahren, wie schnell auf neue Bedrohungen reagiert werden muss. Dies könnte dazu führen, dass Sicherheitslücken bestehen bleiben, bevor entsprechende Maßnahmen umgesetzt werden, was die Sicherheit von Medizinprodukten beeinträchtigen könnte. Die Anforderungen der MDR können für ältere Medizinprodukte, die bereits vor der Einführung der Verordnung in Betrieb waren, schwer umzusetzen sein. Viele dieser Geräte wurden nicht mit den heutigen Cybersicherheitsanforderungen entwickelt und erfüllen möglicherweise nicht die neuen Sicherheitsstandards. Der Aufwand, bestehende Geräte nachzurüsten oder Sicherheitsupdates bereitzustellen, kann erheblich sein. Es fehlt eine klare Regelung oder Unterstützung für den Umgang mit diesen „Legacy"− Geräten, die bereits in großer Zahl im Einsatz sind und eine potenzielle Schwachstelle darstellen. Obwohl die MDR eine bedeutende Verbesserung der Regulierung von Medizinprodukten in der EU darstellt, bleibt die regulatorische Landschaft fragmentiert, insbesondere in Bezug auf globale Normen und Standards. Verschiedene Länder und Regionen, wie die USA mit der FDA, verfolgen unterschiedliche Ansätze zur Cybersicherheit, was es für international tätige Hersteller schwierig machen kann, einheitliche Standards umzusetzen. Diese Fragmentierung erschwert die Harmonisierung der Cybersicherheitsanforderungen, was zu Inkonsistenzen in der Produktentwicklung und -sicherheit führen könnte.

Verordnung (EU) 2017/746 über In-vitro-Diagnostika (IVDR)

Die IVDR [82] enthält spezifische Regelungen zur Cybersicherheit von In-vitro-Diagnostika (IVD), die den Schutz vernetzter Systeme und personenbezogener Daten sicherstellen sollen. Diese Anforderungen sind in verschiedenen Artikeln und Anhängen der Verordnung detailliert beschrieben. Ein zentrales Element ist das Risikomanagement, das gemäß Anhang I, Kapitel I, Punkt 3 als fortlaufender, iterativer Prozess gestaltet sein muss. Hersteller sind verpflichtet, potenzielle Gefährdungen zu identifizieren, zu bewerten und geeignete Maßnahmen zur Risikokontrolle zu ergreifen, insbesondere für softwarebasierte und vernetzte Produkte. Ziel ist es, Cybersicherheitsrisiken während des gesamten Lebenszyklus eines Produkts kontinuierlich zu überwachen und zu minimieren. Darüber hinaus verpflichtet Artikel 68, Absatz 4 die Hersteller, technische und organisatorische Maßnahmen zu ergreifen, um verarbeitete personenbezogene Daten vor unbefugtem Zugriff, unrechtmäßiger Verarbeitung und Verlust zu schützen. Dies ist besonders wichtig bei der Übertragung sensibler Daten über Netzwerke, da der Schutz der Vertraulichkeit und Integrität dieser Daten von zentraler Bedeutung ist, insbesondere bei Produkten, die Patientendaten erfassen und verarbeiten. Des Weiteren legt Anhang I, Kapitel II, Punkt 16.2 fest, dass softwarebasierte und netzwerkfähige Produkte so gestaltet werden müssen, dass Sicherheitsrisiken minimiert werden. Dies betrifft insbesondere Produkte, die drahtlose Technologien wie Bluetooth oder WLAN verwenden, wobei Maßnahmen zum Schutz vor Cyberangriffen implementiert werden müssen, um die Funktionalität der

Geräte und die Integrität der Daten zu gewährleisten. Gemäß Artikel 78 sind Hersteller außerdem dazu verpflichtet, ein System zur Überwachung nach dem Inverkehrbringen einzurichten. Dieses System dient dazu, sicherheitsrelevante Daten zu sammeln und Cybersicherheitsrisiken kontinuierlich zu bewerten, sodass notwendige Maßnahmen zur Risikominderung ergriffen werden können. Hersteller müssen sicherstellen, dass regelmäßig Updates und Sicherheitsmaßnahmen durchgeführt werden, um neuen Bedrohungen angemessen begegnen zu können. [82]

Eine der größten Schwächen der IVDR im Hinblick auf die Cybersicherheit ist der Mangel an detaillierten technischen Leitlinien. Zwar fordert die Verordnung, dass Hersteller Cybersicherheitsmaßnahmen ergreifen, es fehlen jedoch klare Vorgaben oder Standards, wie diese Maßnahmen konkret umzusetzen sind. Diese Lücke kann zu unterschiedlichen Interpretationen und Umsetzungsansätzen führen. Die Anforderungen der IVDR können für ältere IVD-Geräte schwer umzusetzen sein. Viele ältere Geräte wurden nicht mit den heutigen Cybersicherheitsanforderungen entwickelt und erfüllen möglicherweise nicht die Sicherheitsstandards, die die IVDR vorschreibt. Es gibt keine klaren Leitlinien, wie mit diesen „Legacy"-Geräten umgegangen werden soll. Hersteller und Gesundheitsdienstleister könnten daher vor der Herausforderung stehen, entweder kostspielige Nachrüstungen durchzuführen oder diese Geräte vom Markt zu nehmen, was zu erheblichen Kosten und Unsicherheiten führen kann. Ein weiteres Problem der IVDR besteht darin, dass es keine klaren Vorgaben gibt, wie schnell auf neu auftretende Cybersicherheitsbedrohungen reagiert werden muss. Obwohl die Verordnung verlangt, dass Hersteller Systeme zur Überwachung und Behebung von Risiken implementieren, fehlen spezifische Fristen für die Bereitstellung von Updates oder Sicherheitsmaßnahmen.

Verordnung (EU) 2016/679 - Datenschutz-Grundverordnung (DSGVO)

Die DSGVO regelt den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und den freien Datenverkehr in der EU. Die Verordnung stellt sicher, dass die Rechte und Freiheiten der betroffenen Personen bei der Datenverarbeitung gewahrt werden. Die DSGVO legt besonderen Wert auf den Schutz der Integrität und Vertraulichkeit personenbezogener Daten. Dies ist eng mit der Cybersicherheit verknüpft, da der Schutz vor Cyberangriffen, unbefugtem Zugriff und Datenverlust zentrale Aspekte der Verordnung sind. Unternehmen sind verpflichtet, geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Sicherheit der Daten zu gewährleisten.Darüber hinaus fördert die DSGVO eine proaktive Sicherheitsstrategie, bei der potenzielle Risiken frühzeitig erkannt und entsprechende Maßnahmen getroffen werden. [80]

Gemäß Artikel 5 der DSGVO müssen Medizingeräte, die personenbezogene Daten verarbeiten, sicherstellen, dass die Daten auf rechtmäßige, faire und transparente Weise verarbeitet werden. Die Erhebung und Verarbeitung von Gesundheitsdaten, die als besondere Kategorie personenbezogener Daten gemäß Artikel 9 gelten, erfordert dabei besondere Schutzmaßnahmen. Artikel 32 der DSGVO fordert, dass Verantwortliche und Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Im Fall von Medizingeräten bedeutet dies, dass die Cybersicherheit der Geräte den Anforderungen der DSGVO

entsprechen muss, einschließlich Maßnahmen gegen unbefugten Zugriff, Datenverlust und Cyberangriffe. Dies umfasst auch die Pseudonymisierung und Verschlüsselung von Daten. Artikel 33 und 34 der DSGVO verlangen, dass Datenschutzverletzungen, einschließlich solcher, die durch Cyberangriffe auf Medizingeräte verursacht werden, innerhalb von 72 Stunden den zuständigen Datenschutzbehörden gemeldet werden. Dies erfordert von Herstellern von Medizingeräten, Prozesse zur Erkennung und Meldung von Sicherheitsvorfällen zu implementieren.

Die DSGVO stellt hohe Anforderungen an den Datenschutz, was die Cybersicherheit von Medizingeräten direkt beeinflusst. Eine zentrale Herausforderung ist die rasche Entwicklung von Technologien und die sich ändernden Bedrohungslandschaften im Bereich der Cybersicherheit. Hersteller müssen kontinuierlich ihre Produkte an neue Sicherheitsanforderungen anpassen, um die Einhaltung der DSGVO sicherzustellen. Dies erfordert regelmäßige Software-Updates und Sicherheitspatches, um Schwachstellen zu beheben. Ein weiteres Problem ist, dass Medizingeräte oft über einen langen Zeitraum genutzt werden. Dies bedeutet, dass Hersteller sicherstellen müssen, dass auch ältere, bereits in Gebrauch befindliche Geräte den Anforderungen der DSGVO entsprechen. Die Herausforderung besteht darin, dass Cybersicherheitsrisiken sich im Laufe der Zeit ändern, was zu regelmäßigen Aktualisierungen der Sicherheitsmechanismen führen kann.

Richtlinie (EU) 2022/2555 - NIS-2-Richtlinie

Die NIS-2-Richtlinie zielt darauf ab, ein hohes gemeinsames Cybersicherheitsniveau in der Europäischen Union zu gewährleisten. Sie ersetzt die vorherige NIS-Richtlinie und erweitert deren Anwendungsbereich, um den sich entwickelnden Bedrohungen für die Cybersicherheit gerecht zu werden. Die Richtlinie legt Anforderungen für die Cybersicherheit in den Mitgliedstaaten fest und definiert die Pflichten von Organisationen, die als wesentliche oder wichtige Einrichtungen eingestuft werden. Sie erweitert nicht nur den Geltungsbereich und die Verpflichtungen gegenüber der vorherigen NIS-Richtlinie, sondern betont auch die Notwendigkeit eines koordinierten, unionsweiten Ansatzes zur Cybersicherheit. Die Anforderungen an das Risikomanagement und die Meldepflichten sind besonders relevant, da sie Organisationen dazu zwingen, proaktive Maßnahmen zur Risikominderung zu ergreifen und eine schnelle Reaktion auf Sicherheitsvorfälle zu gewährleisten. Die Betonung auf Zusammenarbeit und Informationsaustausch ist entscheidend, um eine wirksame Verteidigung gegen komplexe, grenzüberschreitende Cyberbedrohungen zu ermöglichen. Durch die Einführung strengerer Aufsichts- und Durchsetzungsmechanismen stellt die Richtlinie sicher, dass Cybersicherheit nicht nur ein technisches, sondern auch ein regulatorisches und organisatorisches Thema ist. [70]

Artikel 21 und 23 legen fest, dass wesentliche Einrichtungen, zu denen auch Einrichtungen im Gesundheitswesen und Unternehmen, die Medizingeräte produzieren, gehören, Maßnahmen zur Risikominderung ergreifen müssen. Diese Maßnahmen umfassen den Schutz vor Bedrohungen wie Ransomware und gezielten Angriffen auf vernetzte Geräte. Die Pflicht zur Meldung von Sicherheitsvorfällen sorgt für Transparenz und schnelle Reaktionsmechanismen, was insbesondere bei lebenswichtigen Medizingeräten von entscheidender Bedeutung ist. Die Durchsetzung strenger Maßnahmen (Artikel 33) wird

durch die Überwachung der Mitgliedstaaten sichergestellt. Im Bereich Medizingeräte ist dies besonders relevant, da die Aufsichtsbehörden sicherstellen müssen, dass die Hersteller und Betreiber angemessene Cybersicherheitsvorkehrungen getroffen haben, um die Integrität und Sicherheit der Geräte zu gewährleisten. Die Sanktionen für Verstöße verstärken die Verpflichtung der Hersteller, kontinuierlich sicherheitsrelevante Updates zu implementieren.

Unmittelbare Konsequenzen hat die neue Richtlinie für die Hersteller von Medizinprodukten noch nicht. Das liegt auch daran, dass Österreich die Änderungen erst in nationales Gesetz überführen muss. Die NIS-2-Richtlinie stellt Hersteller von Medizingeräten vor besondere Herausforderungen, da sie kontinuierliche Anpassungen an die Cybersicherheitslandschaft erfordert. Insbesondere die Meldepflicht und die Kooperation mit den zuständigen Behörden bedeuten für Hersteller zusätzlichen Aufwand und erfordern eine klare Zuweisung von Verantwortlichkeiten. Die Umsetzung der NIS2-Richtlinie im Bereich der Medizingeräte wird durch mehrere Herausforderungen erschwert. Eine der Hauptschwierigkeiten besteht in der Überschneidung der Meldepflichten zwischen der NIS2-Richtlinie und der MDR [81]. Während die NIS2-Richtlinie Gesundheitsdienstleister als „wesentliche Einheiten“ einstuft und ihnen strenge Meldepflichten bei Cybersicherheitsvorfällen auferlegt, fordert die MDR [81] von Herstellern medizinischer Geräte die Meldung schwerwiegender Vorfälle, die die Patientensicherheit betreffen. Dies kann zu zwei Wegen für die Meldepflichten führen. Zusätzlich gibt es Herausforderungen durch abweichende Anforderungen an die Meldefristen in beiden Regelungen. Die NIS2-Richtlinie verlangt eine Benachrichtigung innerhalb von 24 Stunden nach Entdeckung eines Vorfalls, während die MDR [81] eine Frist von bis zu 15 Tagen gewährt.

Verordnung (EU) 2019/881 - Rechtsakt zur Cybersicherheit

Die Verordnung (EU) 2019/881, auch bekannt als Cybersecurity Act, legt den rechtlichen Rahmen für die Arbeit der Agentur der Europäischen Union für Cybersicherheit (ENISA) fest und führt ein europäisches Zertifizierungsprogramm für die Cybersicherheit von Informations- und Kommunikationstechnik (IKT) ein. Die Verordnung stärkt die Rolle der ENISA und etabliert verbindliche Regeln für die Cybersicherheitszertifizierung innerhalb der EU. Die Verordnung (EU) 2019/881 stellt einen bedeutenden Schritt zur Stärkung der Cybersicherheitsinfrastruktur in der EU dar. Durch die Einführung eines einheitlichen Zertifizierungssystems wird das Vertrauen in die Sicherheit von IKT-Produkten und -Diensten erhöht, was besonders im Hinblick auf den zunehmenden Einsatz vernetzter Geräte und das Internet der Dinge (IoT) wichtig ist. Die Stärkung der ENISA als zentrale Instanz für Cybersicherheit in der EU unterstützt die Mitgliedstaaten dabei, ein hohes Niveau an Cybersicherheit zu erreichen und grenzüberschreitende Cyberbedrohungen effektiver zu bekämpfen. Die Betonung auf „Security by Design“ und „Security by Default“ ist besonders relevant, da diese Ansätze dazu beitragen, Sicherheitslücken von Anfang an zu minimieren und die Notwendigkeit nachträglicher Patches zu reduzieren. Dies ist ein wichtiger Aspekt im Kampf gegen die zunehmenden und immer komplexeren Cyberbedrohungen. [83]

Cybersecurity Act ist in erster Linie auf die Cybersicherheit von Informations- und Kommunikationstechnologie (IKT)-Produkten, -Dienstleistungen und -Prozessen ausgerichtet. Der Schwerpunkt dieser Verordnung liegt auf der Schaffung eines europaweiten Zertifizierungsrahmens für die Cybersicherheit dieser IKT-Produkte, nicht jedoch speziell auf Medizingeräten. Der Cybersecurity Act könnte jedoch in bestimmten Fällen anwendbar sein, wenn es um IKT-Komponenten oder Netzwerksysteme geht, die in Medizingeräten integriert sind. Zum Beispiel wenn Medizingeräte auf Software oder Netzwerksysteme angewiesen sind, die IKT-Sicherheitsanforderungen unterliegen, könnte der Zertifizierungsrahmen relevant sein. Eine der größten Schwierigkeiten ist die Integration von Cybersicherheitszertifizierungen in den stark regulierten Markt für Medizingeräte. Der Cybersecurity Act zielt darauf ab, eine einheitliche Zertifizierung für Cybersicherheitsmaßnahmen innerhalb der EU zu etablieren. Allerdings stehen Hersteller von Medizingeräten vor dem Problem, dass diese Zertifizierungen in bestimmten Mitgliedstaaten unterschiedlich umgesetzt und angewendet werden könnten, was die Harmonisierung im gesamten Binnenmarkt erschwert. Zudem gibt es Überschneidungen zwischen bestehenden und neuen Anforderungen des Cybersecurity Act und den spezifischen Vorschriften der MDR [81]. Während der Cybersecurity Act eine allgemeine Cybersicherheitszertifizierung fordert, verlangen die MDR [81] und die NIS2-Richtlinie [70] spezifische, sektorgebundene Maßnahmen. Die Koordination dieser unterschiedlichen Anforderungen stellt eine Herausforderung dar, da Unklarheiten darüber bestehen, welche Normen und Zertifizierungen vorrangig sind und wie diese Regelungen in der Praxis nebeneinander existieren können

3.3.4 Relevante Normen für die Cybersicherheit von Medizinprodukten

Die Cybersicherheit von Medizinprodukten wird durch eine Vielzahl von internationalen Normen sichergestellt. Im Folgenden werden die wichtigsten Normen zusammengefasst, die für die Cybersicherheit von Medizinprodukten relevant sind:

EN ISO 13485 - Medizinprodukte - Qualitätsmanagementsysteme - Anforderungen für regulatorische Zwecke

Die EN ISO 13485 ist eine Norm, die Anforderungen an Qualitätsmanagementsysteme für Organisationen definiert, die in der Herstellung von Medizinprodukten tätig sind. Diese Norm stellt sicher, dass Medizinprodukte und zugehörige Dienstleistungen konsequent die Anforderungen der Kunden sowie die geltenden gesetzlichen Vorschriften erfüllen. Im Bezug auf Cybersicherheit ist das Kapitel 7 Produktrealisierung vor allem relevant. Der Entwicklungsprozess von Medizinprodukten umfasst mehrere Phasen, darunter Planung, Eingaben, Ergebnisse, Bewertung, Verifizierung und Validierung. Die Ergebnisse der Entwicklung müssen den festgelegten Anforderungen entsprechen und eine sichere Anwendung des Produkts gewährleisten. Ein weiterer wichtiger Aspekt ist die Beschaffung. Hier müssen Kriterien für die Beurteilung und Auswahl von Lieferanten festgelegt und deren Leistung überwacht werden, um sicherzustellen, dass die beschafften Produkte den Anforderungen entsprechen. Die Produktion und Dienstleistungserbringung müssen ebenfalls genau überwacht werden, insbesondere hinsichtlich der Installation, Instandhaltung

und Validierung von Prozessen. Ein bedeutender Abschnitt der Norm befasst sich mit der Messung, Analyse und Verbesserung. Organisationen sind verpflichtet, Rückmeldungen zu sammeln und auszuwerten, einschließlich der Berichterstattung an Regulierungsbehörden im Falle bestimmter unerwünschter Ereignisse oder Reklamationen. [29]

Hinsichtlich der Cybersecurity, obwohl die Norm nicht explizit auf dieses Thema eingeht, gibt es mehrere Bereiche, in denen Cybersecurity implizit eine Rolle spielt. Beispielsweise betonen die Anforderungen an das Risikomanagement und die Entwicklungsplanung die Notwendigkeit, alle relevanten Risiken, einschließlich Cybersecurity-Risiken, zu identifizieren und zu mindern. Auch die Validierung von Prozessen und Produkten muss sicherstellen, dass die entwickelten Systeme sicher und zuverlässig sind, was den Schutz vor Cyberangriffen einschließt. Zudem verlangen die Abschnitte zur Kommunikation und Dokumentation eine gründliche Erfassung und Verfolgung aller relevanten Informationen, was auch Sicherheitsvorfälle und Cybersecurity-Updates umfassen sollte. Besonders relevant sind dabei die Anforderungen an die Verbindung und Schnittstellen von Medizinprodukten, die verifiziert und validiert werden müssen, um sicherzustellen, dass sie den Sicherheitsanforderungen entsprechen. Die Notwendigkeit von Anwenderschulungen zur Sicherstellung der sicheren Anwendung von Medizinprodukten wird ebenfalls betont. Dies könnte auch Schulungen zu sicheren digitalen Praktiken umfassen. Zudem ist die Erfüllung regulatorischer Anforderungen essenziell, wobei zunehmend auch Anforderungen an die Cybersecurity von Medizingeräten gestellt werden.

Die EN ISO 13485 passt sich außerdem den Anforderungen der MDR [81] und IVDR [82] an.

EN ISO 14971 - Medizinprodukte - Anwendung des Risikomanagements auf Medizinprodukte

Die EN ISO 14971 beschreibt den Prozess des Risikomanagements speziell für Medizinprodukte und deren Zubehör. Ziel dieser Norm ist es, einen systematischen Ansatz bereitzustellen, um die mit der Nutzung von Medizinprodukten verbundenen Risiken zu identifizieren, zu bewerten, zu kontrollieren und kontinuierlich zu überwachen. Der Anwendungsbereich umfasst alle Medizinprodukte und Zubehörteile und stellt sicher, dass Risiken während des gesamten Lebenszyklus des Produkts angemessen beherrscht werden. Der Risikomanagement-Prozess, der in der Norm detailliert beschrieben wird, besteht aus mehreren Schritten. Dazu gehören die Risikoanalyse, Risikobewertung, Risikokontrolle sowie die fortlaufende Überwachung. Die Ergebnisse dieses Prozesses müssen dokumentiert und regelmäßig überprüft werden. Eine wichtige Rolle spielt dabei die Unternehmensleitung, die dafür verantwortlich ist, dass die notwendigen Ressourcen für das Risikomanagement zur Verfügung stehen und die entsprechenden Prozesse im Unternehmen implementiert werden. Ein weiterer zentraler Punkt der Norm ist die Kompetenz des Personals. Es wird gefordert, dass das Personal, das mit dem Risikomanagement betraut ist, über die notwendige Ausbildung und Kompetenz verfügt, um Risiken adäquat zu identifizieren und zu bewerten. Die Risikokontrolle sieht vor, dass Risiken so weit wie möglich reduziert werden müssen, entweder durch ihre vollständige Eliminierung oder durch eine Reduzierung auf ein akzeptables Niveau. Ein wesentlicher Bestandteil dieser

Risikokontrolle ist die Analyse des Restrisikos, also des verbleibenden Risikos nach der Implementierung von Kontrollmaßnahmen. Falls Restrisiken bestehen, muss eine Nutzen-Risiko-Analyse durchgeführt werden, um festzustellen, ob der Nutzen des Produkts das verbleibende Risiko überwiegt. Nach der Markteinführung eines Medizinprodukts verlangt die Norm eine fortlaufende Überwachung und Sammlung von Informationen, um sicherzustellen, dass die getroffenen Risikokontrollen weiterhin wirksam sind. [30]

Die EN ISO 14971 behandelt explizit auch Aspekte der Cybersecurity, die für Medizinprodukte relevant sind. Im Anhang C werden verschiedene Sicherheitsgefährdungen und Umstände beschrieben, die speziell auf Cybersecurity hinweisen:

1. Datenbezogene Gefährdungen - Zugang, Verfügbarkeit, Vertraulichkeit, Übertragung und Integrität von Daten werden als mögliche Gefährdungen aufgelistet.
2. Sicherheitsbezogene Ereignisse und Umstände - Ungesicherte Datenanschlüsse (z.B. Netzwerkanschlüsse, serielle Anschlüsse, USB-Anschlüsse). - Unverschlüsselte Daten. - Software-Schwachstellen, die ausgenutzt werden können. - Software-Aktualisierungen ohne Bestätigung der Authentisierung.

Mit Berücksichtigung dieser Punkte in der Risikoanalyse bietet die EN ISO 14971 dem Hersteller eine grundlegenden Rahmen, um sicherzustellen, dass Cyber-Risiken effektiv und aktiv bewältigt werden.

Die EN ISO 14971 passt sich außerdem den Anforderungen der MDR [81] und IVDR [82] an. Die Einhaltung dieser Norm ist somit entscheidend für die Erfüllung regulatorischer Anforderungen und den Schutz der Patientensicherheit bei der Nutzung von Medizinprodukten. Während EN ISO 14971 das Risikomanagement für physische und funktionale Aspekte von Medizinprodukten abdeckt, ergänzen EN ISO/IEC 27001 [32] und ISO 27799 [45] diese durch das Management von Informationssicherheitsrisiken, insbesondere bei vernetzten Medizingeräten und der Verarbeitung sensibler Gesundheitsdaten. Ein integrierter Ansatz, der sowohl physische als auch informationstechnische Risiken berücksichtigt, ist entscheidend. Dies erfordert die Implementierung von Sicherheitskontrollen aus EN ISO/IEC 27001 [32] und ISO 27799 [45] parallel zum Risikomanagementprozess nach EN ISO 14971. Die EN ISO 14971 und die EN 62304 [21] sind eng miteinander verknüpft, da beide Normen Risikomanagement verlangen, speziell für die Entwicklung und Wartung von Software in Medizingeräten. Hersteller sollte sicherstellen, dass der Software-Entwicklungsprozess gemäß EN 62304 [21] nahtlos in den Risikomanagementprozess nach EN ISO 14971 integriert ist.

EN 62304 - Medizingeräte-Software – Software-Lebenszyklus- Prozesse

Die EN 62304 legt umfassende Anforderungen für die Entwicklung und Wartung von Software in Medizinprodukten fest, mit dem Ziel, deren Sicherheit und Wirksamkeit zu gewährleisten. Die Norm gilt für eigenständige Medizinsoftware sowie für Software, die Teil eines Medizinprodukts ist, und sieht eine Klassifizierung in drei Sicherheitsklassen (A, B, C) vor, basierend auf dem potenziellen Risiko für den Patienten. Der Entwicklungsprozess umfasst die Erstellung eines Entwicklungsplans, die Analyse von Sicherheitsanforderungen

(wie Datenschutz und Authentifizierung) und die Integration und Verifikation aller Softwarekomponenten. [21]

Für die Softwarewartung beschreibt die Norm einen Wartungsplan, der eine systematische Erfassung und Bearbeitung von Rückmeldungen sicherstellt. Ein zentraler Bestandteil der Norm ist das Risikomanagement, das die Identifikation und Kontrolle risikobehafteter Software-Komponenten verlangt, um Gefährdungssituationen zu verhindern. Zusätzlich wird ein Problemlösungsprozess vorgeschrieben, der die Untersuchung und Behebung aller entdeckten Probleme dokumentiert. Cybersicherheit wird in der EN 62304 nicht als separates Thema behandelt. Es werden jedoch Aspekte integriert. Im Kapitel 5.2 Analyse der Software Anforderungen wird vom Hersteller für alle Sicherheitsklassen gefordert, dass Anforderungen für die Datensicherheit sowie Anforderungen an die Benutzerschnittstelle, die durch Software implementiert ist, definiert werden. Zusätzlich sollen Anforderungen bezüglich IT-Netzwerk-Aspekten festgelegt werden. Es wird zwar auch ein Risikomanagementprozess vom Hersteller gefordert, indem potenzielle Gefährdungssituationen und deren Ursachen identifiziert und entsprechende Maßnahmen zur Risikobeherrschung implementiert werden. Allerdings gibt es keinen zusätzliches Unterkapitel bezüglich Cybersicherheit oder angeführte Beispiele. Der Wartungsprozess stellt sicher, dass nach der Freigabe auftretende Sicherheitsprobleme systematisch dokumentiert, untersucht und behoben werden, was eine grundlegende Grundlage für den Schutz medizinischer Software vor Cyberbedrohungen darstellt. Ein weiterer Aspekt für die Cybersicherheit wird im Zuge des Problemlösungsprozess beleuchtet. In diesem Kapitel wird vom Hersteller erwartet, dass er für jedes Problem mit der Medizinprodukt-Software einen Problembericht erstellt, indem auch die Auswirkungen auf die Datensicherheit diskutiert werden müssen. [21]

Die EN 62304 deckt sich im Punkt mit der Entwicklung und Konfiguration mit den Anforderungen der EN ISO 13485 [29]. Im Vergleich mit der EN ISO 14971 [30], schafft es die EN 62304 den Bezug auf die Software zu erweitern, bietet aber im Aspekt mit der Cybersicherheit noch zu wenig Information beziehungsweise Beispiele. Die EN 62304 bietet ein kleines Grundgerüst für die Cybersicherheit der Medizinprodukt-Software, ist aber alleine nicht ausreichend.

IEC 60601-1 - Medical electrical equipment – Part 1: General requirements for basic safety and essential performance

Die IEC 60601-1 definiert grundlegende Sicherheits- und Leistungsanforderungen für medizinische elektrische Geräte, um Risiken für Patienten und Anwender zu minimieren. Die Norm fordert einen Risikomanagement-Prozess, sichert essentielle Leistungsmerkmale und spezifiziert Schutzmaßnahmen gegen elektrische, mechanische und Strahlungsgefahren. Für programmierbare Systeme gelten zusätzliche Anforderungen zur Vermeidung unsicherer Zustände durch Softwarefehler. Detaillierte Kennzeichnungen, Dokumentationen und Tests gewährleisten die Sicherheit und Zuverlässigkeit dieser Geräte. [39]

Kapitel 14.6 fordert die Identifikation bekannter und vorhersehbarer Gefahren, einschließlich solcher, die durch Software- und Hardwarefehler oder die Integration in IT-Netzwerke entstehen können. Hierbei wird ausdrücklich auf Gefahren wie unerwünschtes Feedback,

Datenverlust, Datenintegrität und unautorisierte Datenzugriffe hingewiesen. Diese Anforderungen sind direkt auf die Cybersicherheit anwendbar, da sie sicherstellen, dass potenzielle Schwachstellen und Bedrohungen frühzeitig erkannt und adressiert werden. Das Kapitel 14.8 legt fest, dass das Design von PEMS auf einer robusten Architektur basieren muss, die unter anderem Redundanz, Fehlersicherheit und Schutz vor Fehlverhalten umfasst. Diese Maßnahmen sind wesentlich, um sicherzustellen, dass Medizingeräte auch im Falle eines Cyberangriffs oder Systemfehlers sicher weiterarbeiten können. Besondere Anforderungen gelten für PEMS, die in IT-Netzwerke integriert werden sollen (siehe Kapitel 14.13). Hierbei müssen Sicherheitsvorgaben für die Netzwerkkonfiguration und die Datenübertragung berücksichtigt werden, um sicherzustellen, dass die Verbindung des Medizingeräts zu einem Netzwerk nicht zu Sicherheitsrisiken führt. Dies schließt auch die Notwendigkeit ein, dass Hersteller klare Anweisungen zur sicheren Implementierung und zum Betrieb in einem Netzwerk bereitstellen.

Die IEC 60601-1 verlangt ein umfassendes Risikomanagement für medizinische elektrische Geräte und knüpft dabei direkt an die EN ISO 14971 [30] an, welche den Prozess zur Risikobewertung und -minimierung für Medizingeräte definiert. Die Norm fordert Sicherheits- und Risikokontrollmaßnahmen, die sich systematisch in einem Informationssicherheits-Managementsystem (ISMS) gemäß EN ISO/IEC 27001 [32] umsetzen lassen.

EN 82304-1 - Gesundheitssoftware Teil 1: Allgemeine Anforderungen für die Produktsicherheit

Die EN 82304-1 Norm befasst sich umfassend mit dem gesamten Lebenszyklus von Gesundheitssoftware-Produkten, von der Planung und Entwicklung über die Validierung und Installation bis hin zur Wartung und Außerbetriebnahme. Sie zielt darauf ab, die Sicherheit, Effektivität sowie die Daten- und Systemsicherheit dieser Software während ihrer gesamten Nutzung sicherzustellen. Ein zentraler Bestandteil der Norm ist das Risikomanagement, das darauf abzielt, Gefährdungen zu identifizieren und zu bewerten, die bei der Bereitstellung, Nutzung oder Außerbetriebnahme der Gesundheitssoftware auftreten können. Organisationen müssen sicherstellen, dass die Kriterien des Risikomanagements mit denen der Softwarehersteller übereinstimmen. Dies schließt eine umfassende Dokumentation und Kommunikation ein, um die Einhaltung der Norm nachzuweisen. Dazu gehören Risikobewertungen, Testprotokolle und Nachweise über die Implementierung von Sicherheitsmaßnahmen, wobei alle relevanten Akteure angemessen informiert und in den Prozess eingebunden werden müssen. Ein weiterer wichtiger Aspekt ist die Validierung und Verifikation der Gesundheitssoftware. Sie muss getestet und überprüft werden, um sicherzustellen, dass sie den festgelegten Anforderungen entspricht und sicher betrieben werden kann. Dies beinhaltet die Durchführung von Tests und Überprüfungen, um die Integrität und Sicherheit der Software zu bestätigen. [23]

Obwohl die EN 82304-1 Norm speziell für Gesundheitssoftware gilt, die unabhängig von spezifischer Hardware arbeitet, sind ihre Prinzipien und Anforderungen auch auf Medizingeräte anwendbar. Die Norm verlangt bereits bei der Definition der Nutzungsanforderungen, dass der der Hersteller die Sicherstellung der Privatsphäre und Informationssicherheit, wie Authentifizierung, Datenintegrität und Schutz vor böswilligen Absichten

definiere muss (Kapitel 4.2). Diese müssen auch verifiziert werden (Kapitel 4.3). Ebenfalls bei den Systemanforderungen wird der Hersteller schon aufgefordert sich Anforderungen bezüglich Interoperabilität und muss Merkmale bezüglich Beeinträchtigung der Informationssicherheit ermitteln, erkennen und protokollieren (Kapitel 4.5). Zusätzlich wird gefordert, dass Merkmale zum Schutz der wesentlichen Funktionen definiert werden um zum Beispiel im Notfallbetriebsmodus die wesentlichen Funktionen aufrechterhält, selbst wenn die Software angegriffen wird. In der Gebrauchsanweisung muss der Hersteller Informationen bezüglich den Einstellungen zur Informationssicherheit enthalten, sowie eine Beschreibung der Reaktion der Software, wenn die Informationssicherheit komprimiert wurde (Kapitel 7). Wenn die Software in einem fremden IT-Netzwerk betrieben wird, muss der Hersteller seine Anforderungen beschreiben, die das fremde IT-Netzwerk erfüllen muss, damit die Software einwandfrei funktioniert.

Die DSGVO [80] spielt eine wichtige Rolle bei der Informationssicherheit, die in der EN 82304-1 ebenfalls behandelt wird. Insbesondere in Bezug auf den Schutz personenbezogener Daten und die Sicherstellung der Privatsphäre kann mithilfe der Umsetzung der EN 82304-1 erreicht werden. Die EN 82304-1 basiert stark auf der EN 62304 [21] und erfordert, dass Gesundheitssoftware den gesamten Lebenszyklus der Softwareentwicklung abdeckt, von der Konzeption über das Design bis hin zur Wartung. Sie ergänzt die EN 62304 [21] um die zusätzlichen Punkte im Hinblick der Informationssicherheit und deckt die Validierung der Software ab und kann in den Entwicklungsprozess leicht hinzugefügt werden. Vor allem wenn die Software als ein eigenständiges Medizinprodukt deklariert wird, ist die Validierung nach der IEC 60601-1 [39] nicht mehr anwendbar.

EN IEC 80001-1 - Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten Teil 1: Sicherheit, Effektivität, Daten- und Systemsicherheit bei Implementierung und Gebrauch von eingebundenen Medizinprodukten oder eingebundener Gesundheitssoftware

Die Norm EN IEC 80001-1 beschreibt die Anforderungen an das Risikomanagement für IT-Netzwerke, die medizinische Geräte und Gesundheitssoftware beinhalten. Diese Norm legt fest, dass Organisationen in allen Phasen des Lebenszyklus eines IT-Systems im Gesundheitswesen ein umfassendes Risikomanagement durchführen müssen, um die Schutzziele Sicherheit, Effektivität sowie Daten- und Systemsicherheit zu gewährleisten. Das Risikomanagement ist dabei ein integraler Bestandteil aller Aktivitäten und wird von der Gesundheitsorganisation verantwortet, obwohl bestimmte Verantwortlichkeiten delegiert werden können. Ein strukturierter Ansatz ist notwendig, um einheitliche und vergleichbare klinische Ergebnisse zu erzielen, und es wird besonderer Wert darauf gelegt, proaktiv auf Veränderungen und Risiken zu reagieren. Das soziotechnische Umfeld, in dem die Organisation agiert, hat dabei großen Einfluss auf alle Aspekte des Risikomanagements. Der Risikomanagementprozess umfasst die Risikoanalyse, Risikobewertung und Risikobeherrschung über den gesamten Lebenszyklus des IT-Systems. Organisationen müssen einen detaillierten Risikomanagementplan erstellen, der alle relevanten Aktivitäten und Verantwortlichkeiten festlegt. Dieser Prozess beginnt bei der Beschaffung und Installation der Systeme und erstreckt sich über ihre gesamte Betriebsdauer bis hin zur

Außerbetriebnahme. Ein wichtiger Aspekt der Norm ist die kontinuierliche Bewertung der Wirksamkeit des Risikomanagementplans, um sicherzustellen, dass alle Maßnahmen den aktuellen Anforderungen entsprechen. Darüber hinaus sollten Organisationen ständig nach Möglichkeiten suchen, den Risikomanagementprozess zu verbessern, basierend auf neuen Erkenntnissen und sich verändernden Bedingungen. Insgesamt bietet die Norm eine umfassende Anleitung zur Sicherstellung der Sicherheit, Effektivität und Daten- sowie Systemsicherheit in vernetzten Gesundheitssystemen. [27]

Die Grundsätze der EN IEC 80001-1 im Kapitel 4 betonen die Notwendigkeit eines umfassenden und integrierten Risikomanagements für IT-Systeme im Gesundheitswesen. Die EN IEC 80001-1 bezieht sich allerdings auf die Gesundheitsorganisationen und nicht auf den Hersteller selbst und ist auf Medizingeräte selbst nicht anwendbar. Bei der Umsetzung der EN ISO 14971 [30] werden bereits die angeführten Anforderungen der EN IEC 80001-1 erfüllt. Es werden auch keine speziellen Anforderungen an die Hersteller definiert, die dieser für eine Integration in ein IT-System umsetzen muss.

ISO 81001-1 - Health software and health IT systems safety, effectiveness and security – Part 1: Principles and concepts

Die ISO 81001-1 legt grundlegende Prinzipien für die Sicherheit, Wirksamkeit und Schutz von Gesundheitssoftware und -IT-Systemen fest und fordert ein Lebenszyklusmanagement, um Risiken zu minimieren. Sie betont das komplexe soziotechnische Umfeld, in dem diese Systeme eingesetzt werden, und die Notwendigkeit eines koordinierten Managements aller Systeme und Komponenten im Gesundheitswesen. Die Norm definiert klare Rollen und Verantwortlichkeiten sowie ein systematisches Risikomanagement, um Gefahren frühzeitig zu erkennen und zu kontrollieren.[46]

Das Sicherheitsmanagement (siehe 5.3.4) ist essentiell, um sicherzustellen, dass alle möglichen Sicherheitsrisiken während des gesamten Lebenszyklus eines Medizingeräts identifiziert und adressiert werden. Dies schließt die Entwicklung von Sicherheitsstrategien, die Implementierung von Sicherheitsmaßnahmen sowie die kontinuierliche Überwachung und Anpassung der Sicherheitsvorkehrungen ein. Diese proaktive Haltung hilft, potenzielle Schwachstellen frühzeitig zu erkennen und zu beheben. Die Norm fordert die Implementierung eines strukturierten Prozesses zur Bewertung von Sicherheitsrisiken und die Ergreifung entsprechender Maßnahmen, um diese Risiken zu minimieren (siehe 5.3.2). Insbesondere für Medizingeräte, die direkt mit der Gesundheit und Sicherheit von Patienten verbunden sind, ist dies von entscheidender Bedeutung, um potenzielle Gefahren zu minimieren. Medizingeräte müssen in bestehende IT-Systeme und Netzwerke integriert werden, was eine sichere und reibungslose Interoperabilität erfordert. Die Norm fordert, dass die Cybersicherheitsanforderungen auch bei der Integration und dem Zusammenspiel verschiedener Systeme berücksichtigt werden (sieh 4.3). Die Norm betont die Bedeutung der Schulung und Kompetenzentwicklung für alle Beteiligten (siehe 5.2.2).

Die Einhaltung der ISO 81001-1 hilft Herstellern, die Anforderungen der MDR [81] in Bezug auf die Sicherheit und Leistung von Medizingeräten zu erfüllen, insbesondere

hinsichtlich der Sicherheitsanforderungen. ISO 81001-1 ergänzt die EN 62304 [21], indem sie spezifische Anforderungen an die Sicherheit, Wirksamkeit und Sicherheit von Gesundheitssoftware und IT-Systemen definiert. Die EN 62304 [21] fokussiert auf die Softwareentwicklungsprozesse, während ISO 81001-1 sicherstellt, dass Sicherheitsaspekte in jedem Schritt des Softwarelebenszyklus berücksichtigt werden. Die Risikomanagementprozesse in ISO 81001-1 können direkt mit EN ISO 14971 [30] verbunden werden, um ein umfassendes Management der Risiken, die mit der Nutzung von Medizingeräten verbunden sind, zu gewährleisten. ISO 81001-1 erweitert EN ISO 14971 [30] um spezifische Anforderungen an die Cybersicherheit.

EN IEC 81001-5-1 - Gesundheitssoftware und Gesundheits-IT-Systeme Sicherheit, Effektivität und Security - Teil 5-1: Security - Aktivitäten im Produktlebenszyklus

Die Norm EN IEC 81001-5-1 legt umfassende Cybersicherheitsanforderungen für Medizingeräte fest und strukturiert diese entlang des gesamten Produktlebenszyklus. Die Norm fordert zunächst die Integration der Cybersicherheitsaktivitäten in ein Qualitätsmanagementsystem (QMS) gemäß Kapitel 4.1 und 4.2, das etwa auf ISO 13485 basiert. Hierbei müssen klare Rollen und Verantwortlichkeiten für die Cybersicherheit festgelegt werden, sodass alle Mitarbeitenden im Lebenszyklus eines Produkts wissen, welche Sicherheitsanforderungen zu berücksichtigen sind. Cybersicherheit wird so zu einem festen Bestandteil der Qualitätskultur im Unternehmen. Ein zentraler Bestandteil ist das Risikomanagement in Kapitel 5.1 bis 5.4. Cybersicherheitsrisiken müssen durchgehend systematisch bewertet werden, wobei Bedrohungen wie unbefugter Zugriff und Datenverlust identifiziert werden. Diese lebenszyklusorientierte Risikobewertung sorgt dafür, dass nicht nur in der Entwicklungsphase, sondern auch während der Nutzung und Wartung potenzielle Risiken adressiert werden, um Cybersicherheitsanforderungen kontinuierlich an die aktuelle Bedrohungslage anzupassen. In Kapitel 6 sind detaillierte Sicherheitsmaßnahmen festgelegt. Insbesondere Kapitel 6.2 bis 6.4 verlangen technische Sicherheitskontrollen wie Identifikations- und Authentifizierungsprotokolle, um sicherzustellen, dass nur autorisierte Benutzer oder Systeme Zugriff auf das Gerät haben. Diese Anforderungen gelten insbesondere für vernetzte Geräte, deren Kommunikation durch Verschlüsselung und andere Schutzmaßnahmen gesichert sein muss, um die Integrität und Vertraulichkeit der Informationen zu gewährleisten. Lebenszyklusprozesse und Dokumentation werden in Kapitel 7.1 bis 7.6 ausführlich behandelt. Cybersicherheitsaktivitäten müssen kontinuierlich über den gesamten Lebenszyklus des Geräts erfolgen, was sichere Entwicklung, Integration, regelmäßige Tests und Sicherheitsüberprüfungen umfasst. Hierzu gehört auch eine umfassende Dokumentation der Sicherheitsmaßnahmen, die sowohl internen Überprüfungen als auch als Nachweis für Behörden dient, um die Einhaltung der Sicherheitsstandards zu belegen. Abschließend beschreibt Kapitel 8 das Vorfall- und Problemmanagement, das in den Unterkapiteln 8.2 und 8.3 strukturiert ist. Hersteller müssen Prozesse zur Erfassung, Bewertung und Behebung von Cybersicherheitsvorfällen etablieren. Der Problemlösungsprozess umfasst die Berichterstattung und Ursachenanalyse, um Sicherheitslücken zeitnah zu beheben und zukünftige Risiken zu minimieren.

Regelmäßige Anpassungen der Sicherheitsmaßnahmen sind erforderlich, um auf neue Bedrohungen und technologische Entwicklungen reagieren zu können. [28]

Die Umsetzung dieser Norm ist besonders wichtig, da sie eine umfassende Grundlage für die Entwicklung, Implementierung und Wartung sicherer Medizingeräte, indem sie spezifische Anforderungen an die Cybersecurity und die Minimierung von Risiken im gesamten Produktlebenszyklus berücksichtigt. Die Anforderungen aus der NIST [65], EN IEC 62443-Reihe und FDA Guidance-Dokumente wurden speziell für den Health Software umgemünzt. Da MDR [81] und IVDR [82] spezifische Sicherheitsanforderungen für Medizinprodukte festlegen, ist die Berücksichtigung von EN IEC 81001-5-1 notwendig, um den Schutz vor Cyberrisiken zu gewährleisten und regulatorische Compliance zu erreichen. Die EN 62304 [21] definiert den Lebenszyklus von Software für Medizinprodukte und ist stark mit der EN IEC 81001-5-1 verbunden. Die EN IEC 81001-5-1 setzt eine Entwicklungsprozess gemäß der EN 62304 [21] bereits voraus und definiert welche spezifischen Aktivitäten in den entsprechenden Phasen des Entwicklungsprozesses notwendig sind, um Cybersecurity zu gewährleisten. Dasselbe gilt für die EN 82304-1 [23]. Außerdem erweitert die Norm die EN ISO 14971[30] durch spezielle Anforderungen an das IT-Sicherheitsrisikomanagement. Jedoch könnten präzisere Vorgaben hilfreich sein, um die Erfüllung der Anforderungen zu erleichtern.

EN ISO/IEC 27000 - Information technology — Security techniques — Information security management systems — Overview and vocabulary

Die Norm EN ISO/IEC 27000 bietet einen umfassenden Überblick über Informationssicherheits - Managementsysteme (ISMS) und definiert wesentliche Begriffe, die in der ISMS - Normenfamilie häufig verwendet werden. Sie ist auf Organisationen jeglicher Art und Größe anwendbar, einschließlich Unternehmen, Behörden und gemeinnützigen Organisationen. Die Norm beschreibt ein Rahmenwerk, das Organisationen dabei unterstützt, die Sicherheit ihrer Informationswerte, wie finanzielle Daten, geistiges Eigentum und personenbezogene Informationen, zu verwalten. Sie fördert die Entwicklung und Umsetzung geeigneter Maßnahmen zum Schutz dieser Informationen. Ein zentrales Element der Norm ist das ISMS, ein systematischer Ansatz, der Richtlinien, Verfahren und Ressourcen umfasst, um die Informationswerte einer Organisation zu schützen. Dieser Ansatz basiert auf einer Risikobewertung und hilft Organisationen, Risiken effektiv zu managen und ihre Sicherheitsziele zu erreichen. Zu den grundlegenden Prinzipien eines ISMS zählen das Bewusstsein für die Notwendigkeit von Informationssicherheit, die Übertragung von Verantwortung, die Verpflichtung der Geschäftsführung, die Durchführung von Risikobewertungen sowie die Integration von Sicherheitsmaßnahmen in Informationssysteme und Netzwerke. Ein ISMS trägt dazu bei, Informationen gegen vielfältige Bedrohungen zu schützen, und stellt sicher, dass Sicherheitsmaßnahmen effektiv in die Unternehmensprozesse integriert werden. [31]

Die regelmäßige Bewertung und Behandlung von Risiken stellt sicher, dass Medizingeräte gegen aktuelle und zukünftige Bedrohungen geschützt sind. Ein ISMS hilft zudem, regulatorische Anforderungen zu erfüllen und gewährleistet, dass Sicherheitsmaßnahmen stets auf dem neuesten Stand sind. Ein weiteres Schlüsselelement der EN ISO/IEC 27000

ist die kontinuierliche Überwachung und Verbesserung der Sicherheitsmaßnahmen. Für Medizingeräte bedeutet dies, dass Hersteller regelmäßig die Sicherheit ihrer Produkte überprüfen und sicherstellen müssen, dass alle Software-Updates und Sicherheits-Patches zeitnah implementiert werden. Dies hilft, neue Bedrohungen zu erkennen und die Sicherheit der Geräte kontinuierlich zu verbessern. Die MDR verlangt, dass Hersteller die Sicherheit ihrer Produkte über den gesamten Lebenszyklus hinweg gewährleisten, einschließlich der Cybersicherheit. Die Implementierung der EN ISO/IEC 27000 unterstützt die Einhaltung dieser regulatorischen Anforderungen, indem sie sicherstellt, dass Informationssicherheitsmaßnahmen umfassend und systematisch angewendet werden. EN ISO 14971 [30] bietet ein Rahmenwerk für das Risikomanagement von Medizinprodukten, das durch die Risikobewertungsprozesse der EN ISO/IEC 27000 ergänzt werden kann, um speziell auf Cyberrisiken einzugehen. Die EN ISO/IEC 27000 bildet die Basis für ein gemeinsames Verständnis und die Anwendung der nachfolgenden Normen, insbesondere EN ISO/IEC 27001 [32] und EN ISO/IEC 27002 [33]. Die Norm dient als Leitfaden für das Verständnis und die Implementierung der spezifischen Anforderungen und Kontrollen, die in den weiteren Normen beschrieben werden.

EN ISO/IEC 27001 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Die EN ISO/IEC 27001 spezifiziert Anforderungen für die Einrichtung, Pflege und Verbesserung eines Informationssicherheitsmanagementsystems (ISMS) in Organisationen. Sie verfolgt einen risikobasierten Ansatz, um Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicherzustellen und das Vertrauen der Interessengruppen zu stärken. Die Norm betont das Engagement des Managements, die Integration des ISMS in Geschäftsprozesse und die Bereitstellung notwendiger Ressourcen. Sie verlangt, Risiken zu bewerten, Sicherheitsziele festzulegen und deren Erreichung zu planen. Die Leistung des ISMS wird regelmäßig überwacht, und Organisationen sollen durch Korrekturmaßnahmen und kontinuierliche Verbesserungen sicherstellen, dass ihr ISMS stets aktuell bleibt. [32]

Die EN ISO/IEC 27001 verlangt, dass Informationen durch geeignete Sicherheitsmaßnahmen geschützt werden. Dies ist besonders wichtig, um den Schutz der Privatsphäre der Patienten zu gewährleisten und gesetzliche Anforderungen, wie die Datenschutz-Grundverordnung (DSGVO) [80] in der EU, zu erfüllen. Die Norm stellt sicher, dass die Integrität der Daten durch verschiedene Kontrollen gewährleistet wird, wie z.B. durch Zugriffsmanagement und kryptografische Techniken. Der Zugang zu Medizingeräten und den darin enthaltenen Daten sollte streng kontrolliert werden, um sicherzustellen, dass nur autorisiertes Personal auf sensible Daten zugreifen kann. Dies reduziert das Risiko eines unbefugten Zugriffs, der zu Datenschutzverletzungen oder Datenmanipulation führen könnte (siehe Kapitel 9.1). Die EN ISO/IEC 27001 legt Wert auf die Verfügbarkeit von Informationen und Diensten, um sicherzustellen, dass Medizingeräte auch im Falle eines Sicherheitsvorfalls weiterhin funktionieren können. Da Medizingeräte oft in kritischen medizinischen Umgebungen eingesetzt werden, ist es unerlässlich, dass es Pläne für Notfälle und die Wiederherstellung gibt. Dies stellt sicher, dass Geräte auch im Falle eines Sicherheitsvorfalls oder Systemausfalls schnell wieder in Betrieb genommen werden

können (siehe Kapitel 8.2, 8.3). Die Norm fordert ein umfassendes Risikomanagement, das für Medizingeräte besonders wichtig ist. Es ermöglicht die Identifizierung und Bewertung von Risiken, die durch Cyberangriffe entstehen könnten, und die Implementierung geeigneter Maßnahmen, um diese Risiken zu minimieren (siehe Kapitel 6.1). Das Bewusstsein für Cybersecurity-Bedrohungen und die richtige Kommunikation sind entscheidend, um Sicherheitsvorfälle zu verhindern und korrekt darauf zu reagieren. Mitarbeiter müssen wissen, wie sie Bedrohungen erkennen und melden können. Die EN ISO/IEC 27001 fordert daher die Durchführung von regelmäßigen Schulungen und Sensibilisierungsprogrammen für alle Personen, die mit Medizingeräten arbeiten (siehe Kapitel 7.3, 7.4).

Die EN ISO/IEC 27001 bietet einen umfassenden Rahmen für das Management von Informationssicherheitsrisiken, die für die MDR-Konformität relevant sein könnten. Die NIS2-Richtlinie [70] fordert von kritischen Infrastrukturen strenge Cybersicherheitsmaßnahmen, die durch die EN ISO/IEC 27001 systematisch und prozessorientiert umgesetzt werden können. Die EN ISO/IEC 27001 ergänzt die EN 62304 [21], die den Lebenszyklus von Software für Medizinprodukte definiert, durch Anforderungen an die Informationssicherheit, insbesondere beim Design und der Entwicklung von Software. Die Norm bietet ebenfalls eine umfassende Struktur zur Integration von Informationssicherheitsrisiken in das allgemeine Risikomanagement gemäß der EN ISO 14971 [30].

EN ISO/IEC 27002 - Information security, cybersecurity and privacy protection—Informationsecuritycontrols

Die EN ISO/IEC 27002 bietet Organisationen eine umfassende Anleitung zur Umsetzung von Informationssicherheitsmaßnahmen als Teil eines ISMS nach EN ISO/IEC 27001 [32]. Die Norm umfasst organisatorische, personelle, physische und technologische Sicherheitskontrollen, um den Schutz von Informationen zu gewährleisten. Sie betont, dass Informationssicherheit mehr als technische Maßnahmen umfasst und ein systematisches Management erfordert, das regelmäßig überprüft und an neue Risiken angepasst wird. Die Norm unterstützt Organisationen dabei, Sicherheitskontrollen an unterschiedliche Kontexte und den gesamten Lebenszyklus von Informationen anzupassen. [33]

Das Zugriffsmanagement (siehe 5.15) spielt eine zentrale Rolle bei der Sicherheit von Medizingeräten. Daher ist es essenziell, strenge Zugriffsrichtlinien zu implementieren, die gewährleisten, dass nur autorisierte Personen auf die Geräte zugreifen können. Mithilfe der Entwicklung eines Incident-Management-Plans laut 5.24, der spezifische Schritte zur Erkennung, Reaktion und Wiederherstellung nach einem Cyberangriff auf Medizingeräte beschreibt, kann der Hersteller schneller und effektiver reagieren. Dieser Punkt kann entscheidend sein um Schäden zu minimieren und vor allem die Verfügbarkeit der Medizingeräte sicherzustellen. Die EN ISO/IEC 27002 fordert ebenfalls Sicherheitsanforderungen für Netzwerke (siehe 8.20). Der Hersteller soll Netzwerksicherheitsmaßnahmen, wie Firewalls, Verschlüsselung und regelmäßigen Sicherheitsüberprüfungen implementieren dass die Kommunikation zwischen den Medizingeräten sicher bleibt. Das Management von Sicherheitslücken ist von entscheidender Bedeutung, da Schwachstellen in Medizingeräten von Angreifern ausgenutzt werden könnten, um das System zu kompromittieren. Um

dieses Risiko zu minimieren, fordert die EN ISO/IEC 27002 regelmäßige Sicherheitsüberprüfungen und Updates, die darauf abzielen, bekannte Schwachstellen zu beheben und so die Sicherheit der Medizingeräte kontinuierlich zu gewährleisten (siehe 8.8). Damit die personenbezogen Daten, die das Medizingerät verarbeitet, vor unbefugtem Zugriff geschützt ist, fordert die EN ISO/IEC 27002 die Implementierung von Datenschutzmaßnahmen (siehe 5.34). Softwarefehler in Medizingeräten können schwerwiegende Sicherheitslücken verursachen. Aus diesem Grund ist die Anforderung 8.25 Secure development life cycle für Medizingeräte wichtig umzusetzen. Um dies zu erreichen empfiehlt die EN ISO/IEC 27002 die Trennung von Entwicklungs-, Test- und Produktionsumgebungen, um eine klare Abgrenzung der jeweiligen Prozesse zu gewährleisten. Weiterhin sollten Leitlinien für die Sicherheit im gesamten Lebenszyklus der Softwareentwicklung eingeführt werden, einschließlich der Integration von Sicherheitsaspekten in die Softwareentwicklungsmethodik und der Verwendung sicherer Kodierungsrichtlinien für jede eingesetzte Programmiersprache. In der Spezifikations- und Entwurfsphase sollten Sicherheitsanforderungen definiert und Sicherheitskontrollpunkte in den Projekten etabliert werden. Zudem sind umfassende System- und Sicherheitstests, wie Regressionstests, Code-Scans und Penetrationstests, unerlässlich. Der Quellcode und die Konfigurationen sollten in sicheren Repositories aufbewahrt und die Sicherheit in der Versionskontrolle sichergestellt werden. Entwickler sollten über das notwendige Wissen zur Anwendungssicherheit verfügen und regelmäßig geschult werden.

NIST 800-53 [65] bietet einen Rahmen für die Auswahl und Implementierung von Sicherheits- und Datenschutzkontrollen. EN ISO/IEC 27002 bietet ergänzende und detailliertere Sicherheitskontrollen, die auf die spezifischen Bedürfnisse von Medizingeräten zugeschnitten werden können. Die Kombination von beiden ermöglicht es dem Hersteller, robuste Sicherheitspraktiken zu implementieren. Die EN ISO/IEC 27002 ergänzt die EN 62304 [21] durch die Bereitstellung von Sicherheitskontrollen, die in den Entwicklungsprozess integriert werden sollten, um sicherzustellen, dass die Software sicher und frei von bekannten Schwachstellen ist. Weiteres kann die EN ISO/IEC 27002 die EN ISO 14971 [30] durch spezifische Kontrollen, um Risiken im Zusammenhang mit Informationssicherheit und Cyberangriffen zu behandeln, ergänzen. Hersteller sollten die Risikomanagementprozesse gemäß EN ISO 14971 [30] um die spezifischen Sicherheitskontrollen der EN ISO/IEC 27002 erweitern, um ein umfassendes Sicherheitsprofil für Medizingeräte zu gewährleisten. ISO 27799 [45] spezifiziert die Anwendung von EN ISO/IEC 27002 im Gesundheitswesen und konzentriert sich speziell auf den Schutz von personenbezogenen Gesundheitsinformationen (PHI). Hersteller sollten die Sicherheitskontrollen der EN ISO/IEC 27002 in Verbindung mit den spezifischen Anforderungen der ISO 27799 [45] umsetzen, um eine umfassende Sicherheitsstrategie zu entwickeln, die sowohl allgemeine als auch branchenspezifische Bedrohungen adressiert. Allerdings basiert die aktuelle ISO 27799 [45] noch auf der älteren Version EN ISO/IEC 27002. Durch die Umstrukturierung der Kapitel in der aktuellsten Version der EN ISO/IEC 27002 ist die Zuweisung der Anforderung schwierig. Abhilfe gibt es im Zuge einer Korrespondenz Tabelle im Anhang B.

ISO 27799 - Health informatics — Information security management in health using ISO/IEC 27002

Die ISO 27799 bietet Gesundheitsorganisationen Leitlinien zur Informationssicherheit, angepasst an die Anforderungen im Gesundheitswesen, und unterstützt die Umsetzung von EN ISO/IEC 27002 [33] für den Schutz persönlicher Gesundheitsdaten. Die Norm fordert die Einführung einer regelmäßig überprüften Informationssicherheitspolitik und eine klare Organisation der Sicherheitsverantwortlichkeiten, einschließlich eines Informationssicherheitsmanagementforums (ISMF) und der Trennung von Aufgaben zur Minimierung von Missbrauchsrisiken. Sie verlangt spezifische Sicherheitsmaßnahmen für mobile Geräte, geregelten Zugriff auf Gesundheitsinformationen und den Einsatz kryptographischer Kontrollen. Zudem müssen physische und technische Schutzmaßnahmen wie Malware-Prävention sowie Prozesse zur Informationssicherheitskontinuität und Vorfallbewältigung etabliert werden, um Datenverfügbarkeit in Krisensituationen sicherzustellen. [45]

Die Norm fordert, dass jede Organisation, die mit Gesundheitsinformationen arbeitet, eine formalisierte Informationssicherheitsrichtlinie entwickelt, die spezifisch auf die Bedürfnisse des Gesundheitswesens zugeschnitten ist. Diese Richtlinie muss sowohl die rechtlichen als auch die ethischen Verpflichtungen des Schutzes persönlicher Gesundheitsdaten umfassen (siehe Kapitel 5). Für Medizingeräte bedeutet dies, dass klare Richtlinien vorhanden sein müssen, die den sicheren Umgang mit sensiblen Gesundheitsdaten regeln, insbesondere in Hinblick auf die Übertragung und Speicherung dieser Daten durch die Geräte. Ohne solche Richtlinien besteht ein erhöhtes Risiko, dass Sicherheitslücken nicht erkannt oder nicht effektiv geschlossen werden. Die ISO 27799 legt großen Wert auf die Kontrolle des Zugriffs auf Gesundheitsinformationen. Es wird gefordert, dass der Zugriff streng reguliert wird, basierend auf den definierten Rollen und Verantwortlichkeiten der Benutzer (siehe Kapitel 9). Für Medizingeräte ist es unerlässlich, dass der Zugriff auf gespeicherte oder verarbeitete Gesundheitsdaten nur autorisierten Personen oder Systemen gewährt wird. Dies minimiert das Risiko, dass unbefugte Personen Zugriff auf sensible Informationen erhalten oder die Funktionalität des Geräts kompromittieren. Die Norm betont die Notwendigkeit, kryptographische Maßnahmen zu implementieren, um die Vertraulichkeit und Integrität von Gesundheitsdaten zu gewährleisten. Dies betrifft sowohl die Datenübertragung als auch die Datenspeicherung (siehe Kapitel 10). Medizingeräte, die Daten über Netzwerke übertragen oder diese speichern, müssen sicherstellen, dass die Daten verschlüsselt werden, um sie vor Abhör- und Manipulationsversuchen zu schützen. Verschlüsselung ist ein wesentliches Mittel, um den Datenschutz zu gewährleisten und die Integrität der Daten zu sichern. ISO 27799 verlangt, dass alle Aktivitäten, die mit der Verarbeitung von Gesundheitsdaten zusammenhängen, überwacht und protokolliert werden. Dazu gehört auch die regelmäßige Überprüfung dieser Protokolle, um Sicherheitsvorfälle zu erkennen und entsprechend zu reagieren (siehe Kapitel 12). Für Medizingeräte ist es wichtig, dass sie in der Lage sind, alle sicherheitsrelevanten Aktionen zu protokollieren. Dies ermöglicht es, im Falle eines Sicherheitsvorfalls nachzuvollziehen, wer wann und wie auf die Daten zugegriffen hat. Diese Transparenz ist entscheidend, um auf Vorfälle schnell reagieren und Maßnahmen ergreifen zu können. Die Norm fordert, dass Organisationen klare Prozesse für das Management von Sicherheitsvorfällen etablieren, einschließlich der Sammlung von

Beweismaterialien und der Bewertung der Auswirkungen auf die Informationssicherheit (siehe Kapitel 16). Für Medizingeräte ist es entscheidend, dass im Falle eines Cyberangriffs oder einer anderen Sicherheitsverletzung schnell und effizient gehandelt werden kann. Ein gut definiertes Vorfallmanagement stellt sicher, dass Risiken minimiert und Schäden begrenzt werden.

Die MDR [81] fordert von Medizinproduktehestellern umfassende Maßnahmen zur Risikominimierung, einschließlich Informationssicherheit, während die ISO 27799 spezifische Leitlinien bietet, die helfen, diese Anforderungen zu erfüllen und die Cybersicherheit der Produkte zu gewährleisten. Die NIS2-Richtlinie [70] und die Datenschutz-Grundverordnung (DSGVO) [80] stellen rechtliche Rahmenbedingungen für die Cybersicherheit und den Datenschutz dar. ISO 27799 bietet praktische Leitlinien, wie diese gesetzlichen Anforderungen im Kontext der Gesundheitsinformatik umgesetzt werden können. Die ISO 27799 und die EN ISO/IEC 27002 [33] sind eng miteinander verbunden, da die ISO 27799 speziell für das Gesundheitswesen entwickelt wurde und auf den allgemeinen Prinzipien der EN ISO/IEC 27002 [33] aufbaut. Während die EN ISO/IEC 27002 [33] allgemeine Leitlinien für Informationssicherheits-Managementsysteme (ISMS) bietet, passt die ISO 27799 diese Leitlinien an die speziellen Anforderungen des Gesundheitswesens an, insbesondere im Umgang mit sensiblen Gesundheitsdaten. Die EN IEC 81001-5-1 [28] fokussiert auf die Cybersicherheit in der Softwareentwicklung für Medizingeräte, während die ISO 27799 spezifische Anforderungen zum Schutz von Gesundheitsinformationen bereitstellt.

ISO/IEC 27032 - Cybersecurity — Guidelines for Internet security

Die ISO/IEC 27032 ist eine internationale Norm, die sich auf die Cybersicherheit konzentriert und spezifische Leitlinien für die Internetsicherheit bereitstellt. Sie erklärt die Beziehung zwischen Internetsicherheit, Websicherheit, Netzwerksicherheit und Cybersicherheit und bietet Organisationen, die das Internet nutzen, umfassende Informationen über relevante Sicherheitsaspekte. Dabei werden die verschiedenen Zusammenhänge zwischen diesen Sicherheitsbereichen beleuchtet und beschrieben, wie sie zusammenwirken, um eine umfassende Sicherheit zu gewährleisten. Ein zentrales Thema der Norm ist die Bewertung und Behandlung von Risiken, die durch die Nutzung des Internets entstehen. Es werden spezifische Bedrohungen wie Malware, Phishing und Identitätsdiebstahl detailliert beschrieben, und es wird erläutert, wie Organisationen diese Bedrohungen sowie Schwachstellen und Angriffsvektoren bewerten und entsprechend darauf reagieren können. Die Norm hebt die Bedeutung von Sicherheitsrichtlinien und Maßnahmen hervor, wie etwa die Implementierung von Informationssicherheitsmanagementsystemen (ISMS), Zugangskontrollen, die Sensibilisierung von Mitarbeitern und das Management von Sicherheitsvorfällen. Zudem identifiziert die Norm verschiedene Interessengruppen wie Nutzer, Regierungsbehörden, Internetdienstanbieter und Standardisierungsorganisationen und beschreibt deren Rollen in der Gewährleistung der Internetsicherheit. [49]

Ein zentraler Aspekt ist der Schutz der Patientendaten, der durch die Implementierung von Zugangskontrollen und Verschlüsselungstechnologien, wie VPN und HTTPS, gewährleistet wird (Kapitel 9.2.3). Diese Maßnahmen sind entscheidend, um die Vertraulichkeit

und Integrität sensibler Daten sicherzustellen. Darüber hinaus sollten Medizingerätehersteller regelmäßige Sicherheitsupdates bereitstellen, um bekannte Sicherheitslücken zu schließen und die Geräte gegen neu auftretende Bedrohungen abzusichern. Ebenso wichtig ist die Schulung des medizinischen Personals. Durch gezielte Schulungs- und Sensibilisierungsprogramme wird sichergestellt, dass die Mitarbeiter sich der potenziellen Bedrohungen bewusst sind und wissen, wie sie sich und die Geräte effektiv schützen können (Kapitel 9.2.4). Ein effektives Vorfallmanagement ist ebenfalls unerlässlich, um schnell auf Sicherheitsvorfälle reagieren zu können, die die Funktionsfähigkeit der Medizingeräte beeinträchtigen könnten (Kapitel 9.2.10). Zudem ist eine enge Zusammenarbeit mit Lieferanten, insbesondere Cloud-Dienstleistern und Softwareanbietern, erforderlich, um sicherzustellen, dass alle Sicherheitsanforderungen konsequent erfüllt werden.

Die ISO/IEC 27032 kann Unternehmen dabei unterstützen, die Anforderungen der NIS2-Richtlinie [70] zu erfüllen, indem sie spezifische Cybersicherheitsmaßnahmen und Schutzmechanismen gegen Internetbedrohungen bereitstellt. Durch die Bereitstellung technischer und organisatorischer Maßnahmen trägt die ISO/IEC 27032 dazu bei, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten im Internet zu sichern und somit die Einhaltung der DSGVO [80] zu fördern. Die Norm kann auch als Ergänzung zur EN ISO 14971 [30] herangezogen werden, um gezielt Risiken zu adressieren, die durch Cyberbedrohungen für medizinische Geräte entstehen. Die ISO/IEC 27032 ergänzt die EN ISO/IEC 27001 [32] und EN ISO/IEC 27002 [33], indem sie spezifische Leitlinien für die Sicherheit im Internet und den Schutz vor Cyberbedrohungen bietet. Während die EN ISO/IEC 27001 [32] und EN ISO/IEC 27002 [33] allgemeine Anforderungen und Kontrollen für Informationssicherheits-Managementsysteme (ISMS) festlegen, konzentriert sich die ISO/IEC 27032 auf Bedrohungen, die speziell aus der Nutzung des Internets resultieren. ISO/IEC 27032 kann ergänzend zur ISO 27799 [45] eingesetzt werden, um spezifische Internetbedrohungen in diesem Bereich zu adressieren.

EN 62443-2-1 - Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program

Die Norm EN 62443-2-1 beschreibt die wesentlichen Anforderungen für die Einrichtung eines Cybersicherheitsmanagementsystems (CSMS) für industrielle Automatisierungs- und Steuerungssysteme (IACS). Sie dient als Leitfaden für die Entwicklung, Implementierung und kontinuierliche Verbesserung eines solchen Sicherheitsprogramms, das sowohl in großen als auch kleinen Unternehmen angewendet werden kann. Die Norm legt fest, welche Elemente ein CSMS enthalten sollte, um IACS wirksam vor Cyberangriffen zu schützen. Dazu gehört eine gründliche Risikobewertung, die die spezifischen Bedürfnisse einer Organisation im Umgang mit Cyberrisiken dokumentiert und potenzielle Bedrohungen, Schwachstellen und deren Auswirkungen identifiziert und bewertet. Ein weiterer Schwerpunkt der Norm liegt auf der Adressierung dieser Risiken durch die Entwicklung von Sicherheitsrichtlinien und das Bewusstsein innerhalb der Organisation. Dies umfasst Schulungen für das Personal, die Festlegung von Verantwortlichkeiten und die Implementierung ausgewählter Sicherheitsmaßnahmen, wie Personal-, physische und

netzwerkbezogene Schutzmaßnahmen. Darüber hinaus wird die Bedeutung einer strukturierten Umsetzung und Dokumentation von Sicherheitsmaßnahmen hervorgehoben, einschließlich Risikomanagement, Systementwicklung und Planung für den Umgang mit Sicherheitsvorfällen. Schließlich betont die Norm die Notwendigkeit, das CSMS kontinuierlich zu überwachen und zu verbessern. Dies schließt die Sicherstellung der Konformität mit den festgelegten Richtlinien und die regelmäßige Überprüfung und Anpassung des CSMS ein, um es an sich ändernde Bedrohungen und Anforderungen anzupassen. Insgesamt bietet die Norm einen umfassenden Rahmen für den Schutz industrieller Systeme vor Cyberbedrohungen und betont die Wichtigkeit einer dynamischen und anpassungsfähigen Sicherheitsstrategie. [22]

Auch wenn die Norm nicht für Medizingeräte angedacht ist, bietet sie eine umfassende Grundlage für die Einrichtung eines CSMS, das auch auf Medizingeräte anwendbar ist. Die Implementierung eines CSMS kann dazu beitragen, die Sicherheitsrisiken zu minimieren, indem es systematische Ansätze zur Identifikation und Bewertung von Risiken sowie zur Implementierung von Schutzmaßnahmen bietet. Insbesondere die Anforderungen an Netzwerksicherheit, Zugriffskontrollen und Vorfallmanagement sind entscheidend, um sicherzustellen, dass Medizingeräte vor unbefugtem Zugriff und Cyberangriffen geschützt sind. Vom Vorgehen der Risikoidentifikation, -klassifizierung und -bewertung ähnelt das Vorgehen an die EN ISO 14971 [30], jedoch betrachtet die EN 62443-2-1 zusätzlich den Punkt geschäftliche Begründung (Business Rationale). Diese Begründung basiert auf den möglichen finanziellen, sicherheitsbezogenen, umweltbezogenen und anderen Konsequenzen, die sich aus einem Cybervorfall ergeben könnten. Das Ziel ist es, das Management der Organisation dazu zu bringen, die Notwendigkeit und den Nutzen von Investitionen in die Cybersicherheit zu verstehen und zu unterstützen. Dieser Punkt kann ebenfalls bei Medizingeräten von Vorteil sein.

Vergleich der Normen EN 62443-2-1 (2009) und EN IEC 62443-2-1 (2019 Entwurf)

Die grundlegende Struktur und Zielsetzung der Normen von 2009 und 2019 bleiben ähnlich, jedoch gibt es mehrere wichtige Änderungen und Erweiterungen in der Version von 2019 [24]:

1. Formalisierung der Konformitätsbewertung: Die neue Version enthält detaillierte Anforderungen und Verfahren für Konformitätsbewertungen, einschließlich der Rolle unabhängiger Drittparteien.
2. Erweiterte Anforderungen an die Organisation: Die 2019er-Version legt mehr Fokus auf die organisatorische Vorbereitung und definiert detailliertere Anforderungen für Sicherheitsrollen, Verantwortlichkeiten und Schulungen.
3. Zusätzliche Sicherheitsmaßnahmen: Neue Maßnahmen wurden hinzugefügt, insbesondere in Bezug auf die Sicherheit von drahtlosen Netzwerken und Fernzugriffen.
4. Erweiterte Netzwerk- und Kommunikationssicherheit: Es gibt spezifischere Anforderungen an die Segmentierung und den Schutz von Netzwerken sowie an die Verwaltung von Netzwerkzugriffen und -diensten.

5. Komponentensicherheit und Patch-Management: Die neue Version enthält ausführlichere Anforderungen zur Härtung von Geräten, zum Schutz vor Malware und zum Management von Sicherheitspatches.

6. Datenschutz und Benutzerzugriffskontrolle: Es wurden zusätzliche Anforderungen für den Schutz von Daten, die Verwaltung kryptographischer Schlüssel und die Kontrolle von Benutzerzugriffen aufgenommen.

EN IEC 62443-4-1 - IT-Sicherheit für industrielle Automatisierungssysteme Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung

Die Norm EN IEC 62443-4-1 legt die Anforderungen an einen sicheren Entwicklungsprozess für Produkte fest, die in industriellen Automatisierungssystemen eingesetzt werden. Dabei steht der gesamte Entwicklungslebenszyklus (Secure Development Lifecycle, SDL) im Fokus, der verschiedene Phasen umfasst: die Definition von IT-Sicherheitsanforderungen, den sicheren Entwurf und die sichere Implementierung von Produkten, die regelmäßige Verifikation und Validierung der Sicherheitsaspekte sowie die Behandlung von Sicherheitsmängeln und das Management von Sicherheitsupdates. Die Norm betont die Wichtigkeit eines durchgängig sicheren Entwicklungsprozesses, der sicherstellt, dass alle potenziellen Sicherheitsrisiken frühzeitig erkannt und behoben werden. Dieser Prozess endet nicht mit der Markteinführung des Produkts, sondern umfasst auch den gesamten Lebenszyklus, einschließlich des Patch-Managements und der sicheren Entsorgung des Produkts. Ziel der Norm ist es, die IT-Sicherheit während des gesamten Entwicklungsprozesses zu gewährleisten und Produkte so zu entwickeln, dass sie vor aktuellen und zukünftigen Bedrohungen geschützt sind. Die Anforderungen richten sich dabei an Produktentwickler und Instandhalter, nicht jedoch an Integratoren oder Endanwender. [25]

Die EN IEC 62443-4-1 Norm bietet eine umfassende Grundlage für die Entwicklung sicherer Produkte in der industriellen Automatisierung, die auch für Medizingeräte anwendbar ist. Die Norm deckt alle Phasen des Produktlebenszyklus ab und stellt sicher, dass Produkte von der Entwurfsphase bis zur Außerbetriebnahme sicher bleiben. Durch die Einbindung von Sicherheitsüberprüfungen, Patch-Management und kontinuierlicher Verbesserung bietet die Norm eine robuste Struktur zur Bekämpfung von Cyberbedrohungen.

EN IEC 62443-4-2 - IT-Sicherheit für industrielle Automatisierungssysteme Teil 4-2: Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme (IACS)

Die EN IEC 62443-4-2 definiert technische Sicherheitsanforderungen für Komponenten industrieller Automatisierungs- und Steuerungssysteme (IACS) auf verschiedenen Sicherheitsniveaus. Sie umfasst Maßnahmen zur Identifikation und Authentifizierung von Nutzern und Geräten, Zugangskontrollen, Schutz der Systemintegrität sowie Vertraulichkeit und sichere Datenlöschung. Zudem verlangt die Norm die Überwachung

sicherheitsrelevanter Ereignisse und schnelle Reaktionsmechanismen. Durch die Erfüllung dieser Anforderungen wird ein umfassender Schutz der Systemkomponenten gegen Bedrohungen sichergestellt. [26]

Eine besonders wichtige Anforderung ist die Identifizierung und Authentifikation (FR 1), da sie sicherstellt, dass nur autorisierte Personen und Prozesse Zugriff auf die Medizingeräte haben. Eine starke Authentifizierung, wie die Nutzung von Multi-Faktor-Authentifizierung und Zertifikaten, ist hier essenziell, um unbefugten Zugriff zu verhindern, der die Patientensicherheit gefährden könnte. Die Systemintegrität (FR 3) ist ebenfalls von großer Bedeutung, da sie Manipulationen oder Veränderungen an den Geräten verhindert, die durch Malware oder unautorisierte Eingriffe verursacht werden könnten. Dies ist entscheidend, um sicherzustellen, dass die Geräte wie vorgesehen funktionieren und keine Gefahr für die Patienten darstellen. Regelmäßige Integritätsprüfungen und Schutzmechanismen gegen Schadcode sind hierbei von zentraler Bedeutung. Ein weiterer kritischer Aspekt ist die Vertraulichkeit der Daten (FR 4). Medizingeräte verarbeiten häufig hochsensible personenbezogene Daten, deren Schutz vor unbefugtem Zugriff und Missbrauch oberste Priorität hat. Der Einsatz von Verschlüsselungstechniken sowohl für ruhende Daten als auch für die Datenübertragung ist notwendig, um die Vertraulichkeit zu gewährleisten. Die Verfügbarkeit der Ressourcen (FR 7) ist besonders in Notfallsituationen entscheidend, da die ständige Einsatzbereitschaft von Medizingeräten lebenswichtig sein kann. Cyberangriffe, die die Verfügbarkeit beeinträchtigen, könnten schwerwiegende Auswirkungen auf die Patientenversorgung haben. Maßnahmen zum Schutz vor Denial-of-Service-Angriffen und zur schnellen Wiederherstellung der Systeme nach einem Angriff sind daher unerlässlich. Die Fähigkeit zur rechtzeitigen Reaktion auf Ereignisse (FR 6) ist ebenfalls entscheidend, um sicherheitsrelevante Vorfälle frühzeitig zu erkennen und zu beheben. Echtzeit-Monitoring und Protokollierungsmechanismen sind wichtig, um alle sicherheitsrelevanten Ereignisse zu dokumentieren und entsprechende Gegenmaßnahmen einzuleiten. Für Medizingeräte sind alle genannten Anforderungen wichtig, jedoch müssen sie spezifisch angepasst werden, um den besonderen Anforderungen der Medizintechnik gerecht zu werden.

In Verknüpfung mit der EN ISO 14971 [30] kann mithilfe der EN IEC 62443-4-2 spezifische Risiken mit Cybersicherheit adressiert werden. Zusätzlich können die technischen Sicherheitsanforderungen aus der EN IEC 62443-4-2 als spezifische Risikokontrollmaßnahme innerhalb der Risikomanagementprozess implementiert werden. Die EN ISO 13485 [29] betont die Wichtigkeit von Designkontrollen, diese können durch die Sicherheitsanforderungen und -praktiken aus EN IEC 62443-4-2 erweitert werden. Beide Standards unterstreichen die Notwendigkeit eines effektiven Lieferantenmanagements. EN IEC 62443-4-2 fügt zusätzlich Anforderungen hinzu, um sicherzustellen, dass Komponenten und Software von Drittanbietern sicher und vertrauenswürdig sind.

ISO/IEC 15408-1 - Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model

Die Norm ISO/IEC 15408-1 legt die grundlegenden Konzepte und Prinzipien für die Bewertung von IT-Sicherheitsprodukten fest. Sie definiert ein allgemeines Bewertungsmo-

dell, das als Grundlage für die Beurteilung der Sicherheitseigenschaften von IT-Produkten dient. Dieses Dokument gibt einen umfassenden Überblick über alle Teile der ISO/IEC 15408-Reihe, erklärt wesentliche Begriffe und Abkürzungen und beschreibt das zentrale Konzept des Evaluierungsgegenstands (TOE - Target of Evaluation). Zudem werden der Evaluierungskontext und die Zielgruppen, an die sich die Evaluationskriterien richten, dargestellt. Ein zentraler Bestandteil der Norm ist der Evaluierungsgegenstand (TOE), der verschiedene Formen annehmen kann, wie zum Beispiel Software, Firmware, Hardware oder eine Kombination dieser Elemente. Der TOE kann auch ein Teil eines IT-Produkts oder eine spezielle Technologie sein, die möglicherweise nie zu einem vollständigen Produkt wird. Die Norm behandelt außerdem die wesentlichen Sicherheitskonzepte, einschließlich der Identifizierung von Vermögenswerten und Bedrohungen sowie der Entwicklung von Gegenmaßnahmen zur Risikominderung. Dabei wird sowohl die Angemessenheit als auch die Korrektheit dieser Gegenmaßnahmen analysiert, um sicherzustellen, dass die Sicherheitsziele erreicht werden. In der ISO/IEC 15408-1 werden zwei Hauptarten der Evaluierung beschrieben: die ST-/TOE-Evaluierung und die Evaluierung von Schutzprofilen (PP). Diese Evaluierungen helfen dabei, die Sicherheitseigenschaften eines TOE systematisch zu bewerten und festzustellen, ob sie den festgelegten Anforderungen entsprechen. Schutzprofile dienen dazu, allgemeine Anforderungen an einen bestimmten TOE-Typ zu beschreiben, während Pakete benannte Sätze von Sicherheitsanforderungen darstellen, die wiederverwendet werden können. Insgesamt bietet die Norm ISO/IEC 15408-1 einen strukturierten Rahmen für die Evaluierung von IT-Sicherheitsprodukten, indem sie einheitliche Kriterien und Methoden bereitstellt, die die systematische Bewertung der Sicherheitseigenschaften dieser Produkte ermöglichen. [47]

Insgesamt bietet die ISO/IEC 15408-1 Norm einen robusten Rahmen für die Evaluierung und Zertifizierung der Sicherheit von IT-Produkten, einschließlich Medizingeräten. Durch die Förderung einer strukturierten und konsistenten Methodik zur Sicherheitsbewertung trägt die Norm zur Verbesserung der Cybersicherheit und zur Schaffung sicherer IT-Umgebungen bei. Die NIS2-Richtlinie [70] zielt darauf ab, ein hohes Maß an Cybersicherheit in der EU zu gewährleisten. Die ISO/IEC 15408-1 kann herangezogen werden, um die Sicherheitsbewertungen von IT-Produkten, die in kritischen Infrastrukturen, einschließlich des Gesundheitswesens, eingesetzt werden, zu unterstützen. Dies trägt dazu bei, die Konformität mit den Anforderungen der NIS2-Richtlinie [70] sicherzustellen. Außerdem kann die Norm zur Bewertung der Sicherheitsfunktionen von IT-Komponenten in Medizinprodukten herangezogen werden, um sicherzustellen, dass diese Komponenten den Sicherheitsanforderungen entsprechen, die im Rahmen des Risikomanagements nach EN ISO 14971 [30] festgelegt wurden. Diese Verbindung ist besonders wichtig für Hersteller von Medizinprodukten, um die Konformität mit regulatorischen Anforderungen sicherzustellen. Zusätzlich kann sie genutzt werden, um die Sicherheit von Softwarekomponenten, die in Medizinprodukten verwendet werden, zu bewerten. Dies unterstützt die Einhaltung der EN 62304 [21], indem sichergestellt wird, dass die Software nicht nur funktional, sondern auch sicher ist. Die ISO/IEC 29147 [50] und die ISO/IEC 30111 [51] ergänzen die ISO/IEC 15408-1, indem sie sicherstellen, dass Schwachstellen, die während der Sicherheitsbewertung eines IT-Produkts identifiziert werden, effektiv gemeldet und

adressiert werden. Dies ist besonders wichtig, um die kontinuierliche Sicherheit und Integrität der bewerteten Produkte zu gewährleisten.

Vergleich der Normen ISO/IEC 15408-1 (2009) und ISO/IEC DIS 15408-1 (2023 Entwurf)

Der Entwurf der ISO/IEC DIS 15408-1 von 2023 behält die grundlegenden Konzepte der vorherigen Version bei, führt jedoch mehrere Erweiterungen und Klarstellungen ein [52].

Die Version von 2023 erweitert und verfeinert viele der in der 2009er Version enthaltenen Konzepte. Zu den wesentlichen Änderungen gehören:

1. 1. Erweiterte Definitionen und Konzepte: Die 2023er Version führt neue Begriffe und detailliertere Definitionen für bestehende Konzepte ein, um eine klarere und präzisere Evaluierung zu ermöglichen.
2. 2. Detailliertere Evaluierungsmethoden: Es gibt ausführlichere Leitlinien und Methoden zur Evaluierung von Schutzprofilen und Sicherheitsvorgaben, insbesondere für komplexe und zusammengesetzte Systeme.
3. 3. Erweiterte Evaluierungsprozesse: Die neue Version betont die Notwendigkeit von konsistenten und wiederholbaren Evaluierungsprozessen und bietet erweiterte Anleitungen für die Durchführung von Evaluierungen.
4. 4. Berücksichtigung neuer Technologien: Die 2023er Version berücksichtigt die Entwicklungen in der IT-Sicherheit und passt die Evaluierungsmethoden an moderne Technologien und Bedrohungsszenarien an.

Die Version von 2023 erweitert und verfeinert die Konzepte und Methoden der 2009er Version, um den aktuellen Anforderungen und Technologien besser gerecht zu werden.

ISO/IEC 15408-2 - Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components

Die ISO/IEC 15408-2 bietet einen Katalog von Sicherheitsfunktionen zur Bewertung der IT-Sicherheit von Produkten und stellt sicher, dass diese grundlegenden Sicherheitsanforderungen genügen und gegen Bedrohungen geschützt sind. Die Norm ist flexibel und kann auf verschiedene IT-Produkte und -Umgebungen angepasst werden, was eine maßgeschneiderte Sicherheitsbewertung ermöglicht. Ihr Ziel ist es, eine standardisierte Grundlage für die Bewertung von IT-Sicherheitsfunktionen zu schaffen und die Vergleichbarkeit zwischen verschiedenen Produkten zu erleichtern. [48]

Authentifizierung und Autorisierung (siehe Kapitel 11) sind von höchster Bedeutung, um sicherzustellen, dass nur befugtes Personal auf Medizingeräte und die damit verbundenen Patientendaten zugreifen kann. Die Implementierung strenger Authentifizierungsprotokolle reduziert das Risiko unbefugter Zugriffe, die zu Datenschutzverletzungen oder sogar zu Manipulationen der Geräte führen könnten. Die Verschlüsselung der Daten

(siehe Kapitel 9 und 10) ist entscheidend für den Schutz sensibler Gesundheitsdaten, sowohl bei der Übertragung als auch bei der Speicherung. Insbesondere bei vernetzten Medizingeräten ist die Verschlüsselung ein Muss, um sicherzustellen, dass Patientendaten vor Abhörversuchen und unbefugtem Zugriff geschützt sind. Eine kontinuierliche Sicherheitsüberwachung (siehe Kapitel 12) ermöglicht es, potenzielle Angriffe frühzeitig zu erkennen und abzuwehren. Für Medizingeräte, die in Echtzeit arbeiten, kann eine Verzögerung in der Erkennung und Reaktion auf Sicherheitsbedrohungen schwerwiegende Folgen haben, weshalb diese Maßnahme von besonderer Wichtigkeit ist. Außerdem gibt die ISO 15408-2 detaillierte Anforderungen für Sicherheitsaudit (siehe Kapitel 7), dass auch für Medizingeräte dazu beitragen kann dass Informationen zu sicherheitsrelevanten Aktivitäten erkannt, aufgezeichnet, gespeichert und analysiert werden.

Die MDR [81] und IVDR [82] fordern von Herstellern umfassende, dokumentierte Risikomanagementprozesse einschließlich Cybersicherheit, wobei die ISO/IEC 15408-2 einen Rahmen zur Implementierung und Bewertung der Sicherheitsfunktionen bietet, um die Sicherheit von Patientendaten und Geräteintegrität zu gewährleisten. Die ISO/IEC 15408-2 unterstützt die Einhaltung der NIS2-Richtlinie [70], indem sie spezifische Evaluationskriterien festlegt, mit denen die festgelegten Anforderungen geprüft werden können. Die EN IEC 81001-5-1 [28] wird durch die ISO/IEC 15408-2 ergänzt, da sie konkrete Sicherheitsfunktionskomponenten definiert, die implementiert werden müssen, um die in der EN IEC 81001-5-1 [28] festgelegten Sicherheitsziele zu erreichen.

ISO/IEC 29147 - Information technology — Security techniques — Vulnerability disclosure

Die ISO/IEC 29147 Norm behandelt die Offenlegung von Schwachstellen in Produkten und Dienstleistungen durch Anbieter und enthält Anforderungen sowie Empfehlungen, die es ermöglichen, technische Schwachstellen systematisch zu identifizieren, zu handhaben und offenzulegen. Ziel der Norm ist es, das Risiko der Ausnutzung von Schwachstellen zu mindern und dadurch Systeme und Daten zu schützen. Die Norm legt Leitlinien für das Empfangen und Offenlegen von Schwachstellenberichten fest. Anbieter sollen Prozesse und Kommunikationskanäle etablieren, um Berichte über potenzielle Schwachstellen von Anwendern, Forschern und anderen Interessengruppen zu empfangen. Ein strukturierter Prozess zur Bestätigung des Empfangs und zur Priorisierung der Berichte basierend auf der Schwere der Schwachstelle ist ebenfalls erforderlich. Die Norm betont die transparente Kommunikation über die Existenz von Schwachstellen und die Schritte zu deren Behebung sowie die Bereitstellung von Informationen zur Risikominderung bis zur endgültigen Behebung der Schwachstellen. Besonders wichtig ist die Koordination zwischen verschiedenen betroffenen Parteien, insbesondere wenn mehrere Anbieter involviert sind. Weiterhin definiert die Norm zentrale Begriffe und Konzepte, darunter Schwachstellen und deren potenzielle Auswirkungen auf die Vertraulichkeit, Integrität und Verfügbarkeit von Systemen. Es werden Techniken zur Identifikation und Behebung von Schwachstellen sowie die Interaktionen zwischen Komponenten und Systemen, die zu Schwachstellen führen können, beschrieben. Die Norm enthält Empfehlungen zur Implementierung von Sicherheitsmaßnahmen und Patches sowie zum Umgang mit Sicherheitslücken, die durch

Design-Entscheidungen, Implementierungsfehler oder Konfigurationsschwächen entstehen. [50]

Die Implementierung eines strukturierten Schwachstellenmanagementprozesses gemäß der Norm kann dazu beitragen, die Sicherheit dieser Geräte zu erhöhen. Für Medizingeräte bedeutet dies:

- Erhöhung der Patientensicherheit: Durch die systematische Identifikation und Behebung von Schwachstellen können potenzielle Sicherheitsrisiken, die die Patientensicherheit gefährden, minimiert werden.
- Schutz sensibler Gesundheitsdaten: Durch die Offenlegung von Schwachstellen und die Implementierung entsprechender Sicherheitsmaßnahmen wird die Integrität und Vertraulichkeit sensibler Gesundheitsdaten geschützt.

ISO/IEC 29147 bezieht sich auf EN ISO/IEC 27002 [33], speziell auf Abschnitt 12.6.1, der sich mit der Verwaltung technischer Schwachstellen beschäftigt. Die EN ISO/IEC 27002 [33] bietet allgemeine Richtlinien für Informationssicherheitsmanagement, während ISO/IEC 29147 spezifische Leitlinien für die Offenlegung von Schwachstellen in Produkten und Dienstleistungen liefert. Die ISO/IEC 29147 unterstützt den Risikomanagementprozess gemäß der EN ISO 14971 [30], indem sie sicherstellt, dass erkannte Schwachstellen ordnungsgemäß offengelegt werden, um Risiken zu minimieren.

ISO/IEC 30111 - Information technology — Security techniques — Vulnerability handling processes

Die Norm ISO/IEC 30111 befasst sich mit den Prozessen zur Handhabung von Schwachstellen in Produkten und Dienstleistungen. Sie legt Anforderungen und Empfehlungen fest, wie Lieferanten gemeldete potenzielle Schwachstellen bearbeiten und beheben sollten. Der Prozess beginnt mit dem Eingang einer Schwachstellenmeldung, die intern, extern oder öffentlich identifiziert worden sein kann. Danach erfolgt die Verifizierung der Schwachstelle, bei der eine Erstuntersuchung durchgeführt und mögliche Gründe für einen Prozessabbruch, wie etwa Duplikate oder obsolet gewordene Produkte, berücksichtigt werden. Im nächsten Schritt entwickelt der Lieferant Abhilfemaßnahmen, entscheidet über die geeigneten Maßnahmen zur Behebung der Schwachstelle, erstellt Patches oder Updates und testet diese. Nach der Veröffentlichung der Abhilfemaßnahmen erfolgen weitere Wartungen, Rückmeldungen zum Entwicklungszyklus und eine Überwachung der Produktstabilität, um die langfristige Sicherheit zu gewährleisten. Diese Norm sollte in Verbindung mit der ISO/IEC 29147 [50] angewendet werden, die Richtlinien zur Offenlegung von Schwachstellen bietet. [51]

Die ISO/IEC 30111 ist eine zusätzliche Hilfestellung um die IEC 29147 [50] umzusetzen. Vor allem das Kapitel 7 „Prozess für die Behandlung von Schwachstellen"gibt eine Richtung vor welche Schritte man in so einem Prozess befolgen sollte. Medizingeräte-Hersteller können diese Vorgabe des Prozesses umsetzten, um eine effektivere Behandlung von Schwachstellen zu gewährleisten. Durch die Förderung von Transparenz, Zusammenarbeit und proaktiven Sicherheitsmaßnahmen wird eine robustere und sicherere IT-Umgebung

geschaffen. Die Anforderungen der ISO/IEC 30111 zur Schwachstellenbehandlung lassen sich ebenfalls in ein ISMS laut EN ISO/IEC 27001 [32] und EN ISO/IEC 27002 [33] integrieren.

3.3.5 Relevanten Guidance-Dokumente zur Cybersicherheit für Medizingeräte

Die Entwicklung und der sichere Betrieb von vernetzten medizinischen Geräten erfordern die Einhaltung einer Vielzahl von Richtlinien und Empfehlungen, die auf internationaler Ebene von verschiedenen Organisationen entwickelt wurden. Im Folgenden werden die wichtigsten relevanten Dokumente zusammengefasst:

BSI-CS-132 - Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte

Die BSI-CS 132 Guideline bietet umfassende Empfehlungen für Hersteller von netzwerkfähigen Medizinprodukten, um sicherzustellen, dass diese Geräte sicher und zuverlässig betrieben werden können. Die Guideline unterscheidet zwischen drei Betriebsarten: dem medizinischen Betrieb nach Zweckbestimmung, der Konfiguration des Produktes und dem technischen Servicebetrieb. Alle Sicherheitsmaßnahmen sollten über diese verschiedenen Betriebsarten hinweg konsistent sein. Eine zentrale Empfehlung ist die Etablierung eines sicheren Entwicklungszyklus, der die Auswahl und Einrichtung vertrauenswürdiger Werkzeuge, die Trennung von Software-Einheiten sowie den Einsatz sicherer Programmiertechniken umfasst. Es wird betont, dass regelmäßige Cyber-Sicherheitsanalysen durchgeführt werden sollten, um Bedrohungen und Risiken zu identifizieren und entsprechende Gegenmaßnahmen zu implementieren. Im Entwicklungsprozess sollten zudem regelmäßige Reviews und ganzheitliche Sicherheitsbetrachtungen (Security Gates) stattfinden. Automatisierte Codeanalysen und gezielte Suche nach bekannten Schwachstellen, wie beispielsweise Buffer Overflows, sind ebenfalls wesentliche Bestandteile dieses Prozesses. Die Guideline legt großen Wert auf die Durchführung von Penetrationstests und technischen Sicherheitsanalysen, um sowohl bekannte als auch unbekannte Schwachstellen frühzeitig zu identifizieren. Vor der Auslieferung der Produkte sollte sichergestellt werden, dass kein Test-Code oder undokumentierte Zugänge enthalten sind. Ein weiterer wichtiger Aspekt ist der Umgang mit Schwachstellen in Betriebssystemen, Drittkomponenten und Eigenentwicklungen. Hierzu gehört die Bewertung und Behebung von Schwachstellen sowie die Implementierung integrierter Cyber-Sicherheitsmechanismen wie Application Whitelisting und Antivirenlösungen. Ein proaktiver Ansatz zur Schwachstellenbewältigung, einschließlich der Definition von Reaktionszeiten und Notfallprozeduren, ist ebenfalls unerlässlich. Die Guideline betont die Wichtigkeit der regelmäßigen und zeitnahen Versorgung der Produkte mit Patches und Updates, um entdeckte Schwachstellen zu beheben oder abzuschwächen. Der Update-Prozess sollte für Kunden einfach und effizient gestaltet sein, und die Auslieferungskette für Updates und Patches muss gesichert werden, um die Authentizität und Integrität sicherzustellen. Abschließend wird hervorgehoben, dass alle Schnittstellen dokumentiert und der maximale mögliche Schaden durch Angriffe bestimmt werden sollten. Hersteller müssen die Auswirkungen von Schwachstellen und

korrektiven Maßnahmen angemessen kommunizieren und sicherstellen, dass Medizingeräte den notwendigen Sicherheitsanforderungen entsprechen, um einen sicheren Betrieb zu gewährleisten. [8]

Die Empfehlung betont die Bedeutung eines sicheren Softwareentwicklungszyklus (Secure Software Development Lifecycle) und fordert Maßnahmen zur Systemhärtung, Codeanalyse und Penetrationstests, um Schwachstellen frühzeitig zu erkennen und zu beheben. Das Einbeziehen aktueller Sicherheitstechniken und das Festlegen klarer Vorgaben zur Softwareentwicklung verbessern die Gesamtsicherheit erheblich. Die Leitlinie fordert von Herstellern die Implementierung von Mechanismen gegen Schadsoftware und Denial-of-Service-Angriffe sowie von Protokollen zur Angriffserkennung. Zudem werden Anforderungen zur Sicherheit von Updates und Patches gestellt, wodurch die Integrität und Authentizität der Firmware-Updates gesichert wird. Die Empfehlung könnte von detaillierteren Vorgaben zur Bewertung und Priorisierung der identifizierten Sicherheitsrisiken profitieren, insbesondere in Hinblick auf unterschiedliche Gefährdungsstufen und Produktklassen. Dies würde die Anpassung der Maßnahmen an unterschiedliche Produkte vereinfachen. Angesichts der sich rasch entwickelnden Bedrohungen und Technologien wäre eine regelmäßige Aktualisierung des Dokuments wertvoll. Dies würde sicherstellen, dass neue Sicherheitsanforderungen und Techniken zeitnah integriert werden.

IEC TR 80001-2-2 - Application of risk management for IT- networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls

Die IEC TR 80001-2-2 Guideline bietet einen umfassenden Rahmen für die Offenlegung von sicherheitsrelevanten Fähigkeiten und Risiken, die für das Risikomanagement beim Anschluss medizinischer Geräte an IT-Netzwerke von entscheidender Bedeutung sind. Zentrale Empfehlungen umfassen dabei die Implementierung eines systematischen Risikomanagement-Prozesses, der die Identifikation, Analyse, Bewertung und Kontrolle von Risiken integriert, sowie die Festlegung klarer Verantwortlichkeiten und Zuständigkeiten innerhalb des Risikomanagement-Teams. Ein weiterer wesentlicher Punkt ist die Verwendung von Sicherheitsfähigkeiten (Security Capabilities), die spezifisch für medizinische Geräte und IT-Komponenten definiert werden, um die Anforderungen der Benutzer zu verstehen und passende Sicherheitskontrollen zu identifizieren. Diese Fähigkeiten umfassen unter anderem automatische Abmeldung, Audit-Kontrollen, Autorisierung und die Konfiguration von Sicherheitsfunktionen. Zusätzlich empfiehlt die Guideline die Implementierung technischer und organisatorischer Risikokontrollmaßnahmen. Dazu zählen Firewalls, Antivirus-Software sowie Verschlüsselungsmechanismen, wobei die Auswahl geeigneter Risikokontrolloptionen von der beabsichtigten Nutzung der medizinischen Geräte im IT-Netzwerk abhängt. Darüber hinaus ist die Überwachung und Überprüfung ein integraler Bestandteil. IT-Netzwerkumgebungen müssen kontinuierlich überwacht werden, um Sicherheitsvorfälle frühzeitig zu erkennen und angemessen darauf reagieren zu können. Regelmäßige Überprüfungen und Aktualisierungen der Risikomanagement-Strategien und -Maßnahmen sind ebenfalls erforderlich. Die Schulung und Sensibilisierung der Mitarbeiter sind ebenso entscheidend. Alle, die mit dem IT-Netzwerk und den angeschlossenen

medizinischen Geräten arbeiten, sollten regelmäßige Schulungen erhalten, um ein Sicherheitsbewusstsein innerhalb der Organisation zu fördern. Ein zentraler Bestandteil der IEC/TR 80001-2-2 sind spezifische Sicherheitsfähigkeiten. Dazu gehört die automatische Abmeldung (ALOF), die unbefugten Zugriff verhindert, indem Benutzersitzungen nach einer voreingestellten Inaktivitätsperiode automatisch beendet werden. Audit-Kontrollen (AUDT) erfassen und protokollieren den Zugriff auf System- und Gesundheitsdaten. Die Autorisierung (AUTH) sorgt dafür, dass nur bestimmte Rollen innerhalb der Gesundheitsorganisation auf die entsprechenden Daten und Funktionen zugreifen können. Weitere wichtige Funktionen umfassen die Konfiguration von Sicherheitsfunktionen (CNFS), die Anpassung der Sicherheitsmaßnahmen an die Bedürfnisse der Gesundheitsorganisation ermöglicht, sowie die regelmäßige Installation von Cybersicherheits-Produktupdates (CSUP), um die Sicherheit durch Sicherheits-Patches zu gewährleisten. Besonders wichtig ist auch die Deidentifikation von Gesundheitsdaten (DIDT), um sensible Patientendaten zu anonymisieren, sowie Maßnahmen zur Datensicherung und Katastrophenwiederherstellung (DTBK), die nach einem Datenverlust oder Systemausfall die Kontinuität der Geschäftsprozesse sicherstellen. Der Notfallzugriff (EMRG) ermöglicht den Zugriff auf geschützte Daten in kritischen Situationen, während die Integrität und Authentizität von Gesundheitsdaten (IGAU) gewährleistet, dass die Daten unverändert und authentisch bleiben. Ergänzt werden diese Maßnahmen durch den Malware-Schutz (MLDP), der Prävention, Erkennung und Entfernung von schädlicher Software umfasst. Zusätzliche Sicherheitsmechanismen, wie die Knotenauthentifizierung (NAUT) zur Authentifizierung von Geräten im Netzwerk und die Personenauthentifizierung (PAUT) zur eindeutigen Identifizierung und Authentifizierung von Benutzern, sorgen für eine hohe Zugriffssicherheit. Der physische Schutz der Geräte wird durch physische Sperren (PLOK) gewährleistet, und die Sicherheit von Drittanbieter-Komponenten im Produktlebenszyklus (RDMP) wird durch ein strenges Management während der gesamten Produktnutzung sichergestellt. Um die Angriffsfläche zu minimieren, wird die System- und Anwendungshärtung (SAHD) empfohlen, während Sicherheitsanleitungen (SGUD) klare Richtlinien und Anweisungen für Benutzer und Administratoren liefern. Schließlich betont die Guideline die Vertraulichkeit der Gesundheitsdaten-Speicherung (STCF), bei der Verschlüsselungstechnologien zum Schutz gespeicherter Daten eingesetzt werden, sowie die Vertraulichkeit (TXCF) und Integrität (TXIG) der Übertragung von Gesundheitsdaten, um sicherzustellen, dass diese während der Übertragung weder verfälscht noch unbefugt eingesehen werden. Diese umfassenden Empfehlungen und spezifischen Sicherheitsfähigkeiten bieten einen robusten Rahmen für den sicheren Betrieb von vernetzten medizinischen Geräten in IT-Netzwerken. [42]

Die IEC TR 80001-2-2 Guideline bietet einen umfassenden Rahmen für das Management von Risiken in IT-Netzwerken, die medizinische Geräte umfassen. Regelmäßige Risikobewertungen helfen, auf dem neuesten Stand der Bedrohungslage zu bleiben und Sicherheitsmaßnahmen entsprechend anzupassen. Die Kombination aus technischen (z.B. Firewalls, Antivirus-Software, Verschlüsselung) und organisatorischen Maßnahmen (z.B. klare Verantwortlichkeiten, Schulungen) bietet einen umfassenden Schutz gegen Cyberangriffe. Die fortlaufende Überwachung der Netzwerkumgebung ermöglicht es,

Sicherheitsvorfälle frühzeitig zu erkennen und zu beheben, bevor sie größeren Schaden anrichten können. Regelmäßige Schulungen und Sensibilisierungsmaßnahmen fördern ein allgemeines Sicherheitsbewusstsein und stellen sicher, dass alle Mitarbeiter über die neuesten Bedrohungen und Sicherheitspraktiken informiert sind. Die Guideline bietet einen soliden Rahmen für das Management von Cybersecurity -Risiken in IT-Netzwerken ist allerdings bereits schon 2012 veröffentlicht worden. Sie bietet mehrere Beispiele für Sicherheitseigenschaften die ein guter Input für die Definition von Anforderungen und Risiken sein kann und gibt auch ein konkretes Beispiel wie abgeleitete Anforderungen definiert werden können. Sie bietet aber nur grundlegende Leitlinien, aber keine detaillierten technischen Spezifikationen für spezifische Maßnahmen. Dies erschwert die direkte Anwendung auf komplexe IT-Netzwerke und Medizingeräte.

IEC TR 80001-2-8 - Application of risk management for IT- networks incorporating medical devices – Part 2-8: Application guidance – Gui- dance on standards for establishing the security capabilities identified in IEC TR 80001-2-2

Die IEC TR 80001-2-8 Guideline bietet Gesundheitsorganisationen (HDOs) und Herstellern von Medizinprodukten (MDMs) einen Leitfaden zur Anwendung des Rahmens aus IEC TR 80001-2-2 [42]. Diese Guideline identifiziert spezifische Sicherheitskontrollen und deren Anwendung im Risikomanagement von IT-Netzwerken, die medizinische Geräte umfassen. Ein wesentlicher Bestandteil ist die Implementierung eines systematischen Risikomanagement-Prozesses, der die Identifikation, Analyse, Bewertung und Kontrolle von Risiken beinhaltet, während klare Verantwortlichkeiten und Zuständigkeiten innerhalb des Risikomanagement-Teams festgelegt werden. Die Verwendung von Sicherheitsfähigkeiten (Security Capabilities) spielt eine zentrale Rolle in der Umsetzung dieser Kontrollen. Für jede Fähigkeit werden ein Anforderungsziel sowie ein Nutzerbedarf definiert, um den spezifischen Sicherheitsanforderungen gerecht zu werden. Zu den wichtigen Sicherheitsfähigkeiten und den dazugehörigen Kontrollen gehören unter anderem die automatische Abmeldung (ALOF), die unbefugten Zugriff auf Gesundheitsdaten verhindert, indem sie nach einer voreingestellten Inaktivitätsperiode Benutzersitzungen automatisch abmeldet oder sperrt. Audit-Kontrollen (AUDT) ermöglichen die Nachverfolgung von System- und Datenzugriffen durch die Erstellung von Audit-Trails. Die Autorisierung (AUTH) regelt den kontrollierten Zugriff auf Daten und Funktionen basierend auf den spezifischen Rollen der Benutzer. Weiterhin ermöglicht die Konfiguration von Sicherheitsfunktionen (CNFS) eine Anpassung der Sicherheitsmaßnahmen entsprechend den Bedürfnissen der jeweiligen Gesundheitsorganisation. Die Cybersicherheits-Produktupdates (CSUP) garantieren die Verwaltung von Sicherheitsupdates und -patches, während die Gesundheitsdaten-Deidentifikation (DIDT) sicherstellt, dass identifizierbare Patientendaten für unterschiedliche Zwecke anonymisiert werden können. Für den Fall eines Datenverlustes oder Systemausfalls stellt die Datensicherung und Katastrophenwiederherstellung (DTBK) sicher, dass die Geschäftskontinuität aufrechterhalten wird. In Notfallsituationen ermöglicht der Notfallzugriff (EMRG) den Zugriff auf geschützte Gesundheitsdaten. Um die Integrität und Authentizität von Gesundheitsdaten zu gewährleisten, sorgt die Integrität und Authentizität von Gesundheitsdaten (IGAU) dafür, dass

die Daten unverändert und authentisch bleiben. Der Schutz vor schädlicher Software wird durch die Malware-Erkennung/-Schutz (MLDP) gewährleistet, die Prävention, Erkennung und Entfernung von Malware beinhaltet. Zur Authentifizierung von Geräten im Netzwerk dient die Knotenauthentifizierung (NAUT), um die Sicherheit der Gesundheitsdaten zu schützen. Ergänzend dazu sorgt die Personenauthentifizierung (PAUT) für die eindeutige Identifikation und Authentifizierung von Benutzern, um den Zugriff auf Geräte und Netzwerke zu kontrollieren. Weitere Sicherheitsmaßnahmen umfassen physische Sperren am Gerät (PLOK), um unbefugten physischen Zugriff auf Geräte zu verhindern, sowie das Management von Drittanbieter-Komponenten im Produktlebenszyklus (RDMP), das die Sicherheit von Drittanbieter-Komponenten während des gesamten Produktlebenszyklus sicherstellt. Die System- und Anwendungshärtung (SAHD) reduziert die Angriffsfläche durch Abschalten unnötiger Dienste und das Schließen von Ports, während Sicherheitsanleitungen (SGUD) klare Richtlinien und Anleitungen für Benutzer und Administratoren bereitstellen. Zur Sicherung gespeicherter Gesundheitsdaten wird die Vertraulichkeit der Gesundheitsdaten-Speicherung (STCF) durch Verschlüsselungsmaßnahmen gewährleistet. Die Vertraulichkeit der Übertragung (TXCF) schützt die Daten während der Übertragung, und die Integrität der Übertragung (TXIG) sorgt dafür, dass Gesundheitsdaten unverfälscht bleiben. Diese umfassenden Sicherheitskontrollen stellen sicher, dass vernetzte medizinische Geräte in IT-Netzwerken sicher betrieben werden können. [41]

Der Technical Report stellt 19 spezifische Sicherheitsfähigkeiten (Security Capabilities) bereit, die auf die Bedürfnisse von Gesundheitsorganisationen und Medizingeräteherstellern zugeschnitten sind. Er deckt technische, administrative und organisatorische Sicherheitskontrollen ab, welche die Risiken beim Betrieb medizinischer IT-Netzwerke mindern. Ein besonderer Vorteil liegt in der Flexibilität: Die Leitlinien können je nach Risikoprofil und Einsatzumgebung angepasst werden, was eine maßgeschneiderte Implementierung der Sicherheitsmaßnahmen ermöglicht. Die Integration verschiedener internationaler Sicherheitsstandards, wie EN ISO/IEC 27002 [33], ISO 27799 [45] und NIST SP 800-53 [65], schafft eine umfassende Grundlage und fördert die Kompatibilität mit etablierten Sicherheitspraktiken im Gesundheitswesen. Trotz der umfassenden Leitlinien fehlt es dem Technical Report an detaillierten technischen Spezifikationen für die Umsetzung spezifischer Sicherheitsmaßnahmen, was die praktische Anwendung erschweren kann. Die Anpassungsfähigkeit des Technical Reports an unterschiedliche Umgebungen bedeutet auch, dass die Verantwortung für die konkrete Implementierung stark bei den Gesundheitsorganisationen liegt, was in ressourcenbeschränkten Umgebungen eine Herausforderung darstellen kann.

IEC TR 60601-4-5 - Medizinische elektrische Geräte - Teil 4-5: Leitfaden und Bewertung – Sicherheitsbezogene technische Anforderungen für Security

Die IEC TR 60601-4-5 Guideline bietet detaillierte technische Spezifikationen zur IT-Sicherheit von medizinischen Geräten, die in medizinischen IT-Netzwerken eingesetzt werden. Diese Empfehlungen gelten für medizinische elektrische Geräte, medizinische elektrische Systeme und medizinische Software. Das Dokument dient als Leitfaden zur

Integration dieser Geräte in IT-Netzwerke mit definierten Sicherheitsstufen (Security Levels, SL) und basiert auf den Anforderungen aus IEC/TS 62443-1-1, die spezifisch für medizinische Geräte angepasst wurden. Zu den grundlegenden Anforderungen an die IT-Sicherheit gehören Identifikation und Authentifizierung (IAC), Nutzungskontrolle (UC), Systemintegrität (SI), Datenvertraulichkeit (DC), eingeschränkter Datenfluss (RDF), rechtzeitige Reaktion auf Ereignisse (TRE) und Ressourcenverfügbarkeit (RA). Diese Anforderungen stellen sicher, dass medizinische Geräte sicher in vernetzten Umgebungen betrieben werden können. Zur Erfüllung dieser Anforderungen werden verschiedene Maßnahmen empfohlen. Technische Maßnahmen umfassen den Einsatz von Firewalls, Antiviren-Software und Verschlüsselungstechnologien. Administrative Maßnahmen beinhalten die Implementierung von Sicherheitsrichtlinien und -verfahren, während physische Maßnahmen den Schutz der Geräte durch verschlossene Türen und gekapselte Leiterplatten sicherstellen. Eine zentrale Vorgabe der Guideline ist, dass IT-Sicherheitsmaßnahmen die wesentlichen Funktionen der medizinischen Geräte nicht beeinträchtigen dürfen. Darüber hinaus müssen Zugangskontrollen und Notfallzugriffsfunktionen vorhanden sein, um sicherzustellen, dass das Gerät im Notfall zugänglich bleibt. Falls der Sicherheitslevel des IT-Netzwerks (SL-T) den Sicherheitslevel des Geräts (SL-C) übersteigt, sind Maßnahmen zur Minderung von Sicherheitslücken erforderlich. Die Guideline betont zudem die Bedeutung der Datenminimierung, das heißt, medizinische Geräte sollen nur die notwendigen sensiblen und personenbezogenen Daten speichern und übertragen. Zu den spezifischen technischen Anforderungen gehören Hardware-Sicherheitsmaßnahmen, die kritische Komponenten des Geräts durch spezielle Hardware-Mechanismen schützen. Darüber hinaus werden übergreifende Sicherheitsmerkmale beschrieben, wie etwa spezielle Firecall-Funktionen, Sicherheitslevels und die Berücksichtigung der Umgebung, in der das Gerät verwendet wird. Diese umfassenden Anforderungen tragen dazu bei, dass medizinische Geräte sicher und zuverlässig in vernetzten IT-Systemen betrieben werden können. [40]

Die IEC TR 60601-4-5 Guideline betont die Wichtigkeit eines umfassenden und systematischen Ansatzes zur IT-Sicherheit von medizinischen Geräten, die in IT-Netzwerken verwendet werden. Ein strukturierter Risikomanagement-Prozess ist entscheidend, um die Identifikation und Kontrolle von Cybersecurity-Risiken sicherzustellen. Es ist hilfreich für verschiedene Schutzziele jeweils die Security Levels zu bestimmen und bei den Security Levels zwischen einem „Target Security Level", einem „Capabiliy Security Levelünd einem „Achieved Security Levelßu unterscheiden. Dadurch können gewisse Anforderungen priorisiert werden. Jedoch fehlt in dem Technical Report eine klare Vorgehensweise zum Beispiel anhand vom Entwicklungsprozess. Außerdem sind keine Anforderungen bezüglich der Marktbeobachtung enthalten. Zusätzlich gibt die Guidance nicht immer konkrete Anforderungen vor wie man das anhand der Anforderung erkennt, dass DoS Attacken keine „Safety-related“ Funktionen behindern sollte.

MDCG 2019-16 - Guidance on Cybersecurity for medical devices

Die MDCG 2019-16 Guideline bietet einen umfassenden Rahmen für die Cybersicherheit von Medizinprodukten und legt detaillierte Anforderungen und Prozesse fest, um die

Sicherheit und den Schutz von Daten und Systemen während des gesamten Lebenszyklus eines Medizinprodukts zu gewährleisten. Ziel dieser Guideline ist es, Herstellern Anleitungen zur Erfüllung der Cybersicherheitsanforderungen gemäß der Medizinprodukteverordnung (MDR) [81] und der Verordnung über In-vitro-Diagnostika (IVDR) [82] zu geben. Diese Anforderungen betreffen sowohl den Schutz der Privatsphäre und Vertraulichkeit von Daten als auch die Betriebssicherheit der Systeme. Zu den grundlegenden Cybersicherheitskonzepten gehört die Definition von Risiko als Kombination aus der Wahrscheinlichkeit eines Schadens und dessen Schwere. Unter IT-Sicherheit versteht die Guideline den Schutz von Computersystemen vor nachteiligen Auswirkungen auf Hardware, Software und Daten. Informationssicherheit bezieht sich auf den Schutz vor Diebstahl, Löschung oder Veränderung von Daten, während die Betriebssicherheit den Schutz vor beabsichtigten Verfälschungen von Verfahren und Arbeitsabläufen umfasst. Das Sicherheitsrisikomanagement spielt eine zentrale Rolle, indem Sicherheitsrisiken im Rahmen des allgemeinen Risikomanagements analysiert, bewertet und kontrolliert werden. Hersteller müssen Risiken identifizieren, die sich sowohl aus der bestimmungsgemäßen Verwendung als auch aus vorhersehbarer Fehlanwendung ergeben, und geeignete Maßnahmen zur Risikominimierung umsetzen. In der sicheren Konstruktion und Fertigung sollten Sicherheit, Schutz und Wirksamkeit bereits in einem frühen Entwicklungsstadium berücksichtigt und während des gesamten Lebenszyklus eines Produkts aufrechterhalten werden. Der Ansatz der „Sicherheit durch Designßtellt sicher, dass alle sicherheitsrelevanten Aktivitäten sorgfältig geplant und ausgeführt werden. Die Guideline verlangt von den Herstellern, die IT-Mindestanforderungen für Hardware, Netzwerke und Sicherheitsmaßnahmen festzulegen, die für den ordnungsgemäßen Betrieb der Software erforderlich sind. Diese Anforderungen sollten in der Gebrauchsanweisung klar beschrieben und dokumentiert sein, um die Einhaltung der Sicherheitsstandards zu gewährleisten. Nach dem Inverkehrbringen sind Hersteller verpflichtet, ein System zur Überwachung und Vigilanz aufrechtzuerhalten. Cybersicherheitsvorfälle und potenzielle Schwachstellen müssen kontinuierlich überwacht und unverzüglich gemeldet werden, um die Sicherheit und Zuverlässigkeit der Produkte dauerhaft zu gewährleisten. [60]

Die Leitlinie stellt sicher, dass Cybersicherheit über den gesamten Lebenszyklus eines Produkts hinweg berücksichtigt wird – von der Planung und Herstellung bis hin zur Überwachung nach der Markteinführung. Der Fokus auf das Prinzip „Sicherheit durch Design“ stellt sicher, dass Sicherheitsmaßnahmen bereits in der Entwicklungsphase integriert werden, was eine bewährte Praxis in der Cybersicherheit ist. Zusätzlich skizziert sie einen strukturierten Risikomanagementprozess und betont die Bedeutung der kontinuierlichen Überwachung und Aktualisierung von Medizinprodukten, nachdem sie auf den Markt gebracht wurden. Die MDCG 2019-16 macht deutlich, dass Cybersicherheit eine geteilte Verantwortung zwischen Herstellern, Gesundheitsdienstleistern (HCPs) und anderen beteiligten Akteuren ist. Die Leitlinie legt den Schwerpunkt auf die Verantwortung der Hersteller und Gesundheitsdienstleister, geht jedoch nicht ausreichend auf die Risiken ein, die durch Drittanbieter und externe Zulieferer entstehen. Da viele moderne Medizinprodukte auf Software und Komponenten von Drittanbietern angewiesen sind, wäre eine tiefere Auseinandersetzung mit dem Management von Drittanbieterrisiken notwendig.

Zusätzlich gibt sie den Herstellern klare Hinweise zu verschiedenen Sicherheitsfähigkeiten (wie Authentifizierung, Verschlüsselung und Zugriffskontrollen), die sie in ihren Produkten implementieren sollten. Diese konkreten Beispiele sind besonders nützlich für Hersteller, die möglicherweise nicht über umfassende interne Cybersicherheitsressourcen verfügen und praktische Ratschläge benötigen. Obwohl die Leitlinie eine gute Übersicht über potenzielle Cybersicherheitslücken bietet, geht sie nicht tief genug auf spezifische und sich schnell entwickelnde Bedrohungen wie Ransomware oder IoT-basierte Angriffe ein, die zunehmend auf das Gesundheitswesen abzielen. Hersteller könnten sich gezwungen sehen, zusätzliche Informationsquellen zu konsultieren, um diese aufkommenden Bedrohungen besser zu verstehen und zu adressieren. Zwar wird das Thema Legacy-Geräte angesprochen, jedoch fehlt eine detaillierte Anleitung, wie Hersteller und Gesundheitsdienstleister mit älteren, möglicherweise unsicheren Geräten umgehen sollen, die nicht von Grund auf mit Cybersicherheitsfunktionen entwickelt wurden. Da diese Geräte weiterhin in Gesundheitseinrichtungen weit verbreitet sind, wäre eine detailliertere Anleitung zu ihrer Absicherung wünschenswert. Die Leitlinie fördert die Transparenz in Bezug auf die verwendeten Softwarekomponenten, was durch die Einführung einer Software-Stückliste (SBOM) erleichtert werden kann. Es fehlen jedoch praktische Anweisungen, wie Hersteller diese SBOM effektiv erstellen, verwalten und verteilen sollen, insbesondere in komplexen Lieferketten.

Principles and Practices for Medical Device Cybersecurity

Die Guideline bietet umfassende Empfehlungen zur Cybersicherheit von Medizinprodukten und richtet sich an Hersteller, Gesundheitsdienstleister, Regulierungsbehörden und Nutzer. Ihr Hauptziel besteht darin, Cybersicherheitsrisiken zu minimieren und gleichzeitig die Sicherheit und Leistungsfähigkeit von Medizinprodukten aufrechtzuerhalten. Ein zentraler Grundsatz der Cybersicherheit ist die globale Harmonisierung, da die Cybersicherheit von Medizinprodukten ein globales Anliegen ist. Sicherheitsvorfälle können weltweit die Patientensicherheit gefährden, weshalb eine internationale Angleichung der Cybersicherheitsmaßnahmen notwendig ist. Dies soll nicht nur die Sicherheit verbessern, sondern auch Innovationen fördern und den zeitnahen Zugang zu sicheren und wirksamen Medizinprodukten ermöglichen. Ein weiterer Grundsatz ist der Lebenszyklusansatz, der besagt, dass Cybersicherheitsrisiken während des gesamten Lebenszyklus eines Medizinprodukts berücksichtigt werden sollten. Dies umfasst die Phasen Design, Herstellung, Testen und die Überwachung nach dem Inverkehrbringen. Zudem wird die geteilte Verantwortung aller Beteiligten betont, einschließlich Hersteller, Gesundheitsdienstleister, Nutzer und Regulierungsbehörden. Jeder Beteiligte muss seine Verantwortung verstehen und eng zusammenarbeiten, um Cybersicherheitsrisiken kontinuierlich zu überwachen, zu bewerten, zu mindern und darüber zu kommunizieren. Ein proaktiver Informationsaustausch vor und nach der Markteinführung wird ebenfalls als unerlässlich angesehen. Dieser verbessert die Fähigkeit, Bedrohungen zu identifizieren und Risiken effektiv zu managen. Alle Beteiligten sollten aktiv am Informationsaustausch teilnehmen, um die Kommunikation von Cybersicherheitsvorfällen, -bedrohungen und -schwachstellen zu fördern. Vor der Markteinführung sind Sicherheitsanforderungen und Architekturdesign wichtige Überlegungen. Proaktive Maßnahmen wie Bedrohungsmodellierung sollten bereits in der

Entwurfsphase ergriffen werden, da diese effektiver sind als rein reaktive Maßnahmen. Ein umfassendes Risikomanagement sollte alle Phasen des Produktlebenszyklus abdecken, um potenzielle Cybersicherheitsrisiken zu identifizieren, zu bewerten, zu kontrollieren und kontinuierlich zu überwachen. Darüber hinaus sollten die Produkte umfassenden Sicherheitstests unterzogen werden, einschließlich statischer und dynamischer Analysen sowie Penetrationstests. Hersteller müssen klare Dokumentationen über ihre Cybersicherheitsmaßnahmen und Risikomanagementaktivitäten vorlegen, die sowohl für die regulatorische Prüfung als auch für die Überwachung nach der Markteinführung notwendig sind. Nach der Markteinführung sollten Gesundheitsdienstleister sicherstellen, dass die Geräte sicher in ihrer vorgesehenen Umgebung betrieben werden. Ein effektiver Informationsaustausch zwischen allen relevanten Akteuren ist entscheidend, um Cybersicherheitsbedrohungen effektiv zu managen. Es wird auch empfohlen, transparente Verfahren zur koordinierten Schwachstellenoffenlegung zu etablieren, um Sicherheitslücken zu identifizieren und zu beheben. Für ältere Geräte, die nicht mehr ausreichend gegen aktuelle Bedrohungen geschützt werden können, wird der Umgang mit Legacy-Geräten thematisiert. Solche Geräte sollten als veraltet betrachtet und aus dem Verkehr gezogen werden, um die Sicherheit zu gewährleisten. [43]

Die Betonung auf die Berücksichtigung von Cybersicherheitsrisiken während des gesamten Lebenszyklus eines Medizinprodukts, von der Entwicklung bis zum Ende der Unterstützung (End of Support), bietet Herstellern klare Richtlinien zur fortlaufenden Überwachung und Verbesserung der Sicherheitsmaßnahmen. Dieser Ansatz ist besonders nützlich, da er die Hersteller dazu anregt, auch nach der Markteinführung potenzielle Schwachstellen zu überwachen und entsprechende Updates bereitzustellen. Die Guidance betont die geteilte Verantwortung zwischen Herstellern, Gesundheitsdienstleistern und Nutzern, was einen kollaborativen Ansatz zur Cybersicherheit fördert. Jedoch bleiben die spezifischen Rollen und Verantwortlichkeiten der Endnutzer (z.B. Patienten oder Pflegepersonal) vage. Das Dokument bietet klare Empfehlungen zur Sicherheitsarchitektur und -gestaltung, einschließlich der Implementierung von Sicherheitsanforderungen, Risikomanagement und Teststrategien. Ein strukturierter Ansatz für die koordinierte Offenlegung von Schwachstellen (Coordinated Vulnerability Disclosure, CVD) unterstützt Hersteller dabei, Schwachstellen systematisch zu identifizieren und angemessene Maßnahmen zur Risikominderung zu ergreifen, was das Vertrauen der Nutzer und Regulierungsbehörden stärkt. Obwohl das Dokument die Bedeutung der Risikobewertung betont, bleibt es bei der Beschreibung der praktischen Umsetzung eher allgemein. Die spezifischen Methoden und Tools für die Risikobewertung, wie Bedrohungsmodellierung oder Schwachstellenbewertung, könnten detaillierter beschrieben werden, um Herstellern klarere Anweisungen zu geben. Während die Notwendigkeit einer kontinuierlichen Überwachung nach der Markteinführung betont wird, fehlt es an klaren Vorgaben, wie oft und in welchem Umfang diese Überwachung stattfinden sollte. Obwohl der Informationsaustausch als grundlegendes Prinzip festgelegt ist, hängt seine Wirksamkeit stark von der Bereitschaft und den Fähigkeiten der beteiligten Akteure ab. In der Praxis könnte der Mangel an Ressourcen oder Kooperationsbereitschaft den Informationsfluss behindern, was potenziell zu Verzögerungen bei der Behebung von Sicherheitslücken führen könnte.

DRAFT ONR CEN/CLC/TS 18026 - Mehrschichtiger Ansatz für einen Anforderungskatalog für Informations-/Cybersicherheitsmaßnahmen für Cloud-Dienste.

Die DRAFT ONR CEN/CLC/TS 18026 Guideline bietet eine umfassende Reihe von Cybersicherheitsanforderungen für Cloud-Dienste, die sowohl für Anbieter von Cloud-Diensten als auch deren Unterdienstleister gelten. Zu den grundlegenden Prinzipien gehört die Etablierung eines Informationssicherheitsmanagementsystems (ISMS), das der Verwaltung und Kontrolle von Informationssicherheitsrisiken dient. Dabei wird die Trennung von Aufgaben und Verantwortlichkeiten betont, um Interessenkonflikte zu vermeiden. Zudem wird die Kontaktpflege mit Behörden und Interessengruppen empfohlen, um die Einhaltung gesetzlicher Anforderungen sicherzustellen. Die Guideline fordert die Entwicklung und Umsetzung einer Informationssicherheitspolitik, die spezifische Sicherheitsanforderungen und Verfahren festlegt. Diese Politik sollte auch Richtlinien für den Umgang mit Ausnahmen enthalten. Ein Risikomanagement-Prozess zur Identifikation, Bewertung und Behandlung von Risiken ist ebenso erforderlich, wobei regelmäßige Risikobewertungen durchgeführt und entsprechende Maßnahmen zur Risikobehandlung ergriffen werden müssen. Das Personalmanagement wird ebenfalls als zentral angesehen, mit Richtlinien zur Überprüfung der Kompetenz und Vertrauenswürdigkeit der Mitarbeiter. Schulungen und Sensibilisierungsmaßnahmen zur Informationssicherheit sind essenziell, um ein sicheres Arbeitsumfeld zu fördern. Weiterhin wird empfohlen, ein Inventar aller Informationswerte zu führen und deren sichere Handhabung und Nutzung zu regeln. Die Betriebssicherheit umfasst die Planung und Überwachung der IT-Ressourcen, den Schutz vor Malware und die regelmäßige Durchführung von Datensicherungen und Tests, um die Integrität und Verfügbarkeit der Daten sicherzustellen. Sicherheitsrelevante Ereignisse und Vorfälle sollten zudem protokolliert und überwacht werden. Im Bereich des Identitäts-, Authentifizierungs- und Zugriffsmanagements fordert die Guideline die Implementierung von Richtlinien zur Zugriffskontrolle auf Informationen sowie zur Verwaltung von Identitäten und Zugriffsrechten. Diese Rechte sollten regelmäßig überprüft und aktualisiert werden, wobei starke Authentifizierungsmechanismen und der Schutz von Zugangsdaten unerlässlich sind. Die Kommunikationssicherheit spielt ebenfalls eine wichtige Rolle, wobei technische Schutzmaßnahmen zur Sicherung der Netzwerkinfrastruktur implementiert und die Netzwerkverbindungen überwacht werden sollten. Datenströme in gemeinsam genutzten Netzwerken müssen getrennt werden, und es ist eine Dokumentation der Netzwerktopologie sowie der Richtlinien für die Datenübertragung erforderlich. Bei der Entwicklung von Informationssystemen sollten Sicherheitsrichtlinien sowohl bei der Entwicklung als auch bei der Beschaffung berücksichtigt werden. Dies schließt die Sicherheit in der Entwicklungslieferkette und im Entwicklungsumfeld ein. Zudem müssen Schwachstellen in Cloud-Diensten identifiziert und behoben werden. Für das Vorfallsmanagement verlangt die Guideline Richtlinien für die Handhabung, Dokumentation und Meldung von Informationssicherheitsvorfällen. Die Schulung der Nutzer zur Meldepflicht solcher Vorfälle und die Einbindung betroffener Parteien sind ebenfalls wichtige Punkte. Abschließend betont die Guideline die Produktsicherheit, die durch Mechanismen zur Fehlerbehandlung und Protokollierung, effektives Sitzungsmanagement sowie die Auswahl

geeigneter Datenverarbeitungs- und Speicherstandorte gewährleistet werden sollte. [19]

Die Anforderungen an Risikobewertungen und die Behandlung identifizierter Risiken bieten eine Grundlage für Hersteller, potenzielle Schwachstellen systematisch zu erkennen und zu beheben. Die Richtlinien zur Vorfallbewältigung (Incident Management) sind besonders wertvoll. Sie legen fest, wie Informationssicherheitsvorfälle behandelt, dokumentiert und gemeldet werden sollten. Diese klare Struktur hilft Herstellern, im Falle eines Vorfalls schnell und effizient zu reagieren und Schäden zu minimieren. Außerdem wird die Notwendigkeit der Erhaltung von Beweismaterial betont, was für die Analyse und die Prävention zukünftiger Vorfälle entscheidend ist. Die Richtlinien zur Verwaltung von Identitäts- und Zugriffskontrollen sind detailliert und bieten klare Vorgaben zur sicheren Verwaltung von Zugangsrechten. Dies umfasst Mechanismen zur Authentifizierung, zum Schutz von Zugangsdaten sowie zur Überprüfung und Anpassung von Zugriffsrechten. Während das Dokument viele allgemeine Sicherheitsanforderungen abdeckt, bleibt die konkrete Behandlung spezifischer Bedrohungen wie Ransomware oder gezielte Angriffe auf Cloud-Dienste eher oberflächlich. Obwohl das Dokument klare Anforderungen stellt, fehlen oft detaillierte Anweisungen zur praktischen Umsetzung. Es gibt zwar viele Vorgaben, die „erfüllt werden müssen", aber weniger konkrete Schritte, wie diese Maßnahmen effektiv in komplexen Infrastrukturen implementiert werden können. In der sich ständig ändernden Bedrohungslandschaft könnte das Dokument von einem dynamischeren Ansatz profitieren, der regelmäßige Bedrohungsanalysen und Anpassungen der Sicherheitsmaßnahmen stärker betont.

ISO/TR 24971 - Medical devices - Guidance on the application of ISO 14971

Die ISO/TR 24971 Guideline bietet umfassende Leitlinien zur Entwicklung, Implementierung und Aufrechterhaltung eines Risikomanagementsystems für Medizinprodukte gemäß EN ISO 14971 [30]. Ein zentraler Aspekt dieser Guideline ist der Risikomanagementprozess, der Teil eines Qualitätsmanagementsystems sein sollte, jedoch gemäß EN ISO 14971 [30] nicht zwingend erforderlich ist. Dieser Prozess umfasst die Identifikation, Analyse, Bewertung und Kontrolle von Risiken über den gesamten Lebenszyklus eines Medizinprodukts. Die Identifikation von Gefahren und gefährlichen Situationen ist ein weiterer wichtiger Bestandteil. Hierbei ist es entscheidend, Gefahren zu identifizieren, die sich durch Sicherheitslücken ergeben können, insbesondere im Bereich Cybersicherheit und Datenschutz. Diese Sicherheitslücken können zu schwerwiegenden Konsequenzen wie Datenverlust, unbefugtem Zugriff auf Patientendaten oder der Offenlegung personenbezogener Gesundheitsinformationen führen, was letztlich Patienten schaden kann. Das Sicherheitsrisikomanagement verwendet oft andere Terminologien als EN ISO 14971 [30], jedoch gibt es Entsprechungen zwischen den Begriffen. Zentrale Begriffe, die dabei eine Rolle spielen, sind Sicherheit, Bedrohung, Schwachstelle, Vertraulichkeit, Integrität und Verfügbarkeit. Der Prozess des Risikobewertung und -kontrolle ist ähnlich wie bei anderen Risikomanagementprozessen. Er umfasst die Festlegung von Akzeptanzkriterien, die Bewertung und Kontrolle von Risiken sowie die kontinuierliche Überwachung. Es wird darauf hingewiesen, dass durch Sicherheitsmaßnahmen möglicherweise neue Risiken entstehen können, weshalb diese Maßnahmen sorgfältig bewertet werden müssen. Ein

weiterer wichtiger Aspekt ist die Priorisierung von Vertraulichkeit, Integrität und Verfügbarkeit. Bei der Bewertung sicherheitsrelevanter Risiken muss der Hersteller sicherstellen, dass diese Prioritäten entsprechend der beabsichtigten Verwendung des Medizinprodukts berücksichtigt werden. Besonders kritisch kann beispielsweise der Verlust der Verfügbarkeit bei lebenserhaltenden Geräten sein. Im Anhang F der Guideline werden die Begriffe des Sicherheitsrisikomanagements wie Sicherheit, Bedrohung, Schwachstelle, Vertraulichkeit, Integrität und Verfügbarkeit definiert und erläutert. Zudem wird das Verhältnis zwischen EN ISO 14971 [30] und Sicherheit verdeutlicht. Während Sicherheit im allgemeinen Sinne den Schutz vor feindlichen Handlungen oder Einflüssen betrifft, hat sie im Kontext von Medizinprodukten breitere Auswirkungen. Beispielsweise können Schäden an elektronischen Gesundheitsakten zu falschen Diagnosen führen, was die Patientensicherheit gefährdet. Darüber hinaus beschreibt die Guideline die Eigenschaften des Sicherheitsrisikomanagements, die sich zwar in den Grundschritten ähneln, jedoch in den spezifischen Datenquellen, Analysetools und Techniken variieren können. Im Anhang H werden spezielle Leitlinien für In-vitro-Diagnostika (IVD) aufgeführt. Hier liegt der Fokus auf der Risikobewertung von Merkmalen, die die Patientensicherheit betreffen, wie Systemzuverlässigkeit, Kompatibilität von Komponenten, Softwarezuverlässigkeit und Benutzbarkeit des Systems. Darüber hinaus wird die Bedeutung der digitalen Informationstechnologie hervorgehoben, insbesondere in Bezug auf die korrekte Patienten- und Probenidentifikation sowie die Integrität digitaler Daten und deren Übertragung. [53]

Das Dokument bietet eine klare Struktur für die Implementierung eines Risikomanagementprozesses über den gesamten Lebenszyklus eines Produkts hinweg, von der Entwicklung bis zur Deinstallation. Das Dokument deckt eine Vielzahl von Medizinprodukten ab, von Implantaten bis hin zu Software, bleibt aber bei bestimmten Produkttypen, wie Software als Medizinprodukt (SaMD), oft zu allgemein. Obwohl Cybersicherheitsrisiken behandelt werden, ist die Anleitung dazu in ISO/TR 24971 relativ allgemein und nicht tief genug, um den ständig wachsenden Herausforderungen der Cybersicherheit vollständig gerecht zu werden. Es gibt nur begrenzte Hinweise auf spezifische Bedrohungsmodelle und auf die Bewertung der Auswirkungen von Cyberangriffen auf medizinische Geräte.

Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity (N73)

Die Guideline behandelt die Cybersicherheit von Medizinprodukten, die entweder Software enthalten, wie Firmware und programmierbare Logiksteuerungen, oder ausschließlich als Software existieren, wie zum Beispiel Software als Medizinprodukt (SaMD). Sie hebt die Rolle und Verantwortung von Medizinproduktherstellern (MDMs) und Gesundheitsdienstleistern (HCPs) hervor und gibt Empfehlungen zur Implementierung einer Software-Stückliste (SBOM), um die Transparenz bei der Verwendung von Software in Medizinprodukten zu erhöhen. Eine der zentralen Empfehlungen betrifft das Risikomanagement und die Transparenz, wobei die SBOM eine wichtige Rolle im Cybersicherheitsrisikomanagement spielt – sowohl vor als auch nach der Markteinführung eines Medizinprodukts. Sie hilft dabei, bekannte Schwachstellen in der Software zu überwachen und verhindert, dass Geräte mit potenziellen Cybersicherheitsrisiken in den

Markt gelangen. Die SBOM-Generierung und -Verwaltung sollte während der Design- und Entwicklungsphase eines Produkts erfolgen, wobei die Informationen in einem Softwarekomponenten-Repository gespeichert werden. Bei jeder Veröffentlichung oder Aktualisierung eines Produkts sollte eine neue SBOM erstellt und verteilt werden. Diese SBOM sollte umfassende Informationen zu jeder Softwarekomponente enthalten, einschließlich des Autorennamens, eines Zeitstempels, des Softwarekomponentenlieferanten, sowie Name, Version und eindeutige Identifikatoren der Softwarekomponente und deren Beziehungen zu anderen Komponenten. Die Verteilung und Nutzung der SBOM sollte während des Beschaffungsprozesses oder bei Softwareveröffentlichungen an die HCPs erfolgen. HCPs müssen über die Existenz der SBOM informiert werden und Zugang zu ihr erhalten, entweder direkt vom Hersteller, über das Gerät selbst oder über ein zentrales Repository. Da die SBOM sensible und vertrauliche Informationen enthält, müssen die Kommunikationskanäle angemessen geschützt werden. Die Wartung der SBOM erfordert regelmäßige Aktualisierungen, um Änderungen an den Softwarekomponenten, wie Sicherheitsupdates, Funktionsänderungen oder das Ende der Unterstützung von Komponenten, zu berücksichtigen. Änderungen an der SBOM müssen den HCPs kommuniziert werden, um sicherzustellen, dass sie über potenzielle Risiken informiert sind. Trotz der Vorteile der SBOM gibt es einige Herausforderungen bei der Generierung, Überwachung und Verteilung, insbesondere bei älteren oder bereits auf dem Markt befindlichen Geräten. Standards und Werkzeuge zur Unterstützung der SBOM-Implementierung entwickeln sich stetig weiter, und Hersteller sollten grundlegende Konzepte anwenden und bei Bedarf fortgeschrittenere Verfahren einführen. In verschiedenen Anwendungsfällen kann die SBOM wertvolle Unterstützung bieten. Im Risikomanagement kann sie genutzt werden, um potenzielle Schwachstellen zu identifizieren und den Risikomanagementprozess zu unterstützen. Sie hilft bei der Überwachung und Bewertung von Schwachstellen und trägt zur Aufrechterhaltung eines akzeptablen Risikoprofils bei. Im Schwachstellenmanagement ermöglicht die SBOM die schnelle Identifizierung betroffener Geräte und verbessert die Genauigkeit und Aktualität der Schwachstellenbewertung. Sie unterstützt HCPs bei der Implementierung von Zwischenmaßnahmen zur Risikominderung, während der Hersteller die Auswirkungen bewertet oder Updates entwickelt. Beim Vorfallmanagement hilft die SBOM, sicherheitsrelevante Ereignisse systematisch zu erfassen, zu korrelieren und zu bewerten, wodurch die Handhabung von Sicherheitsvorfällen optimiert wird. [44]

Das Konzept des SBOM (Software Bill of Materials) wird klar erklärt und betont, wie wichtig es ist, Transparenz über die in Medizinprodukten verwendeten Softwarekomponenten herzustellen. Dies ist für Hersteller äußerst nützlich, um potenzielle Sicherheitslücken besser zu identifizieren und bekannte Schwachstellen in Drittanbieter-Software zu überwachen. Das SBOM-Framework deckt sowohl die Entwicklungsphase als auch die Post-Market-Phase ab und ist so gestaltet, dass es während des gesamten Lebenszyklus eines Medizinprodukts nützlich ist. Eine wesentliche Schwäche des Dokuments ist die unzureichende Behandlung von Cloud-Diensten, die zunehmend in Medizinprodukten verwendet werden. Es wird zwar darauf hingewiesen, dass Cloud-Software überprüft werden sollte, aber spezifische Empfehlungen für den Umgang mit Cloud-Sicherheitsrisiken fehlen. Das Dokument erkennt die Schwierigkeiten bei der Implementierung des SBOM-

Frameworks für ältere, bereits auf dem Markt befindliche Geräte an, bietet jedoch keine tiefgehenden Lösungen, wie Hersteller diese Herausforderungen überwinden können. Viele Hersteller haben Schwierigkeiten, umfassende SBOMs für Legacy-Geräte zu erstellen, da die ursprünglichen Softwarequellen möglicherweise nicht mehr verfügbar sind. Es werden gängige Formate wie CycloneDX, SPDX und SWID empfohlen, die zur Automatisierung der SBOM-Erstellung und -Verteilung verwendet werden können. Allerdings wird nicht ausreichend auf die praktischen Herausforderungen bei der Einführung solcher Automatisierungsprozesse eingegangen. Die technischen Anforderungen und die Komplexität der Implementierung bleiben eher oberflächlich behandelt. Während das Dokument auf die Sensibilität von SBOM-Daten hinweist, bleiben detaillierte Maßnahmen zur sicheren Verteilung und zum Schutz dieser Daten vage. Es wäre hilfreich, spezifischere Anforderungen oder Best Practices zur Sicherung der Verteilung von SBOMs festzulegen, um unbefugten Zugriff oder Missbrauch zu verhindern. Obwohl die Verwendung von APIs zur SBOM-Verteilung erwähnt wird, fehlen detaillierte Empfehlungen oder Standards, wie diese APIs sicher und interoperabel gestaltet werden können.

Principles and Practices of Cybersecurity for Legacy Medical Devices (N70)

Die Guideline bietet konkrete Empfehlungen zur Anwendung des Total Product Life Cycle (TPLC) Frameworks auf Legacy-Geräte, um die Implementierung der IMDRF N60-Richtlinie zu unterstützen. Sie konzentriert sich auf medizinische Geräte, die entweder Software enthalten, wie Firmware und programmierbare Logiksteuerungen, oder als reine Software existieren. Der Schwerpunkt liegt darauf, potenzielle Patientenschäden durch Cybersicherheitsbedrohungen zu minimieren. Zentraler Bestandteil der Empfehlungen ist die Anwendung des Total Product Life Cycle Frameworks, das sicherstellt, dass Cybersicherheitsrisiken während aller Phasen des Lebenszyklus eines Medizinprodukts berücksichtigt werden – von der Entwicklung über den Support, den begrenzten Support bis hin zum End of Support (EOS). Planungszyklen für die Cybersicherheit müssen darauf abzielen, den sicheren Betrieb von Medizinprodukten über ihren gesamten Lebenszyklus hinweg zu gewährleisten. Ein weiterer zentraler Punkt ist die Kommunikation. Offene und transparente Kommunikation zwischen allen Beteiligten ist entscheidend, um Bedrohungen effektiv abzuwehren. Medizinprodukthersteller (MDMs) sollten frühzeitig über das End of Life (EOL) und EOS ihrer Produkte informieren, damit Gesundheitsdienstleister (HCPs) die erforderlichen Maßnahmen planen können. Proaktive Kommunikation wird dabei empfohlen, anstatt Informationen nur passiv zur Verfügung zu stellen. Das geteilte Risikomanagement ist ebenfalls ein wesentliches Element der Guideline. Cybersicherheit wird als gemeinsame Verantwortung von MDMs und HCPs angesehen. MDMs sollten ihre Geräte so konzipieren, dass diese während der Support-Phase sicher betrieben werden können und die Sicherheitsrisiken nach EOS minimiert werden. HCPs sollten eng mit den MDMs zusammenarbeiten, um sicherzustellen, dass Geräte mit angemessenen Cybersicherheitsmaßnahmen betrieben werden. Im Rahmen der Risikobewertung und des Übergangs zwischen Lebenszyklusphasen sollten Risikobewertungen durchgeführt werden, um festzustellen, ob Patientensicherheitsrisiken bestehen, wenn ein Gerät oder eine Softwarekomponente das Ende ihrer Unterstützung erreicht. Besteht ein Risiko und das Gerät befindet sich noch in der Support-Phase, sollten MDMs durch Updates oder

Designänderungen Maßnahmen zur Risikominderung ergreifen. Die Guideline beschreibt auch die verschiedenen Stufen des Lebenszyklus. In der Entwicklungsphase sollten MDMs Sicherheit durch Design integrieren, Risikobewertungen durchführen, Bedrohungen identifizieren und Sicherheitsdokumentationen erstellen. In der Support-Phase sollten die Geräte umfassende Cybersicherheitsunterstützung erhalten, einschließlich Software-Patches und Sicherheitsupdates. Außerdem sollten MDMs einen koordinierten Prozess zur Offenlegung von Schwachstellen implementieren. In der Phase des begrenzten Supports befinden sich Geräte, die das EOL erreicht haben, jedoch weiterhin mit eingeschränkter Unterstützung betrieben werden. MDMs sollten weiterhin Cybersicherheitsunterstützung leisten, soweit dies möglich ist, und HCPs über Bedrohungen und erforderliche Sicherheitsmaßnahmen informieren. Schließlich wird nach End of Support (EOS) die Verantwortung für die Cybersicherheit eines Geräts hauptsächlich auf die HCPs übertragen. MDMs sollten HCPs frühzeitig über den Übergang zu EOS informieren und die notwendigen Informationen bereitstellen, um das Gerät entweder sicher zu betreiben oder außer Betrieb zu nehmen. [35]

Das Dokument hebt hervor, wie wichtig eine frühzeitige und transparente Kommunikation über End-of-Life (EOL) und End-of-Support (EOS) ist. Es wird empfohlen, dass Hersteller ihre Kunden (HCPs) mindestens 2-3 Jahre vor EOS informieren, um eine rechtzeitige Planung zu ermöglichen. Dies fördert eine proaktive Planung und reduziert das Risiko, dass veraltete Geräte ohne Schutz weiter verwendet werden. Obwohl das Dokument beschreibt, dass nach EOS die Cybersicherheitsverantwortung auf die Gesundheitsdienstleister übergeht, bleibt es in der Diskussion über konkrete Maßnahmen zur Risikominderung oft vage. Es wird zwar die Bedeutung von Netzwerksegmentierung, Firewalls und Anti-Malware-Lösungen erwähnt, jedoch fehlen spezifische technische Empfehlungen oder Best-Practice-Beispiele, wie diese Lösungen in der Praxis effektiv umgesetzt werden können. Zusätzlich fordert die Guidance die Offenlegung von Sicherheitslücken, gibt jedoch nur wenig spezifische Anweisungen, wie Hersteller den Prozess der Schwachstellenbehebung nach dem EOS unterstützen sollen. Gerade bei älteren Geräten, die keine Updates mehr erhalten, bleibt unklar, wie Gesundheitsdienstleister mit verbleibenden Schwachstellen umgehen sollen. Die finanziellen und personellen Herausforderungen, die mit der Implementierung von Cybersicherheitsmaßnahmen für Legacy-Geräte verbunden sind, werden nur am Rande erwähnt. Viele Gesundheitsdienstleister könnten Schwierigkeiten haben, die notwendigen Mittel und das technische Know-how aufzubringen, um Geräte nach EOS sicher zu betreiben.

3.4 Beispiele und Empfehlungen für die Entwicklung und den Betrieb sicherer medizinischer Geräte und Anwendungen in Bezug auf Cybersecurity

3.4.1 Risikoabschätzung und Bewertung

Eine zentrale Empfehlung zur Verbesserung der Cybersicherheit von medizinischen Geräten ist die Implementierung effektiver Risikobewertungssysteme. Im Paper [75] „A Cyber Risk Scoring System for Medical Devices“ wird ein System vorgeschlagen, das auf den potenziellen negativen Auswirkungen eines Cyberangriffs auf den Patienten basiert. Dieses System verwendet das STRIDE-Modell zur Identifizierung von Sicherheitsbedrohungen und kombiniert dies mit dem Common Vulnerability Scoring System (CVSS), um eine robuste Risikobewertung zu ermöglichen.[75]

Das STRIDE-Bedrohungsmodell ist ein systematischer Ansatz zur Identifikation und Klassifikation von Sicherheitsbedrohungen anhand der Kategorien Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service und Elevation of Privilege [28]. Das Common Vulnerability Scoring System (CVSS) ist ein standardisiertes Bewertungssystem für IT-Sicherheitslücken, das Schwachstellen anhand von Basiseigenschaften, zeitabhängigen Faktoren und umgebungsspezifischen Bedingungen auf einer Skala von 0 bis 10 bewertet. Diese Art von Bewertungssystemen bietet nicht nur Herstellern, sondern auch Gesundheitseinrichtungen und Aufsichtsbehörden eine leicht verständliche und benutzerfreundliche Methode zur Identifizierung und Minimierung von Cyberrisiken. Die Möglichkeit, Risiken für Patienten zu klassifizieren und zu priorisieren, ist besonders entscheidend in einem Bereich, in dem Cyberangriffe unmittelbare Auswirkungen auf die Gesundheit und das Leben von Patienten haben können. [75]

Die Methodik zur Risikoanalyse im Paper „Cybersecurity for Medical Device Manufacturers: Ensuring Safety and Functionality“ orientiert sich an dem Standard EN ISO 14971 und erweitert diesen um spezifische Cybersicherheitsaspekte, die für Medizingeräte relevant sind. Zu Beginn werden die elektronischen Assets, wie Netzwerkkommunikation, Gesundheitsdaten und Softwareinformationen, identifiziert, um diese gezielt schützen zu können. Anschließend folgt die systematische Analyse möglicher Bedrohungen und Angriffe, wobei die Auswirkungen auf die Vertraulichkeit, Integrität und Verfügbarkeit der Assets untersucht werden. Im nächsten Schritt werden potenzielle Sicherheitsrisiken bewertet, um zu prüfen, ob sie eine Gefährdung für die Sicherheit darstellen. Dabei werden mögliche System-Schwachstellen berücksichtigt, die durch unbefugten Zugriff, Datenmanipulation oder Designmängel entstehen könnten. Diese Schwachstellenanalyse wird sowohl von oben nach unten (Top-Down), etwa durch Fehlerbaumanalyse, als auch von unten nach oben (Bottom-Up) mittels Fehlermöglichkeits- und -einflussanalyse (FMEA) durchgeführt, um eine umfassende Bewertung zu gewährleisten. Abschließend werden Risikokontrollen und spezifische Sicherheitsmaßnahmen definiert, die die Wahrscheinlichkeit und Schwere potenzieller Bedrohungen reduzieren. Dazu gehören Mechanismen

für ein sicheres Design, Angriffswegkontrollen sowie Maßnahmen zur Erkennung und Wiederherstellung im Falle eines Angriffs. [86]

Die Methodik zur Risikoanalyse im Paper „Risk assessment of cyber-attacks on telemetry-enabled cardiac implantable electronic devices (CIED)“ folgt einem dreistufigen Ansatz, der auf den Standards ISO/IEC 27005 und NIST SP 800-30 basiert und eine umfassende Bewertung der Cyberrisiken für CIEDs ermöglicht. Zunächst erfolgt eine akteurbasierte Analyse, bei der potenzielle Angreifer, ihre Motive und die möglichen Auswirkungen auf das CIED-System identifiziert werden. Dabei werden Bedrohungen hinsichtlich ihrer Auswirkungen auf Gesundheit, finanzielle Verluste, Lebensqualität und Privatsphäre klassifiziert. In der szenariobasierten Analyse werden daraufhin realistische Angriffsszenarien beschrieben, basierend auf den bekannten Schwachstellen der Geräte. Die Wahrscheinlichkeit des Eintretens dieser Szenarien wird unter Berücksichtigung der technischen Fähigkeiten, der Zugangsmöglichkeiten und der Motivation potenzieller Angreifer bewertet. Abschließend kombiniert die Risikoanalyse die Erkenntnisse beider Schritte, um das Gesamtrisiko für jedes Szenario zu berechnen. Hierbei wird das Risiko nach Schweregraden eingestuft, von untragbar bis vernachlässigbar, und entsprechende Empfehlungen für das Risikomanagement formuliert. Diese Methodik stellt sicher, dass sowohl die technischen Schwachstellen der CIEDs als auch die potenziellen Schäden für Patienten und Gesundheitseinrichtungen umfassend berücksichtigt werden. [63]

3.4.2 Spezifische Sicherheitsprotokolle für medizinische Geräte

Eine wichtige Strategie zur Verbesserung der Cybersicherheit medizinischer Geräte ist die Entwicklung maßgeschneiderter Sicherheitsprotokolle. Das Paper „APSec1.0: Innovative Security Protocol Design for the Artificial Pancreas System"befasst sich mit der Entwicklung eines speziellen Sicherheitsprotokolls für das Künstliche Pankreas-System (APS), ein Implantat, das automatisch den Blutzuckerspiegel überwacht und Insulin abgibt. Die APSec1.0-Methodik umfasst drei Phasen, die den Sicherheitsanforderungen gerecht werden. In der Registrierungsphase wird durch Identifikations- und Authentifizierungsprotokolle sichergestellt, dass nur autorisierte Geräte miteinander kommunizieren. Hierbei kommt das Elliptic-Curve-Diffie-Hellman Ephemeral (ECDHE)-Verfahren zum Einsatz, das „Perfect Forward Secrecy"bietet und damit selbst bei Schlüsselverlust vergangene und zukünftige Sitzungen schützt. In der Kommunikationsphase findet der Datenaustausch zwischen den APS-Komponenten, wie der kontinuierlichen Glukosemessung (CGM) und der Insulinpumpe (IP), über verschlüsselte Kanäle statt, um die Integrität und Vertraulichkeit der Blutzuckerwerte und Insulindosierungen zu gewährleisten. Die Notfallphase tritt bei Ausfall des zentralen Controllers in Kraft, wobei CGM und IP auf einen Notfallschlüssel zurückgreifen, um die Insulinverabreichung sicherzustellen, bis der Controller wieder verfügbar ist. [56]

3.4.3 Sicherheitsanforderungen für Software in medizinischen Geräten

Die Methodik im Paper „Security and Privacy for Implantable Medical Devices“ definiert spezifische Sicherheits- und Datenschutzanforderungen für implantierbare medizinische Geräte (IMDs), um deren besonderen Schutzbedarf zu erfüllen. Die Sicherheitsziele umfassen die Gewährleistung der Verfügbarkeit, um Ausfälle oder Denial-of-Service-Angriffe zu verhindern, die Sicherstellung der Datenintegrität sowie den Schutz der Gerätekonfiguration, sodass nur autorisierte Personen Änderungen vornehmen können. Die Datenschutzziele konzentrieren sich darauf, die Existenz und den Typ des Implantats vor unbefugten Personen zu verbergen und den Zugang zu spezifischen Identifikationsdaten und Messwerten abzusichern. Zudem legt die Methodik besonderen Wert auf Autorisierungs- und Authentifizierungsprozesse, die den Zugang zu IMDs auf berechtigte Akteure wie medizinisches Fachpersonal und Hersteller beschränken, und in Notfällen entsprechend anpassbar sind, um die Sicherheit des Patienten zu gewährleisten. Durch eine fein abgestufte Zugangskontrolle und die Protokollierung aller Zugriffe wird die Auditierbarkeit sichergestellt, wodurch sämtliche Interaktionen nachvollziehbar bleiben. [38]

3.4.4 Frameworks für Bedrohungserkennung und Prävention

Die Bedeutung von automatisierten Systemen zur Erkennung und Prävention von Cyberangriffen nimmt in einer zunehmend vernetzten Welt rasant zu. Im Paper [62] „Extreme learning machine and bayesian optimization-driven intelligent framework for IoMT cyber-attack detection"wird eine maschinelle Lernmethode zur Bedrohungserkennung im Internet der Medizinischen Dinge (IoMT) vorgeschlagen. Dieses Modell kombiniert die Extreme Learning Machine (ELM) mit Bayesianischer Optimierung und zeigt, wie Angriffe in Echtzeit erkannt und darauf reagiert werden können. Da medizinische Geräte und Systeme zunehmend miteinander vernetzt sind, ermöglichen solche intelligenten Frameworks eine dynamische und effiziente Erkennung von Bedrohungen, die auf bösartige Aktivitäten in sensiblen medizinischen Netzwerken hindeuten. Die Skalierbarkeit dieser Systeme und ihre Fähigkeit, auf komplexe Bedrohungen zu reagieren, machen sie zu einem wertvollen Werkzeug zur Sicherstellung der Cybersicherheit in modernen Gesundheitssystemen. [62]

Im Paper [57] „It takes a pirate to know one: ethical hackers for healthcare cybersecurity"wird die Rolle von ethischen Hackern bei der Verbesserung der Cybersicherheit im Gesundheitswesen hervorgehoben. Penetrationstests sind ein effektives Mittel, um Schwachstellen in IT-Systemen und medizinischen Geräten aufzudecken. Diese Methode wird in anderen Sektoren erfolgreich angewendet, um Sicherheitslücken zu identifizieren und Cybersicherheitsmaßnahmen zu stärken. [57]

3.4.5 Sicherheitsmechanismen für vernetzte Geräte

Im Paper [85] „Cybercrimes Pose Growing Threat to Medical Devices“ werden mehrschichtige Schutzstrategien zur Cybersicherheit für vernetzte Medizingeräte beschrieben. Grundlegender Schutz wird durch Antivirus-Software bereitgestellt, jedoch ist deren Einsatz bei Medizingeräten aufgrund der spezifischen Konfigurationen und Hardware-Beschränkungen oft eingeschränkt. Host Intrusion Detection and Prevention Systems (HIDS/HIPS) bieten zusätzliche Sicherheit durch Whitelisting und Blockieren unbekannter Aktionen und wirken auch gegen Zero-Day-Angriffe. Strenge Zugangskontrollen für Administratoren-Konten, USB-Ports und drahtlose Verbindungen verhindern unbefugten Zugriff, während eine Boot-Konsistenzprüfung das Systemverhalten beim Start überwacht und Abweichungen erkennt. Netzwerksegmentierung und Firewalls tragen durch die Trennung und Absicherung einzelner Netzwerksegmente zum Schutz vor Angriffen bei. Regelmäßige Netzwerkscans und Patch-Management sorgen für die frühzeitige Erkennung und Behebung von Schwachstellen, indem Software und Betriebssysteme stets auf dem neuesten Stand gehalten werden. Ein umfassendes Asset- und Konfigurationsmanagement ermöglicht durch detaillierte Inventarisierung die Überwachung der Systemkonfiguration, was für Wartung und Sicherheitsmanagement essenziell ist. [85]

Die Methodik für IT-Sicherheitsuntersuchungen in vernetzten Medizinprodukten gemäß dem Paper „Cyber-Sicherheitsbetrachtung vernetzter Medizinprodukte“ basiert auf einem strukturierten, umfassenden Prüfansatz. Die Untersuchung beginnt mit einer Analyse der Angriffsoberfläche durch die Bewertung vorhandener Designdokumente, Schnittstellen und Spezifikationen des Medizinprodukts. Besonders wichtig ist die detaillierte Erfassung aller Komponenten, Technologien und Kommunikationsprotokolle, die im Gerät und seiner Umgebung genutzt werden, um mögliche Angriffspunkte zu identifizieren. Die eigentliche Prüfung erfolgt durch spezifische Tests auf verschiedenen Ebenen: Schnittstellen und Kommunikationsprotokolle werden auf Sicherheitslücken wie ungesicherte Authentifizierungsmechanismen, unsichere Kommunikation und Schwachstellen in den Verschlüsselungsmethoden überprüft. In diesen Tests wird häufig eine Kombination aus Black-Box und White-Box-Ansätzen verwendet, wobei der White-Box-Ansatz bevorzugt wird, da er eine effizientere Analyse ermöglicht und die Wahrscheinlichkeit erhöht, Schwachstellen zu erkennen. Zusätzlich umfasst die Methodik Tests auf Hardware-Ebene, bei denen die internen Komponenten auf sicherheitsrelevante Schwachstellen überprüft werden. Durch die Identifikation und Überprüfung physischer Schnittstellen wie USB oder serielle Verbindungen wird die Möglichkeit der Manipulation und des unbefugten Zugriffs untersucht. Der Umfang der Tests erstreckt sich schließlich auf die Analyse von Netzwerkinfrastrukturen und Serverkomponenten, um potenzielle Konfigurationsfehler und bekannte Schwachstellen im System zu identifizieren und abzusichern. [78]

3.4.6 Netzwerküberwachung zur Verbesserung der Cybersicherheit

Das Paper [79] „Selecting a Passive Network Monitoring Solution for Medical Device Cybersecurity Management"hebt die Vorteile einer passiven Netzwerküberwachung (PNM) hervor, um den Netzwerkverkehr zu überwachen, ohne die Funktionalität kritischer medizinischer Geräte zu beeinträchtigen. Die Methode des passiven Netzwerk-Monitorings (PNM) für medizinische Geräte basiert auf der Analyse und Überwachung des Netzwerkdatenverkehrs, ohne dass dabei direkt in die Geräte eingegriffen wird. PNM-Lösungen greifen Kopien des gesamten Netzwerkverkehrs von Netzwerk-Switches oder Netzwerk-TAPs (Test Access Points) ab. Dadurch kann das Monitoring erfolgen, ohne den Betrieb oder die Leistung der Geräte zu beeinträchtigen. Die gesammelten Daten enthalten wichtige Metadaten wie IP-Adressen, MAC-Adressen, Ports und Protokollinformationen, die analysiert werden, um die Geräte im Netzwerk zu identifizieren und deren Kommunikationsmuster zu verstehen, ohne die Inhalte der Pakete zu lesen. Mithilfe spezifischer Algorithmen ordnet das PNM-System jedes überwachte Gerät einer Kategorie zu, beispielsweise einer Infusionspumpe oder einem Beatmungsgerät. Diese Klassifikation erfolgt anhand der einzigartigen Netzwerk-Muster und Protokolle, die die Geräte verwenden, wie HL7 oder DICOM. Auf dieser Basis erstellt die PNM-Lösung eine Inventarliste der verbundenen Geräte, die kontinuierlich aktualisiert wird, wenn Geräte hinzugefügt oder entfernt werden, was eine vollständige Übersicht aller aktiven Geräte und deren Kommunikationsaktivitäten ermöglicht. Durch die ständige Überwachung der Netzwerkkommunikation erkennt das System Abweichungen von den normalen Kommunikationsmustern. Sollte ein Gerät ungewöhnliche Aktivitäten wie unerwartete Verbindungen oder hohe Datenübertragungen zeigen, markiert das PNM-System dies als potenziellen Sicherheitsvorfall und gibt eine Warnung aus. Die gesammelten Daten dienen zudem der Bewertung des Risikoniveaus einzelner Geräte. Geräte mit hohem Risikopotenzial, wie solche mit veralteter Firmware oder ungewöhnlichem Verhalten, können so gezielt überprüft und geschützt werden. [79]

3.4.7 Einfluss menschlicher Faktoren auf die Cybersicherheit

Das Paper [64] „Influence of Human Factors on Cyber Security within Healthcare Organisations“ betont die Bedeutung menschlicher Faktoren für die Stärkung der Cyber-Resilienz im Gesundheitswesen. Ein wesentlicher Punkt ist die Schulung von Mitarbeitenden zur Erkennung und Reaktion auf Social-Engineering-Angriffe wie Phishing. Da menschliche Fehler in stressigen Umgebungen häufig zu Sicherheitslücken führen, beispielsweise durch unautorisierten Zugang oder das Teilen von Passwörtern, wird eine gewohnheitsbasierte Schulung empfohlen. Diese soll sicherstellen, dass Sicherheitspraktiken fest in den Arbeitsalltag integriert werden, sodass beispielsweise das Erkennen von Phishing-Versuchen zur Routine wird. Das Paper unterstreicht zudem die Wichtigkeit kontinuierlicher Sensibilisierungsprogramme, die auf den Kontext des Gesundheitswesens zugeschnitten sind, insbesondere im Hinblick auf den Schutz von Informationen in sozialen Medien, die oft von Angreifern ausgenutzt werden. Es wird empfohlen, Cyber-Hygiene und die regelmäßige Einhaltung von Sicherheitsprotokollen auf allen Ebenen der Organisation zu

fördern. Die Kombination aus technischen Maßnahmen und Verhaltensanpassungen wird als entscheidend für eine robuste Cybersecurity-Strategie betrachtet. [64]

3.5 Beschreibung des Werkzeuges zur Bestimmung des Security Levels

Im Rahmen dieser Masterarbeit wurde eine Checkliste zur Beurteilung des Security Levels eines Medizinprodukts in Bezug auf Cybersecurity entwickelt. Diese Checkliste basiert auf einem Leitfaden des Johner Instituts [54] und wurde in drei Hauptkapitel unterteilt.

A) Allgemeine Anforderungen

B) Anforderungen an die Prozesse

C) Anforderungen an das Produkt

Insgesamt beinhaltet die Checkliste 165 Anforderungen.

3.5.1 Hauptkapitel: A) Allgemeine Anforderungen

Innerhalb des Hauptkapitel „Allgemeine Anforderungen"gliedern sich die Anforderungen in folgende Unterkapitel:

1. Kompetenzen: Dieses Unterkapitel beschäftigt sich mit der Sicherstellung der Kompetenzen innerhalb des Herstellungsprozesses. Hierzu ein Beispiel aus diesem Bereich:

- *Die (Software-) Entwicklungspläne legen produktspezifisch die (darüber hinausgehenden oder abweichenden) Kompetenzen fest*

  Diese Forderung kommt aus folgenden Normen EN 62304, EN ISO 13485 und IEC 60601-1 und ist das Security Level 3 zugeordnet.

2. Prozesse: Das Unterkapitel bezieht sich auf die Dokumentation und Implementierung standardisierter Verfahren für alle wesentlichen Prozesse, die mit dem Lebenszyklus eines Produkts verbunden sind. Hierzu ein Beispiel aus dem Bereich:

- *Der Hersteller muss ein Verfahren für die Entwicklung dokumentieren*

  Diese Forderung kommt aus den Normen EN ISO 13485 und EN 62304 und ist das Security Level 1 zugeordnet.

3.5.2 Hauptkapitel: B) Anforderungen an die Prozesse

Die Anforderungen innerhalb dieses Hauptkapitels sind in die folgenden Unterkapitel unterteilt:

1. Anforderungen an die Produktentwicklung

a) Zweckbestimmung und Stakeholder-Anforderungen: Die Anforderungen befassen sich mit der systematischen Identifikation, Bewertung und Dokumentation von Rollen, Nachbarsystemen, Nutzungsumgebungen, Risiken und regulatorischen Anforderungen. Hierzu ein Beispiel aus dem Bereich:

- *Der Hersteller hat die vorgesehene Nutzungsumgebung festgelegt.*

  Diese Forderung kommt aus folgenden Normen IEC 81001-5-1 und EN IEC 62443-4-1 und ist das Security Level 2 zugeordnet.

b) System- und Software-Anforderungen

i) Authentifizierung und Autorisierung: Diese Anforderungen umfassen die Identifikation, Spezifikation und Sicherung von Datenschnittstellen und Funktionen, die Analyse ihrer Sicherheitsrelevanz sowie die Festlegung von Zugriffsrechten und Mechanismen zur Authentifizierung.

ii) Daten und Kommunikation: Die Anforderungen beinhalten die Identifikation, Bewertung und den Schutz der durch das System verwalteten Daten sowie die Analyse und Absicherung gegen potenzielle Risiken wie Datenverlust, Systemüberlastung, Netzwerkausfälle und Sicherheitsverletzungen.

iii) Patch- und Schwachstellenmanagement: Diese Anforderungen betreffen die strukturierte Planung, Dokumentation und Verwaltung von Patches sowie die Identifikation und Bewertung von SOUP- und OTS-Komponenten.

iv) Sonstiges: Hierzu gehören Anforderungen zur Festlegung von Maßnahmen zur Benachrichtigung der Anwender sowie zur Sicherstellung der grundlegenden Funktionalitäten des Medizinprodukts im Falle von IT-Sicherheitskompromittierungen.

c) System- und Software-Architektur: Die Anforderungen konzentrieren sich auf die umfassende Dokumentation, Analyse und Absicherung von Software-Komponenten, Diensten und Architekturen, einschließlich der Identifikation von Risiken, der Minimierung von Angriffsflächen, der Implementierung von Defense-in-Depth-Prinzipien und der Sicherstellung eines sicheren Betriebs durch Threat-Modeling, sichere Updates, Logging und die kontinuierliche Überprüfung der Systemarchitektur.

d) Implementierung und Erstellung der Software: Die Anforderungen betreffen die Erstellung von IT-sicherheitsorientierten Coding-Guidelines, die Analyse und Absicherung von Software gegen Schadcode und Buffer-Overflows sowie die Bewertung von Änderungen an der Software oder SOUP, um sicherzustellen, dass bestehende Risikobeherrschungsmaßnahmen nicht beeinträchtigt werden

e) Bewertung von Software-Einheiten: Die Anforderungen befassen sich mit der Festlegung und Durchführung von Maßnahmen zur Sicherstellung der Qualität und Sicherheit des Codes, einschließlich der Überprüfung der Einhaltung von Coding-Guidelines, der Durchführung von Code-Reviews nach definierten Kriterien und dem Vier-Augen-Prinzip sowie der Planung und Durchführung von Tests mit klaren Vorgaben für Abdeckung und Verifizierung, insbesondere für SOUP- und OTS-Komponenten

f) System- und Software-Tests: Diese Anforderungen umfassen die sorgfältige Planung und Durchführung von Sicherheits- und Funktionstests. Dazu gehören Portscans, Penetrationstests, Fuzz-Tests, Vulnerability-Scans sowie die Analyse gegen Angriffsvektoren und auf Robustheit. Ergänzt wird dies durch Expertenbewertungen und die Einbeziehung externer Testberichte, um die Sicherheit und Zuverlässigkeit des Systems zu gewährleisten.

g) Produktfreigabe: Die Anforderungen beinhalten eine umfassende Risikoanalyse sowie die detaillierte Dokumentation und Nachvollziehbarkeit von Maßnahmen zur Kontrolle von IT-Sicherheitsrisiken. Dies umfasst die Erstellung von Traceability-Matrizen, Risikomanagement- und Sicherheitsberichten sowie die Planung für die nachfolgende Produktphase, um die Sicherheit und Compliance über den gesamten Lebenszyklus des Produkts sicherzustellen.

Hierzu ein paar Beispiele aus dem Bereich:

- *Der Hersteller hat die vorgesehene Nutzungsumgebung festgelegt.* aus 1)a)

  Diese Forderung kommt aus folgenden Normen EN IEC 81001-5-1 und EN IEC 62443-4-1 und ist das Security Level 2 zugeordnet.

- *Der Hersteller verfügt eine Liste aller SOUP-/OTS-Komponenten* aus dem Unterkapitel 1)b)iii)

  Diese Forderung kommt aus folgenden Normen EN 62304, EN ISO 13485 und IEC 60601-1 und ist das Security Level 2 zugeordnet.

- *Der Hersteller hat Coding-Guidelines erstellt, die Anforderungen spezifisch für die IT-Sicherheit stellt.* aus 1)d)

  Diese Forderung kommt aus folgenden Normen ISO/IEC 15408-2, EN ISO/IEC 27002, ISO 27799, EN IEC 81001-5-1 and EN IEC 62443-4-1 und ist das Security Level 2 zugeordnet.

2. Anforderungen an die der Entwicklung nachgelagerten Phasen

a) Produktion, Distribution, Installation: Die Anforderungen befassen sich mit der Sicherstellung einer kontrollierten und fehlerfreien Auslieferung, Installation und Nutzung des Produkts, einschließlich der Versionskontrolle, der Vermeidung von Verwechslungen, der Erfüllung spezifizierter Anforderungen und der Etablierung effizienter Kommunikationsverfahren mit Betreibern und Anwendern.

b) Marktüberwachung: Diese Anforderungen umfassen die Planung, Erfassung, Bewertung und Nutzung von Informationen aus der Post-Market-Surveillance-Phase. Sie beinhalten die Überwachung von OTS-Komponenten und Technologien sowie die Implementierung von Verfahren zur Identifikation von Sicherheitsanomalien, um die IT-Sicherheit und Konformität des Produkts kontinuierlich sicherzustellen und zu optimieren.

c) Incident Response Plan: Die Anforderungen betreffen die Erstellung eines Incident Response Plans, der den Umgang mit Sicherheitsvorfällen regelt, einschließlich der Bewertung von Marktinformationen, der Entwicklung, Verteilung und Installation von Patches, der Kundenkommunikation sowie von Maßnahmen wie Stilllegung oder Rückruf, ergänzt durch einen Plan für die regelmäßige Bereitstellung und Überprüfung von Patches.

Hierzu ein paar Beispiele aus dem Bereich:

- *Der Hersteller hat beschrieben, wie er überwacht, dass verwendete Technologien und Verfahren (z.B. Kryptologie) noch sicher sind* aus 2)b)

  Diese Forderung kommt aus folgenden Normen EN IEC 81001-5-1 und EN IEC 62443-4-1 und ist das Security Level 3 zugeordnet.

- *Der Hersteller hat einen Plan erstellt, wie er reguläre Patches entwickelt, verteilt und die Verteilung überprüft*

  Diese Forderung kommt aus folgenden Normen EN IEC 81001-5-1 und EN IEC 62443-4-1 und ist das Security Level 3 zugeordnet.

3.5.3 Hauptkapitel: C) Anforderungen an das Produkt

Die Anforderungen dieses Hauptkapitels sind in die nachstehenden Unterkapitel gegliedert:

1. System-/Software-Anforderungen

a) Authentifizierung: Die Anforderungen befassen sich mit der Implementierung und Verwaltung sicherer Authentifizierungs- und Zugriffskontrollmechanismen, einschließlich Passwortregeln, Benutzer- und Rollenmanagement, Schutz vor unautorisierten Zugriffen, Sitzungsmanagement, Sicherheitsprüfungen in Client-Server-Architekturen sowie dem Schutz und der Verwaltung sensibler Authentifikations- und Zugriffselemente.

b) Kommunikation und Speicherung: Die Anforderungen fokussieren sich auf den Schutz der Datenintegrität, Vertraulichkeit und Verfügbarkeit durch Maßnahmen wie Verschlüsselung, Zugriffskontrollen, Überprüfung von Eingaben und Daten, sichere Speicherung, Schutz vor Datenverlust und ungewollten Veränderungen sowie Notfallmechanismen und Wiederherstellungsoptionen für den sicheren Betrieb und die Patientensicherheit.

c) Patches: Die Anforderungen befassen sich mit der sicheren Handhabung von Patches, einschließlich deren Installation, Entfernung (Roll-back), Zugriffsbeschränkungen auf

autorisierte Benutzer, Integritätsprüfungen sowie der sicheren Löschung sensibler Daten bei der Außerbetriebnahme des Produkts.

d) Sonstiges: Die Anforderungen befassen sich mit der Protokollierung und Sicherung wesentlicher Systemaktionen durch ein unveränderbares Audit-Log, die Gewährleistung der korrekten Systemzeit und der Implementierung von Mechanismen zur Erkennung und Reaktion auf Einbrüche oder Angriffe.

Hierzu ein paar Beispiele aus dem Bereich:

- *Das Produkt erlaubt den Benutzern nur dann seine Nutzung, wenn sie sich am Produkt authentifiziert haben* aus 1)a)

  Diese Forderung kommt aus folgenden Normen ISO/IEC 15408-2, EN ISO/IEC 27002, ISO 27799, EN IEC 62443-4-2 und EN ISO/IEC 27001 und ist das Security Level 1 zugeordnet.

- *Das Produkt schützt Daten vor ungewolltem Löschen.* aus 1)b)

  Diese Forderung kommt aus der folgenden Norm ISO/IEC 27002 und ist das Security Level 3 zugeordnet.

2. System-/Software-Architektur: Die Anforderungen fokussieren sich auf die sichere Implementierung von kryptographischen Funktionen mittels bewährter Bibliotheken, die Nutzung unterschiedlicher Schlüssel oder Technologien für separate Zwecke, den Schutz vor Malware und die Verwendung sicherer Versionen von SOUP-/OTS-Komponenten ohne bekannte sicherheitsrelevante Schwachstellen. Hierzu ein Beispiel aus dem Bereich:

- *Die Software basiert auf den Versionen der SOUP-/OTS-Komponenten, für die keine sicherheitsrelevanten Schwachstellen bekannt sind. Ausnahmen sind begründet*

  Diese Forderung kommt aus den folgenden Normen EN IEC 81001-5-1 und EN IEC 62443-4-1 und ist das Security Level 2 zugeordnet.

3. Begleitmaterialien: Die Anforderungen beziehen sich auf die Bereitstellung umfassender Begleitmaterialien, die die IT-Umgebung, Betreiberaktivitäten, Sicherheitsmaßnahmen, den Umgang mit IT-Sicherheitsproblemen und Authentifizierungselementen sowie technische und organisatorische Anweisungen zur Nutzung und Außerbetriebnahme des Produkts klar definieren. Hierzu ein Beispiel aus dem Bereich:

- *Die Gebrauchsanweisung legt die vorgesehene IT-Umgebung für den Betrieb fest.*

  Diese Forderung kommt aus den folgenden Normen EN IEC 81001-5-1, EN 82304-1 und EN IEC 62443-4-1 und ist das Security Level 2 zugeordnet.

3.6 Analyse der Umsetzung von regulatorischen Anforderungen sowie vorhandenen Empfehlungen bezüglich Cybersecurity

3.6.1 Ergebnis Temperaturmesssystem

Derzeit ist ist das Produkt nach der Richtlinie 93/42/EWG zugelassen.

Im Allgemeinen integriert der Hersteller Cybersicherheit-Maßnahmen im gesamten Produktlebenszyklus. Es werden Anforderungen im Bezug auf den Umgang beziehungsweise Verschlüsselung der Daten von den Patienten definiert. Außerdem werden regelmäßig Updates gemacht und im Verlauf des Marktbeobachtungsprozesses wird überprüft ob es zu etwaigen Schwachstellen gekommen ist.

Für den Hersteller sind besonders die Normen EN ISO 13485, EN ISO 14971, EN 62304, IEC 60601-1 und die EN 82304 relevant.

Als Cybersicherheitsmaßnahmen verwendet der Hersteller externe Tools wie „dependabot" und „npm Audit". „dependabot"− Sicherheitsupdates sind automatisierte Pull Requests, die dem Hersteller dabei helfen, Abhängigkeiten mit bekannten Sicherheitslücken zu aktualisieren. „dependabot" erstellt bei Versionsupdates oder Bugfixes automatisch einen Pull Requests von den im jeweiligen Code befindlichen SOUPs. So werden SOUPs aktuell gehalten, um einerseits bekannte Sicherheitslücken zu schließen, aber auch um neue Features zeitnahe in der Software inkludiert zu haben [2]. Das „npm Audit" übermittelt eine Beschreibung der im Projekt konfigurierten Abhängigkeiten an die „konfigurierte Registry" und fordert einen Bericht über bekannte Sicherheitslücken an. Wenn eine Schwachstelle gefunden wird, werden die Auswirkungen und die entsprechenden Abhilfemaßnahmen berechnet [66]. Eine weitere Sicherheitsmaßnahme ergibt sich aus der Produktkonfiguration selbst. So ist der Speicher im Sensor zum Beispiel mit einem "Hardlock"geschützt um die Datenintegrität sicher zu stellen. Zusätzliche wartet die App, die als Schnittstelle dient, auf die Antwort des Servers bevor sie Daten schickt. Im Zuge des Entwicklungsprozesses sowie im Änderungsprozess und Wartungsprozess wird die Software verifiziert und validiert.

Es existiert eine detaillierte Liste aller Rollen, die an der Produktentwicklung beteiligt sind, inklusive der notwendigen Kompetenzen für jede Rolle. Dies stellt sicher, dass alle Beteiligten über die nötigen Fähigkeiten verfügen und ihre Aufgaben ausführlich definiert sind. Die Software-Entwicklungspläne und Sicherheitsanforderungen sind klar dokumentiert und werden regelmäßig überprüft. Diese Pläne beinhalten wichtige Maßnahmen, um die Produktentwicklung sicher zu gestalten.

In jeder Phase des Entwicklungsprozesses wird eine Produktrisikoanalyse durchgeführt, und es gibt etablierte Maßnahmen, um Sicherheitslücken frühzeitig zu identifizieren und zu beheben. Prozesse und Systeme werden regelmäßig auditiert und überwacht, um die Einhaltung von Sicherheitsstandards sicherzustellen. Im Rahmen des Entwicklungsprozesses wurden umfassende Teststrategien definiert, die sicherstellen, dass Sicherheitsfunktionen auf Herz und Nieren geprüft werden.

Das Produkt nutzt Verschlüsselungstechnologien, um sicherzustellen, dass die Kommunikation zwischen verschiedenen Systemen oder Benutzern sicher abläuft. Diese Maßnahme schützt die Daten während der Übertragung.

In mehreren Fällen wurde festgestellt, dass das Produkt Benutzern den Zugang zu bestimmten Funktionen erlaubt, ohne dass eine ausreichende Authentifizierung an den Datenschnittstellen implementiert ist. Dies erhöht das Risiko, dass unautorisierte Benutzer auf kritische Funktionen zugreifen können. Es gibt Anforderungen zur Implementierung von erweiterten Authentifizierungsmethoden (z.B. MFA), die nicht erfüllt wurden. Ohne diese zusätzliche Schutzebene besteht ein erhöhtes Risiko für unbefugte Zugriffe. Es wurden keine ausreichenden Mechanismen implementiert, um sicherzustellen, dass die übertragenen und gespeicherten Daten während der Nutzung nicht verändert werden können. Echtzeit-Überwachung und Protokollierung (Logging) von sicherheitsrelevanten Ereignissen ist nicht in ausreichendem Maß vorhanden. Dadurch können Bedrohungen oder Sicherheitsvorfälle nicht zeitnah erkannt und entsprechend behandelt werden. Das Produkt erlaubt es möglicherweise, dass verschiedene Subsysteme oder Anwendungen ohne ausreichende Isolierung zusammenarbeiten. Dies bedeutet, dass eine Schwachstelle in einem Teil des Systems potenziell den Zugriff auf andere kritische Bereiche ermöglichen könnte.

Zusammenfassend erreicht das Medizinprodukt ein Security Level von 2. Gemäß der Zweckbestimmung des Temperaturmesssystems ist ein Security Level 2 für dieses Produkt ausreichend. Es besteht aber noch Verbesserungspotential, da nicht alle Anforderungen, denen ein Security Level 2 zugeordnet sind, erfüllt wurden.

3.6.2 Ergebnis Vorhersagemodell

Das Produkt ist derzeit nach der Richtlinie 93/42/EWG als Klasse I zertifiziert, wobei derzeit der Artikel 120 der MDR angewendet wird. Die Zulassung gemäß der MDR soll bis 2026/2027 abgeschlossen sein.

Für die Integration von Cybersicherheit im gesamten Produktlebenszyklus setzt der Hersteller auf eine dezentrale Installation der Software ausschließlich beim Kunden, wobei das Krankenhaus (KH) die volle Kontrolle über die Datensicherheit und den Serverzugang hat. Cybersicherheitsanforderungen wie die EN ISO/IEC 27000-Reihe und die IEC TR 80001-2-8 werden in der Client Requirement Specification festgelegt und müssen vom Kunden erfüllt werden.

Der Hersteller orientiert sich bei der Entwicklung seiner Medizinprodukte an wesentlichen Normen wie EN 62304 für Softwarelebenszyklusprozesse, IEC 62366 für Gebrauchstauglichkeit, EN ISO 14971 für Risikomanagement und EN ISO 13485 für Qualitätsmanagement. Spezifische Cybersicherheitsmaßnahmen umfassen eine Authentifizierungsmethode, bei der sich Ärzte im internen Krankenhausnetzwerk ohne zusätzliche Hürden anmelden können, während für den Zugriff über externe Geräte eine 2-Faktor-Authentifizierung vorgeschrieben ist.

Für das Medizinprodukt wurde eine detaillierte Risikobewertung mit den Methoden FMEA (Fehlermöglichkeits- und -einflussanalyse), Fault Tree Analysis und Hazard Analysis etabliert. Die Risiken werden anhand ihrer Eintrittswahrscheinlichkeit und Schweregrad bewertet.

Der Hersteller hat alle relevanten Rollen im Entwicklungsprozess klar definiert. Eine Liste aller Beteiligten, einschließlich Entwicklern, Testern und regulatorischen Experten, wurde erstellt, um eine präzise Aufgabenverteilung sicherzustellen. Für jede dieser Rollen sind die Kompetenzen festgelegt, sodass sichergestellt wird, dass jedes Teammitglied über das notwendige Wissen und die erforderlichen Fähigkeiten verfügt, um die Aufgaben sicher und effizient zu erfüllen. Auch führt der Hersteller angemessene Aufzeichnungen über die Schulungen und erworbenen Kompetenzen der Mitarbeiter, um sicherzustellen, dass alle Beteiligten die Anforderungen der jeweiligen Positionen erfüllen und stets auf dem neuesten Stand der Entwicklung sind.

Darüber hinaus werden produkt- und projektbezogene Entwicklungspläne festgelegt, die sicherstellen, dass die Einhaltung der notwendigen Sicherheitsstandards in der gesamten Softwareentwicklung gewährleistet ist. Dies beinhaltet auch die Implementierung von Verfahren, die sicherstellen, dass Sicherheitsrisiken über den gesamten Entwicklungsprozess hinweg identifiziert und gemindert werden.

Der Hersteller gewährleistet, dass alle Nachbarsysteme, wie Medizingeräte oder andere Informationssysteme, identifiziert und die Schnittstellen zu diesen klar beschrieben werden. Dies hilft, mögliche Interaktionen und Abhängigkeiten frühzeitig zu erkennen und potenzielle Sicherheitsprobleme zu adressieren. Weiterhin wird eine Liste der involvierten Rollen, einschließlich deren Verantwortlichkeiten, erstellt, um die Konformität und Sicherheit des Systems zu gewährleisten. Diese Maßnahmen stellen sicher, dass das Produkt sicher in verschiedene IT-Umgebungen integriert werden kann.

Für die Authentifizierung im internen Krankenhausnetzwerk verwendet der Hersteller eine Token-Logik, die vorab mit dem Kunden abgesprochen wird. Der Zugang erfolgt über einen URL-Link mit automatisch generiertem Token. Der Token enthält Passwörter, die aktuelle Uhrzeit, ist zusätzlich verschlüsselt und nur 30 Sekunden gültig. Der erstellte Token wird auf Seite vom Hersteller auf seine Gültigkeit überprüft. Beim einem Zugriff mit einem externen Gerät wird eine Zwei-Faktor-Authentifizierung verwendet.

Zusätzlich wird sicher gestellt, dass alle Datenschnittstellen durch entsprechende Sicherheitsmechanismen geschützt sind, sodass nur autorisierte und verifizierte Daten verarbeitet werden. Die Kommunikation zwischen dem Produkt und anderen Systemen wird verschlüsselt, um die Vertraulichkeit und Integrität der Daten während der Übertragung zu gewährleisten.

Der Hersteller stellt umfassende Gebrauchsanweisungen zur Verfügung. Diese Anleitungen enthalten detaillierte Informationen über vorgesehene IT-Umgebung. Es wird großen Wert darauf gelegt, dass die Anleitungen die Anforderungen an die Schulung der Benutzer umfassen. Auch die Installations- und Serviceanleitungen enthalten spezifische Informationen zur sicheren Installation und Wartung der Produkte.

Im Risikomanagementprozess gibt es beim Hersteller noch Lücken in der vollständigen Berücksichtigung und Dokumentation aller sicherheitsrelevanten Risiken. Zum Beispiel sind die Maßnahmen zur Identifizierung und Bewertung von Risiken für Nachbarsysteme und Patienten nicht vollständig umgesetzt. Es fehlt eine detaillierte Abschätzung, wie häufig Patienten oder Systeme bestimmten Risiken ausgesetzt sind. Auch ein umfassender Risikomanagementbericht, der den Status der Sicherheitsrisiken und deren Verwaltung transparent darlegt, ist bisher nicht vollständig ausgearbeitet.

Ein weiteres Defizit liegt in der fehlenden Definition von Coding-Guidelines. Der Hersteller hat bisher noch keine detaillierten Richtlinien für die Programmierung festgelegt, die sicherstellen, dass die Software konsistent und sicher entwickelt wird. Zudem fehlt die Implementierung von statischen Code-Analyse-Werkzeugen, die dafür verwendet werden könnten, den Quellcode automatisch auf Schwachstellen zu überprüfen. Diese Methoden sind besonders wichtig, um Fehler und Sicherheitslücken frühzeitig zu erkennen und zu beheben.

Im Bereich der Überwachung und Auswertung gibt es noch keine klaren Vorgaben, wie der Hersteller Betriebsdaten kontinuierlich überwachen wird, um Sicherheitsrisiken zu identifizieren. Ebenso nutzt der Hersteller die gewonnenen Erkenntnisse aus der Überwachung nicht ausreichend, um Prozesse und Produkte zu verbessern. Regelmäßige Audits zur Überprüfung der IT-Sicherheitsprozesse sind ebenfalls nicht etabliert, obwohl solche Audits wesentlich zur Aufrechterhaltung eines hohen Sicherheitsniveaus beitragen könnten.

Zusammenfassend erreicht das Medizinprodukt ein Security Level von 3. Entsprechend der Zweckbestimmung des Vorhersagemodells wird ein Security Level 3 als angemessen erachtet. Es besteht jedoch noch Verbesserungspotenzial, da nicht sämtliche Anforderungen, die diesem Security Level zugeordnet sind, vollständig erfüllt wurden.

3.6.3 Empfehlung für die Produkte um das Security Level zu verbessern

Empfehlungen Temperaturmesssystem

Um die Cybersicherheit des Medizinprodukts zu verbessern, sollten folgende Empfehlungen umgesetzt werden:

Zusammenarbeit mit externen Anbietern

Da der Hersteller mit einem externen Anbieter zusammenarbeitet, ist es entscheidend, klare Cybersicherheitsanforderungen zu definieren. Dazu sollte festgelegt werden, wie der Anbieter mit Aspekten der IT-Sicherheit umgeht und welche Schutzmaßnahmen er implementiert. Dies umfasst:

- Der Anbieter muss transparente Sicherheitsmaßnahmen haben und diese klar kommunizieren, um sicherzustellen, dass alle Parteien den gleichen Schutzstandard verfolgen.

- Der Anbieter sollte einen Plan zur Kommunikation im Falle einer Kompromittierung haben. Es muss klar definiert werden, wie und wann die Anwender informiert werden, wenn eine Sicherheitslücke entdeckt wurde. Zusätzlich sollten kritische Funktionen des Produkts trotz der Kompromittierung weiterhin gewährleistet sein.
- Das Produkt muss Mechanismen enthalten, um Kompromittierungen der IT-Sicherheit zu erkennen, diese in einem Logbuch zu dokumentieren und schnell darauf zu reagieren. Eine schnelle Reaktionszeit kann potenzielle Schäden minimieren.
- Es sollten Mechanismen gefordert werden, um unautorisierte Zugriffe auf das Produkt zu verhindern. Dazu können fortschrittliche Authentifizierungsverfahren oder Verschlüsselungstechniken zählen.
- Regelmäßige Portscans an relevanten Netzwerkschnittstellen sind erforderlich, um potenzielle Schwachstellen in der Kommunikation zu identifizieren und zu beheben.
- Wenn das Medizinprodukt außer Betrieb genommen oder aus dem Verkehr entfernt wird, müssen alle zu schützenden Daten sicher gelöscht oder anderweitig unzugänglich gemacht werden.

Risikomanagement (RM)

Im Risikomanagement sollten folgende Punkte berücksichtigt werden:

- Es muss analysiert werden, welche Folgen eine Überlastung des Systems durch zu viele Anfragen oder Anfragen mit zu großen Datenvolumina (z. B. durch Denial-of-Service-Angriffe) haben kann. Geeignete Maßnahmen zur Abwehr solcher Angriffe müssen implementiert werden.
- Die Konsequenzen eines Netzwerkausfalls oder einer Verschlechterung der Netzqualität müssen untersucht werden. Es ist wichtig, Sicherungsmechanismen zu implementieren, die sicherstellen, dass das Produkt auch bei schlechter Netzqualität ordnungsgemäß funktioniert.
- Eine Analyse der Folgen eines Datenverlusts ist notwendig. Dies umfasst die Identifizierung von Maßnahmen, um den Datenverlust zu verhindern und Wiederherstellungsstrategien (Backup und Restore) zu entwickeln.
- Die häufigsten Schwachstellen und daraus resultierende Bedrohungen sollten identifiziert und Gegenmaßnahmen ergriffen werden. Zusätzlich müssen Risiken durch alle relevanten Angriffsvektoren bewertet werden, um das System gegen verschiedene Angriffsarten abzusichern.

Authentifizierung

Die Authentifizierung ist ein kritischer Bereich, der noch nicht vollständig mit dem externen Anbieter definiert wurde. Es ist wichtig, starke Authentifizierungsmechanismen festzulegen, die den Zugang zu sensiblen Bereichen und Daten des Produkts regeln.

Informationen für die Benutzer

In der Gebrauchsanweisung sollte klar festgelegt werden, welche Aktivitäten die Betreiber durchführen müssen und wie oft dies erfolgen sollte. Diese Punkte sollten regelmäßig überprüft und aktualisiert werden:

- Der Betreiber sollte verpflichtet sein, den Hersteller zeitnah über sicherheitsrelevante Zwischenfälle zu informieren.
- Regelmäßige Sicherheitsupdates und Patches sollten vom Betreiber aufgespielt werden, um das System gegen neue Bedrohungen zu schützen.
- Betreiber sollten angeleitet werden, wie das System kontinuierlich überwacht wird, und regelmäßige Backups sowie Wiederherstellungen (Restore) durchführen, um die Verfügbarkeit der Daten zu gewährleisten.
- Es sollte eine klare Anleitung vorhanden sein, wie das Produkt sicher außer Betrieb genommen wird, inklusive der sicheren Entfernung sensibler Daten und der Deaktivierung aller relevanten Funktionen.

Empfehlungen Vorhersagemodell

Hier sind Empfehlungen, wie der Hersteller die Sicherheit ihrer Produkte und Prozesse weiter steigern kann:

Risikomanagement

Im Risikomanagement sollten folgende Punkte berücksichtigt werden:

- Die Cybersicherheitsrisiken sollten im Bericht separat von anderen Risiken aufgeführt werden
- Es ist erforderlich, zu analysieren, welche Auswirkungen eine Systemüberlastung durch eine hohe Anzahl von Anfragen oder Anfragen mit großen Datenvolumen (z. B. infolge von Denial-of-Service-Angriffen) haben könnte
- Außerdem sollte ein Threat Model erstellt werden

Erweiterung des Testplans um spezifische Sicherheitsmaßnahmen

Um Schwachstellen frühzeitig zu erkennen, sollte der Hersteller einen umfassenden Testplan entwickeln, der fortgeschrittene Sicherheitstests beinhaltet. Dies umfasst:

- Regelmäßige Durchführung von Portscans und Penetrationstests zur Identifizierung und Behebung von Schwachstellen in der Netzwerksicherheit.
- Implementierung von Fuzz-Tests an allen relevanten Datenschnittstellen, die sicherstellen, dass das Produkt auch unter unerwarteten Eingaben oder Angriffen robust bleibt.

- Neben internen Tests sollte der Hersteller regelmäßige eine Überprüfung der Sicherheit gegen die üblichen Angriffsvektoren vorsehen.

Implementierung von Coding-Guidelines und statischer Code-Analyse

Eine formale Definition von Coding-Guidelines sowie die Einführung von Methoden zur statischen Code-Analyse sind entscheidend, um die Qualität und Sicherheit des Codes zu gewährleisten. Der Hersteller sollte:

- Coding-Guidelines etablieren. Diese Richtlinien sollten Best Practices für die sichere Programmierung enthalten, einschließlich Maßnahmen zur Vermeidung häufiger Sicherheitslücken wie unsichere Speicherverwaltung oder fehlende Validierung von Benutzereingaben.
- Statische Code-Analyse-Tools einführen. Durch die Implementierung von Tools zur statischen Code-Analyse kann der Quellcode automatisch auf Sicherheitslücken überprüft werden. Dies ermöglicht es, Schwachstellen frühzeitig zu erkennen und zu beheben, bevor die Software in die Testphase geht.

4 Diskussion

4.1 Anwendbarkeit von Cybersecurity Normen im Medizinprodukte-Bereich

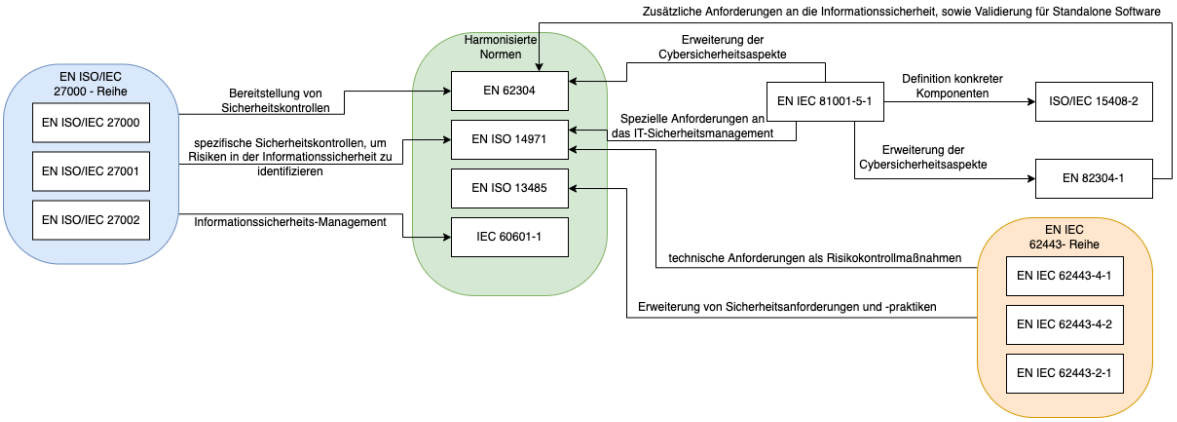

Abbildung 3: Beziehungen der relevanten Normen für Hersteller

Ein zentrales Problem besteht darin, dass es im Bereich der Cybersecurity eine Vielzahl von Normen gibt. Von den zwanzig im Kapitel 3.3.4 aufgeführten Normen sind neben den harmonisierten Normen, die folgenden besonders empfehlenswert:

- EN ISO/IEC 27000 - Reihe, insbesondere die EN ISO/IEC 27002
- EN IEC 62443 - Reihe, insbesondere die EN IEC 62443-4-1
- EN IEC 81001-5-1
- ISO/IEC 15408-2
- EN 82304-1

Der Graph in der Abbildung 3 zeigt, wie die Normen durch gemeinsame Prinzipien wie Qualitätsmanagement, Risikomanagement, Cybersicherheit und Softwareentwicklung miteinander verbunden sind. Jede Norm trägt spezifische Anforderungen bei, die entweder in anderen Normen ergänzt oder weiterentwickelt werden. Die harmonisierten Normen EN ISO 13485, EN ISO 14971, EN 62304 und IEC 60601-1 definieren grundlegende Anforderungen für Medizingeräte, insbesondere im Bereich Software-Lebenszyklus, Risikomanagement und Qualität. Die Normen der EN ISO/IEC 27000-Reihe unterstützen die Sicherheitsanforderungen der harmonisierten Normen, indem sie allgemeine Sicherheitskontrollen bereitstellen, die spezifisch auf Informationssicherheitsrisiken ausgerichtet sind. Die EN IEC 81001-5-1 erweitert die harmonisierten Risikomanagement- und Softwareentwicklungsnormen um Cybersicherheitsaspekte. Dabei kann die ISO/IEC 15408-2 als Hilfe verwendet werden, um konkrete Sicherheitskomponenten zu definieren und deren

Bewertung zu ermöglichen. Die Gesundheitssoftwarenorm EN 82304-1 erweitert die EN 62304 um zusätzliche Anforderungen im Bereich der Informationssicherheit und um die Validierung der Software. Die EN IEC 62443-Reihe ergänzt die harmonisierte EN ISO 13485 um Sicherheitsanforderungen und -praktiken und das Lieferantenmanagement wird um Cybersecurityaspekte erweitert. Außerdem kann mit der Normenreihe spezifische Risiken mir Cybersicherheit adressiert werden. Zusätzlich können die technischen Sicherheitsanforderungen als Risikokontrollmaßnahme implementiert werden.

Weitere Hauptschwierigkeiten liegen darin, dass Normen wie EN 62304, EN IEC 62443 - Reihe, EN ISO 14971, ISO/IEC 27032 oder EN 82304-1 auf eine statische Weise entwickelt werden und sich nur langsam an neue Bedrohungen und Technologien anpassen. In der schnelllebigen Welt der Cybersicherheit, wo Hacker kontinuierlich neue Angriffstechniken entwickeln, hinken Standards und Gesetzgebungen oft hinterher. Zum Beispiel legt die EN 62304 detaillierte Anforderungen an die Softwareentwicklung fest, adressiert aber die Cybersicherheit nur marginal, was die Anwendbarkeit in einem dynamischen Bedrohungsumfeld erschwert.

Die Normen EN IEC 62443-Reihe bieten hingegen einen umfassenden Rahmen für den Schutz industrieller Systeme, der sich auch auf Medizingeräte anwenden lässt. Dennoch erfordert die Implementierung eines Cybersicherheitsmanagementsystems (CSMS) kontinuierliche Verbesserungen und Anpassungen an die sich ändernde Bedrohungslage. Unternehmen stehen vor der Herausforderung, diese Systeme dynamisch zu gestalten, um auf aktuelle Cyberbedrohungen zu reagieren, was Zeit und Ressourcen beansprucht.

Die Normen wie EN 62304, EN ISO 14971 und EN ISO/IEC 27001 definieren zwar Anforderungen an die Entwicklung, das Risikomanagement und die Cybersicherheit von Medizingeräten, sie bieten jedoch nicht immer die Flexibilität, die notwendig ist, um mit den sich ständig ändernden Bedrohungen und Technologien im Bereich der Cybersicherheit Schritt zu halten.

Die ISO/IEC 29147 bietet einen Rahmen für die Offenlegung von Sicherheitslücken in Produkten und Systemen. Sie fordert Hersteller dazu auf, Sicherheitslücken transparent zu dokumentieren und Maßnahmen zur Behebung bereitzustellen. In der Praxis ist diese Norm für Hersteller von Medizingeräten wichtig, da sie es ermöglicht, Schwachstellen zu erkennen und schnell zu beheben, bevor Angreifer diese ausnutzen können. Die Schwierigkeit besteht jedoch darin, dass viele Hersteller veraltete Software verwenden oder nicht über die notwendigen Ressourcen verfügen, um rechtzeitig auf Sicherheitslücken zu reagieren. Die Norm ISO/IEC 30111 ist komplementär zur ISO/IEC 29147 und hat den Vorteil, dass sie eine strukturierte Vorgehensweise zur Schwachstellenanalyse darlegt. Allerdings stößt auch diese Norm an ihre Grenzen, wenn Unternehmen nicht die Ressourcen haben, um zeitnah auf Bedrohungen zu reagieren.

Die Norm EN ISO/IEC 27002 ist aufgrund ihrer Schutzmaßnahmen für Vertraulichkeit, Integrität und Verfügbarkeit von Informationen wichtig für Medizingeräte. Sie unterstützt den Schutz vor unbefugtem Zugriff und Datenverlust. Die Herausforderung besteht darin, dass viele Medizingeräte auf älteren Netzwerken oder Betriebssystemen basieren, was die

Implementierung moderner Sicherheitskontrollen erschwert. Auch die EN ISO/IEC 27001 erfordert umfassende Maßnahmen, die oft schwer auf die spezifischen Anforderungen von Medizingeräten anzupassen sind, da diese Geräte spezifische medizinische Anforderungen haben, die nicht immer mit den allgemeinen IT-Sicherheitsstandards übereinstimmen. Zudem wird die Norm durch die zunehmende Komplexität der Netzwerkanbindung von Geräten herausgefordert, da sie oft nicht für dynamische Bedrohungsumgebungen ausgelegt ist. Die EN ISO/IEC 27000 bietet eine Grundlage, aber keine spezifischen Lösungen für die Cybersicherheitsanforderungen im Gesundheitswesen, insbesondere für vernetzte Medizingeräte.

Die ISO 27799 spezifiziert die Anwendung der EN ISO/IEC 27002 im Gesundheitswesen. Sie ist darauf ausgelegt, medizinische Daten und Systeme vor unbefugtem Zugriff zu schützen. Wie viele andere Normen basiert auch ISO 27799 auf allgemeinen Informationssicherheitskonzepten, die möglicherweise nicht flexibel genug sind, um den schnellen technologischen Wandel und die wachsenden Bedrohungen im Bereich vernetzter Medizingeräte effektiv zu adressieren. Zusätzlich basiert die derzeit gültige ISO 27799 auf einer veralteten Version der EN ISO/IEC 27002.

Die EN IEC 81001-5-1 ist besonders relevant für Hersteller von Medizingeräten, da sie auf die Sicherstellung der Cybersicherheit von Software abzielt, die für medizinische Geräte entscheidend ist. Die Norm fokussiert sich allerdings stark auf Software, während viele Medizingeräte auch hardwareseitige Schwachstellen aufweisen, die nicht durch Software alleine adressiert werden können. Die schnelle Evolution von Bedrohungen erfordert zudem häufigere Aktualisierungen, die über den ursprünglichen Anwendungsbereich der Norm hinausgehen.

Die ISO 81001-1 legt sich stark auf Software-Sicherheitsaspekte, die allerdings oft nur einen Teil der Sicherheitsanforderungen für Medizingeräte darstellen. Zudem erfordert die dynamische Bedrohungslandschaft eine schnellere Anpassung an neue Risiken.

Die ISO/IEC 15408-1 bietet einen international anerkannten Rahmen für die Bewertung von IT-Sicherheit in Informationssystemen. Die Herausforderung liegt darin, dass die Norm statisch ist und einmal zertifizierte Systeme später durch neue Bedrohungen kompromittiert werden könnten, ohne dass eine regelmäßige Neubewertung erfolgt. Die ISO/IEC 15408-2, der zweite Teil, bietet eine strukturierte Methode zur Bewertung der Sicherheitsfunktionen eines Systems, um sicherzustellen, dass es gegen Bedrohungen geschützt ist. Sie bietet zwar eine umfassende Methodik zur Bewertung von Sicherheit, ist jedoch weniger auf die dynamischen Anforderungen von Cybersicherheitsbedrohungen im Gesundheitswesen fokussiert. Zudem ist der Evaluierungsprozess oft langwierig und passt nicht zur schnellen Veränderung von Bedrohungsszenarien. Der Sicherheitsbewertungsprozess sollte durch kontinuierliche Rezertifizierungen und eine bessere Integration von automatisierten Tests verbessert werden, um schnell auf neue Bedrohungen reagieren zu können.

Die IEC 60601-1 ist eine der wichtigsten Normen für die Sicherheit und Leistung von medizinischen elektrischen Geräten. Diese Norm wurde primär für die elektrische Sicherheit

und Leistungsfähigkeit entwickelt und geht nicht auf die modernen Cybersicherheitsrisiken ein, die durch vernetzte Geräte entstehen. Dies führt zu Lücken bei der Abdeckung von Bedrohungen durch Cyberangriffe.

4.2 Identifikation von Verbesserungsmöglichkeiten

Während die bestehenden Normen wie die EN ISO 14971 und EN ISO 13485 wertvolle Rahmenbedingungen für das Risikomanagement und Qualitätsmanagement bieten, könnten sie durch gezielte Erweiterungen in Bezug auf Cybersicherheit verbessert werden. Die Kombination dieser Normen mit spezifischeren Sicherheitsanforderungen aus der EN ISO/IEC 27001 oder der EN IEC 81001-5-1, die IT-Sicherheitsanforderungen über den gesamten Lebenszyklus von Medizingeräten abdeckt, könnte eine umfassendere Sicherheit gewährleisten.

Eine Verbesserung könnte darin bestehen, dass Normen dynamischere Updates und erweiterte Szenarien für Cybersicherheitsrisiken integrieren. Beispielsweise sollte die EN ISO 14971, die traditionell physische und funktionale Risiken betrachtet, explizit Cyberrisiken und Bedrohungsmodelle in ihre Anforderungen integrieren.

Zusätzlich könnte eine engere Integration der EN IEC 62443-Reihe, insbesondere der technischen Anforderungen für die Gerätesicherheit (EN IEC 62443-4-2), in die bestehenden Medizinnormen einen stärkeren Fokus auf spezifische Sicherheitsaspekte bei vernetzten Medizingeräten ermöglichen. Diese Norm behandelt umfassend Themen wie Authentifizierung, Systemintegrität und die Verfügbarkeit von Ressourcen, die für die Cybersicherheit von Medizingeräten essentiell sind.

Um die Cybersicherheit von Medizingeräten zu verbessern, sollten mehrere Änderungen und Ergänzungen in den bestehenden Normen vorgenommen werden:

- **Erweiterung des Risikomanagements um Cyberrisiken:** Normen wie die EN ISO 14971 sollten um spezifische Anforderungen zur Bewertung und Minimierung von Cyberrisiken ergänzt werden. Dies könnte durch die Integration von Bedrohungsmodellen und Szenarien für Angriffe auf vernetzte Geräte erreicht werden.
- **Integration von Cybersicherheitskontrollen über den gesamten Lebenszyklus:** Normen wie EN IEC 81001-5-1 decken bereits den gesamten Lebenszyklus von Gesundheitssoftware ab. Es wäre jedoch notwendig, dies weiter auszubauen und umfassende Post-Market-Cybersicherheitskontrollen zu fordern, um sicherzustellen, dass Geräte auch nach ihrer Inbetriebnahme sicher bleiben.
- **Regelmäßige Überarbeitung und Aktualisierung:** Normen sollten regelmäßig überarbeitet werden, um neue Sicherheitsbedrohungen und technologische Fortschritte zu berücksichtigen. Besonders in Bereichen wie der künstlichen Intelligenz oder der Vernetzung von Medizingeräten müssen Sicherheitsanforderungen angepasst werden.

- **Branchenspezifische Cybersicherheitsvorgaben:** Eine stärkere Fokussierung auf branchenspezifische Anforderungen für das Gesundheitswesen wäre sinnvoll. Die allgemeine Anwendung von Normen wie EN ISO/IEC 27001 kann zwar helfen, grundlegende Sicherheitsmaßnahmen zu etablieren, jedoch sollten spezifische Anforderungen, wie bereits in der ISO 27799, für Medizingeräte integriert werden, um deren Sicherheit in der Praxis besser zu gewährleisten.
- **Flexibilisierung der Sicherheitsanforderungen:** Normen sollten dynamisch gestaltet werden, sodass sie nicht nur auf heutige Bedrohungen reagieren, sondern auch zukunftssicher sind. Dies könnte durch die Einbindung von Echtzeit-Risikoüberwachung und die Nutzung von Künstlicher Intelligenz (KI) zur Bedrohungsanalyse erreicht werden.

4.3 Verantwortlichkeiten und Cybersecurity

Rolle der Hersteller: Cybersicherheit durch Design und kontinuierliche Pflege

Die Hersteller von Medizingeräten tragen die primäre Verantwortung für die Implementierung von Cybersicherheitsmaßnahmen während der Entwicklung und des gesamten Lebenszyklus eines Produkts. Im Rahmen der Normen wie IEC 60601-1, EN 62304 und EN 82304-1 sind sie verpflichtet, Risikomanagementprozesse zu implementieren und Sicherheitskontrollen sowohl in der Entwicklungsphase als auch nach der Markteinführung aufrechtzuerhalten. Sie tragen die Verantwortung, Schwachstellen zu identifizieren, zu bewerten und zu beheben. Die kontinuierliche Bereitstellung von Software-Updates, Sicherheitspatches und Sicherheitsanleitungen für die Endnutzer ist ebenfalls von entscheidender Bedeutung. Hersteller sind verpflichtet, sichere Entwicklungsprozesse zu etablieren, die sicherstellen, dass medizinische Geräte den gängigen Sicherheitsstandards entsprechen und potenzielle Schwachstellen bereits während der Designphase minimiert werden. Dabei wird betont, dass Hersteller Sicherheitsfunktionen wie Verschlüsselung, Sicherheitsprotokolle und regelmäßige Software-Updates in ihre Produkte integrieren müssen, um die Cybersicherheit langfristig zu gewährleisten. [86]

Ein wesentlicher Aspekt der Verantwortung von Herstellern ist die kontinuierliche Überwachung und Aktualisierung der Geräte nach ihrer Einführung auf den Markt. Da Cyberbedrohungen sich ständig weiterentwickeln, reicht es nicht aus, die Geräte einmalig auf Sicherheitslücken zu überprüfen. Hersteller müssen regelmäßige Software-Patches und Sicherheitsupdates bereitstellen, um neu auftretende Bedrohungen abzuwehren. Der Mangel an regelmäßigen Updates ist eine der größten Schwächen im Cybersicherheitsmanagement von Medizingeräten. [34]

Darüber hinaus verwenden viele Hersteller veraltete Software in ihren Geräten, die nicht mit aktuellen Sicherheitsstandards kompatibel ist. Dies stellt eine erhebliche Gefahr für die Patientensicherheit dar, da Angreifer leicht Zugang zu solchen Systemen erhalten können. Hersteller müssen daher sicherstellen, dass sie nicht nur moderne Software

verwenden, sondern auch auf künftige Bedrohungen vorbereitet sind, indem sie dynamische Sicherheitsmaßnahmen integrieren. [4]

Rolle der Gesundheitsdienstleister: Sichere Nutzung und Netzwerkumgebung

Die Gesundheitsdienstleister (HCPs), also Krankenhäuser und Kliniken, tragen eine ebenso wichtige Verantwortung, wenn es um den sicheren Einsatz von Medizingeräten in ihren Netzwerken geht. Gesundheitsdienstleister müssen nicht nur die Geräte selbst sicher einsetzen, sondern auch die Netzwerksicherheit sicherstellen. In der Praxis bedeutet dies, dass die HCPs robuste Sicherheitsprotokolle in ihre IT-Infrastruktur integrieren müssen, um die Medizingeräte vor externen Bedrohungen zu schützen. [78]

Viele vernetzte Medizingeräte sind auf Datenübertragung und Interoperabilität angewiesen, was sie anfälliger für Cyberangriffe macht, wenn die Netzwerksicherheit nicht ausreichend gewährleistet ist. Unsichere Netzwerke oder veraltete Netzwerkprotokolle können dazu führen, dass Angreifer auf die Geräte zugreifen und die Patientendaten manipulieren oder den Betrieb der Geräte beeinträchtigen. Daher müssen HCPs proaktiv handeln, indem sie Firewalls, Zugangskontrollsysteme und regelmäßige Netzwerküberprüfungen implementieren, um Sicherheitslücken zu schließen. [85]

Ein weiteres Problem, ist der Mangel an Schulungen für das medizinische Personal im Umgang mit vernetzten Medizingeräten. Oftmals liegt die Verantwortung für die Sicherheit der Geräte nicht nur bei den IT-Abteilungen, sondern auch beim medizinischen Personal, das die Geräte im täglichen Betrieb verwendet. Das Verständnis für Sicherheitsbedrohungen und die richtigen Verfahren zur Vermeidung von Fehlern (wie etwa Phishing-Angriffen) sind für die Verhinderung von Sicherheitsvorfällen entscheidend. Hier wird empfohlen, dass HCPs regelmäßige Schulungen und Sensibilisierungsprogramme anbieten, um das Personal für potenzielle Sicherheitsrisiken zu schulen. [67]

Rolle der Nutzer: Bewusstsein und korrekte Handhabung

Auch die Endnutzer, zu denen sowohl medizinisches Personal als auch Patienten zählen, spielen eine wichtige Rolle in der Cybersicherheit von Medizingeräten. Die Nutzer müssen nicht nur in der Lage sein, die Geräte korrekt zu bedienen, sondern auch Sicherheitsprotokolle zu befolgen, die vom Hersteller oder den Gesundheitsdienstleistern bereitgestellt werden. Dies umfasst einfache Maßnahmen wie Passwortschutz, die Sicherstellung, dass die Geräte in einer sicheren Umgebung betrieben werden, und die regelmäßige Überprüfung auf Sicherheitswarnungen oder Systemaktualisierungen. [9]

Ein weiteres wichtiges Thema ist die Notwendigkeit einer klaren Kommunikationsstruktur zwischen Herstellern, HCPs und Nutzern. In Fällen, in denen Sicherheitsupdates oder Patches erforderlich sind, müssen die Hersteller sicherstellen, dass diese Informationen den Nutzern rechtzeitig und klar zur Verfügung gestellt werden. Gleichzeitig müssen die Nutzer in der Lage sein, auf Schwachstellen oder Sicherheitsbedrohungen zu reagieren und die entsprechenden Updates zu installieren. Ein Mangel an Kommunikation oder Verständnis

der Sicherheitsanforderungen kann zu kritischen Ausfällen oder Sicherheitsverletzungen führen. [74]

Notwendigkeit eines koordinierten Ansatzes

Die Verantwortung für die Cybersicherheit eines Medizingeräts liegt nicht bei einem Akteur allein. Es müssen Hersteller, Gesundheitsdienstleister und Nutzer gleichermaßen in den Prozess eingebunden sein. Eine klare Verantwortungsaufteilung und kontinuierliche Zusammenarbeit sind der Schlüssel, um auf neue Bedrohungen effektiv zu reagieren und die Sicherheit der Patienten zu gewährleisten. [86]

Die Krisenkommunikation und der schnelle Informationsaustausch zwischen den Akteuren sind entscheidend, um auf Sicherheitsvorfälle zu reagieren und Schäden zu minimieren. Hier wird vorgeschlagen, dass Hersteller regelmäßig Sicherheitsprüfungen durchführen und Gesundheitsdienstleister in Echtzeit über entdeckte Sicherheitslücken informieren. Dies ermöglicht es den HCPs, Sicherheitsmaßnahmen schnell zu implementieren und sicherzustellen, dass die Geräte weiterhin sicher betrieben werden. [85]

Herausforderungen der geteilten Verantwortung

Die geteilte Verantwortung stellt jedoch auch erhebliche Herausforderungen dar. Beispielsweise können Medizingeräte und IT-Systeme während ihres Einsatzes potenziellen Schwachstellen ausgesetzt sein, die erst lange nach ihrer Markteinführung entdeckt werden. In solchen Fällen müssen die Hersteller in der Lage sein, rechtzeitig Updates bereitzustellen und HCPs sollten sicherstellen, dass diese Maßnahmen korrekt implementiert werden. Ein weiteres Problem besteht darin, dass veraltete Geräte (Legacy Devices) oftmals nicht mehr durch aktuelle Sicherheitsupdates geschützt werden können. Hier muss das Risikomanagement sowohl von den Herstellern als auch den Gesundheitsdienstleistern verbessert werden, um potenzielle Sicherheitslücken zu minimieren. [35] [46]

5 Schlussfolgerung

Es wird verdeutlicht, dass die Analyse der regulatorischen Anforderungen eine zentrale Rolle für die Cybersicherheit vernetzter Medizingeräte spielt. Die Untersuchung zeigt, dass Vorgaben wie die MDR und relevante Normen zwar grundlegende Standards für den Schutz sensibler Patientendaten und die funktionale Sicherheit der Geräte bieten, jedoch hinsichtlich ihrer konkreten Umsetzung in einem dynamischen digitalen Umfeld herausfordernd bleiben.

Die Arbeit zeigt, dass die Erfüllung dieser regulatorischen Anforderungen für Hersteller oft komplex und mit erheblichem Aufwand verbunden ist, insbesondere da es eine Vielzahl an Normen gibt, die sich mit dem Thema der Cybersecurity beschäftigen. Von den zwanzig angeführten Normen in dieser Arbeit sind, neben den harmonisierten Normen, die EN ISO/IEC 27002, die EN IEC 62443-4-1, die EN IEC 81001-5-1, ISO/IEC 15408-2 und die EN 82304 als Grundlage für Hersteller zu empfehlen.

Außerdem erfordert die Cybersicherheit von Medizingeräten eine enge Zusammenarbeit zwischen Herstellern, Gesundheitsdienstleistern und Nutzern, um durch sicheres Design, geschützte Netzwerke und geschulte Anwender Bedrohungen wirksam zu begegnen.

Das Temperaturmesssystem erfüllt viele grundlegende Cybersicherheitsanforderungen, darunter Verschlüsselung und regelmäßige Updates. Schwächen bestehen jedoch bei der Authentifizierung, der Überwachung sicherheitsrelevanter Ereignisse und der Isolation von Subsystemen. Das aktuelle Security Level 2 ist ausreichend, könnte jedoch durch gezielte Verbesserungen optimiert werden. Das Vorhersagemodell integriert wichtige Sicherheitsmaßnahmen wie 2-Faktor-Authentifizierung und verschlüsselte Kommunikation. Es fehlen jedoch detaillierte Coding-Guidelines, kontinuierliche Überwachung und umfassende Risikoberichte. Trotz Erreichung von Security Level 3 gibt es weiteres Verbesserungspotenzial zur Erhöhung der Sicherheit.

Literatur

[1] M. Abdur u. a. “Security Issues in the Internet of Things (IoT): A Comprehensive Study”. In: *International Journal Of Advanced Computer Science And Applications* 8.6 (2017). DOI: https://doi.org/10.14569/ijacsa.2017.080650.

[2] *About Dependabot version updates - GitHub Docs*. GitHub Docs. Abgerufen am 2. November 2024, von https://docs.github.com/en/code-security/dependabot/dependabot-version-updates/about-dependabot-version-updates. 2024.

[3] B. Alexander, S. Haseeb und A. Baranchuk. “Are implanted electronic devices hackable?” In: *Trends in Cardiovascular Medicine* 29.8 (2018), S. 476–480. DOI: https://doi.org/10.1016/j.tcm.2018.11.011.

[4] D. Arney u. a. “Biomedical Devices and Systems Security”. In: *Department Of Computer And Information Science, University Of Pennsylvania, Philadelphia, PA, 19104*. 2011.

[5] E. Biasin und E. Kamenjašević. “Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals”. In: *International Cybersecurity Law Review* 3.1 (2022), S. 163–180. DOI: https://doi.org/10.1365/s43439-022-00054-x.

[6] L. Bracciale, P. Loreti und G. Bianchi. “Cybersecurity vulnerability analysis of medical devices purchased by national health services”. In: *Scientific Reports* 13.1 (2023). DOI: https://doi.org/10.1038/s41598-023-45927-1.

[7] C. Brookson u. a. “Definition of Cybersecurity - Gaps and overlaps in standardisation”. In: (2015). DOI: https://doi.org/10.2824/4069.

[8] *BSI-CS-132, Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte*. BSI-Veröffentlichungen zur Cyber-Sicherheit, 2018. URL: https://www.allianz-fuer-cybersicherheit.de/dok/6603528.

[9] AT&T Business. *Medical Device Security Improves Healthcare and Patient Safety*. Abgerufen am 2. November 2024. o. D. URL: https://www.business.att.com/learn/articles/how-medical-device-security-can-improve-patient-safety.html.

[10] M. P. Carello u. a. “A Systematization of Cybersecurity Regulations, Standards and Guidelines for the Healthcare Sector”. In: *arXiv (Cornell University)* (2023). DOI: https://doi.org/10.48550/arxiv.2304.14955.

[11] M. Clarke und K. Martin. “Managing cybersecurity risk in healthcare settings”. In: *Healthcare Management Forum* 37.1 (2023), S. 17–20. DOI: https://doi.org/10.1177/08404704231195804.

[12] M. Cole Harvey u. a. *ASPR TRACIE Technical Assistance Request*. 2022.

[13] SPHINX Consortium und E. Markakis. *D2.1 Advanced Cyber Security threats digest and analysis*. 2019.

[14] *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*. U.S. Department of Health u. a., 2014.

[15] Symantec Corporation. *Symantec Industry Focus: Medical Device Security*. Abgerufen am 2. November 2024. 2016. URL: https://docs.broadcom.com/doc/symc-med-device-security-en.

[16] L. Coventry und D. Branley. "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward". In: *Maturitas* 113 (2018), S. 48–52. DOI: https://doi.org/10.1016/j.maturitas.2018.04.008.

[17] S. Das u. a. "Cybersecurity: The need for data and patient safety with cardiac implantable electronic devices". In: *Heart Rhythm* 18.3 (2020), S. 473–481. DOI: https://doi.org/10.1016/j.hrthm.2020.10.009.

[18] *Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices*. U.S. Department of Health u. a., 2017.

[19] *DRAFT ONR CEN/CLC/TS 18026:2023, Mehrschichtiger Ansatz für einen Anforderungskatalog für Informations-/Cybersicherheitsmaßnahmen für Cloud-Dienste*. Normentwurf. Austrian Standrads International, 2023.

[20] Drägerwerk AG & Co. KGaA. *Wichtiger Sicherheitshinweis! Maßnahme zur Steigerung der Cybersicherheit*. 2022.

[21] *EN 62304:2006 + Cor.:2008 + A1:2015, Medizingeräte-Software – Software-Lebenszyklus-Prozesse*. Deutsch. OVE Österreichischer Verband für Elektrotechnik, 2016.

[22] *EN 62443-2-1:2009 , Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*. Englisch. Normentwurf. OVE Österreichischer Verband für Elektrotechnik, 2009.

[23] *EN 82304-1:2017, Gesundheitssoftware Teil 1: Allgemeine Anforderungen für die Produktsicherheit*. Deutsch. OVE Österreichischer Verband für Elektrotechnik, 2018.

[24] *EN IEC 62443-2-1:2019, Security for industrial automation and control systems Part 2-1: Security program requirements for IACS asset owners*. Englisch. Normentwurf. OVE Österreichischer Verband für Elektrotechnik, 2019.

[25] *EN IEC 62443-4-1:2018, IT-Sicherheit für industrielle Automatisierungssysteme Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung*. Deutsch. OVE Österreichischer Verband für Elektrotechnik, 2018.

[26] *EN IEC 62443-4-2:2019, IT-Sicherheit für industrielle Automatisierungssysteme Teil 4-2: Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme (IACS)*. Deutsch. OVE Österreichischer Verband für Elektrotechnik, 2020.

[27] *EN IEC 80001-1:2021, Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten Teil 1: Sicherheit, Effektivität, Daten- und Systemsicherheit bei Implementierung und Gebrauch von eingebundenen Medizinprodukten oder eingebundener Gesundheitssoftware*. Deutsch. OVE Österreichischer Verband für Elektrotechnik, 2023.

[28] *EN IEC 81001-5-1:2022, Sicherheit, Effektivität und Security. Gesundheitssoftware und Gesundheits-IT-Systeme*. Deutsch. OVE Österreichischer Verband für Elektrotechnik, 2023.

[29] *EN ISO 13485:2016-03 + AC:2018-03 + A11:2021-09, Medizinprodukte — Qualitätsmanagementsysteme — Anforderungen für regulatorische Zwecke*. Deutsch. ÖVE Österreichischer Verband für Elektrotechnik und Austrian Standards International, 2022.

[30] *EN ISO 14971:2019-12 + A11:2021-12, Medizinprodukte — Anwendung des Risikomanagements auf Medizinprodukte*. Deutsch. ÖVE Österreichischer Verband für Elektrotechnik und Austrian Standards International, 2022.

[31] *EN ISO/IEC 27000:2020-02, Information technology — Security techniques — Information security management systems — Overview and vocabulary*. Deutsch. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), 2020.

[32] *EN ISO/IEC 27001:2023-07, Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. Englisch. ÖVE Österreichischer Verband für Elektrotechnik und Austrian Standards International, 2023.

[33] *EN ISO/IEC 27002:2022-11, Information security, cybersecurity and privacy protection — Information security controls*. Englisch. OVE Österreichischer Verband für Elektrotechnik, 2023.

[34] K. Fu und J. Blum. "Controlling for cybersecurity risks of medical device software". In: *Communications Of The ACM* 56.10 (2013), S. 35–37. DOI: `https://doi.org/10.1145/2508701`.

[35] Medical Device Cybersecurity Working Group. *IMDRF/CYBER WG/N70FINAL:2023, Principles and Practices for the Cybersecurity of Legacy Medical Devices*. 2023.

[36] *Guidance for Industry Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software*. 2005.

[37] *Guidance for Industry Wireless Medical Telemetry Risks and Recommendations*. U.S. Department Of Health u. a., 2000.

[38] D. Halperin u. a. "Implantable Electronics Security and Privacy for Implantable Medical Devices". In: *PERVASIVE Computing* (2008), S. 30–31.

[39] *IEC 60601-1:2005 + AMD1:2012 + AMD2:2020 CSV, Medical electrical equipment – Part 1: General requirements for basic safety and essential performance*. Englisch. Consolidated version of the standard including amendments. International Electrotechnical Commission (IEC), 2020.

[40] *IEC TR 60601-4-5:2021, Medizinische elektrische Geräte - Teil 4-5: Leitfaden und Bewertung – Sicherheitsbezogene technische Anforderungen für Security*. International Electrotechnical Commission (IEC), 2023.

[41] *IEC TR 80001-2-8:2016 Edition 1.0, Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2*. International Electrotechnical Commission (IEC), 2016.

[42] *IEC/TR 80001-2-2:2012-07 Edition 1.0, Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls*. International Electrotechnical Commission (IEC), 2012.

[43] *IMDRF/CYBER WG/N60FINAL:2020, Principles and Practices for Medical Device Cybersecurity*. International Medical Device Regulators Forum, 2020. URL: `https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf`.

[44] *IMDRF/CYBER WG/N73FINAL:2023, Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity*. Medical Device Cybersecurity Working Group, 2023.

[45] *ISO 27799:2016, Health informatics — Information security management in health using ISO/IEC 27002*. Englisch. International Organization for Standardization (ISO), 2016.

[46] *ISO 81001-1:2021, Health software and health IT systems safety, effectiveness and security – Part 1: Principles and concepts*. Englisch. International Organization for Standardization (ISO), 2021.

[47] *ISO/IEC 15408-1:2009, Corrected version 2014-01-15, Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*. Englisch. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), 2020.

[48] *ISO/IEC 15408-2:2008, Corrected version 2011-06, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components*. Englisch. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), 2020.

[49] *ISO/IEC 27032:2023, Cybersecurity — Guidelines for Internet security*. Englisch. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), 2023.

[50] *ISO/IEC 29147:2018-10, Information technology — Security techniques — Vulnerability disclosure*. Englisch. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), 2018.

[51] *ISO/IEC 30111:2019, Information technology — Security techniques — Vulnerability handling processes*. Englisch. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), 2019.

[52] *ISO/IEC DIS 15408-1:2023 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*. Englisch. Normentwurf. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), 2024.

[53] *ISO/TR 24971:2020, Medical devices - Guidance on the application of ISO 14971*. International Organization for Standardization (ISO), 2020.

[54] Johner-Institut. *it-security-guideline/Guideline-IT-Security_ DE.md at master · johner-institut/it-security-guideline*. GitHub. 2021. URL: https://github.com/johner-institut/it-security-guideline/blob/master/Guideline-IT-Security_DE.md.

[55] Johnson & Johnson Vision. *Dringender Sicherheitshinweis*. In FSN2021-07. 2021.

[56] J. Kim u. a. "APSec1.0: Innovative Security Protocol Design with Formal Security Analysis for the Artificial Pancreas System". In: *Sensors* 23.12 (2023), S. 5501. DOI: https://doi.org/10.3390/s23125501.

[57] G. Lorenzini, D. M. Shaw und B. S. Elger. "It takes a pirate to know one: ethical hackers for healthcare cybersecurity". In: *BMC Medical Ethics* 23.1 (2022). DOI: https://doi.org/10.1186/s12910-022-00872-y.

[58] T. Mahler u. a. "Know Your Enemy: Characteristics of Cyber-Attacks on Medical Imaging Devices". In: *RSNA Conference 2017*. 2017.

[59] A. L. Martínez, M. G. Pérez und A. Ruiz-Martínez. "A Comprehensive Review of the State-of-the-Art on Security and Privacy Issues in Healthcare". In: *ACM Computing Surveys* 55.12 (2022), S. 1–38. DOI: https://doi.org/10.1145/3571156.

[60] *MDCG 2019-16 Guidance on Cybersecurity for medical devices*. Medical Device Coordination Group, 2019.

[61] Medtronic GmbH. *Dringende Sicherheitsinformation*. In *Insulinpumpe MiniMed^{TM} 508 und Insulinpumpen der Serie MiniMed^{TM} Paradigm^{TM}*. 2023.

[62] J. Nayak u. a. "Extreme learning machine and bayesian optimization-driven intelligent framework for IoMT cyber-attack detection". In: *The Journal Of Supercomputing* 78.13 (2022), S. 14866–14891. DOI: https://doi.org/10.1007/s11227-022-04453-z.

[63] M. Ngamboé u. a. "Risk assessment of cyber-attacks on telemetry-enabled cardiac implantable electronic devices (CIED)". In: *International Journal Of Information Security* 20.4 (2020), S. 621–645. DOI: https://doi.org/10.1007/s10207-020-00522-7.

[64] S. Nifakos u. a. “Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review”. In: *Sensors* 21.15 (2021), S. 5119. DOI: https://doi.org/10.3390/s21155119.

[65] *NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations*. National Institute of Standards und Technology, 2020. DOI: https://doi.org/10.6028/NIST.SP.800-53r5. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[66] *npm-audit | npm Docs*. Abgerufen am 2. November 2024, von https://docs.npmjs.com/cli/v10/commands/npm-audit. Apr. 2024.

[67] R. Piggin. *Cybersecurity of medical devices*. BSI, 2017. URL: https://www.bsigroup.com/LocalFiles/EN-AU/ISO%2013485%20Medical%20Devices/Whitepapers/White_Paper___Cybersecurity_of_medical_devices.pdf.

[68] *Postmarket Management of Cybersecurity in Medical Devices*. U.S. Department of Health u. a., 2016.

[69] X. Qian u. a. “Radiofrequency remote monitor software patch update without cybersecurity implantable cardioverter-defibrillator firmware update increases the risk of inappropriate implantable cardioverter-defibrillator therapies”. In: *HeartRhythm Case Reports* 8.2 (2022), S. 69–72. DOI: https://doi.org/10.1016/j.hrcr.2021.12.016.

[70] *Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)*. EUROPÄISCHES PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION, 2022.

[71] C. Rosenzweig. *IT-Sicherheit im Gesundheitswesen*. Abgerufen am 2. November 2024. Mai 2024. URL: https://www.johner-institut.de/blog/gesundheitswesen/it-sicherheit-im-gesundheitswesen/.

[72] W. Saltzstein. “Bluetooth Wireless Technology Cybersecurity and Diabetes Technology Devices”. In: *Journal Of Diabetes Science And Technology* 14.6 (2019), S. 1111–1115. DOI: https://doi.org/10.1177/1932296819864416.

[73] SOOIL Development Co., Ltd. *Dringende Sicherheitsmitteilung*. 2020.

[74] A. D. Stern u. a. “Cybersecurity features of digital medical devices: an analysis of FDA product summaries”. In: *BMJ Open* 9.6 (2019), e025374. DOI: https://doi.org/10.1136/bmjopen-2018-025374.

[75] I. Stine u. a. “A cyber risk scoring system for medical devices”. In: *International Journal of Critical Infrastructure Protection* 19 (2017), S. 32–46. DOI: https://doi.org/10.1016/j.ijcip.2017.04.001.

[76] M. Theocharidou und I. Lella. *ENISA Threat Landscape Report: Health Sector (January 2021 to March 2023)*. 2023.

[77] N. M. Thomasian und E. Y. Adashi. "Cybersecurity in the Internet of Medical Things". In: *Health Policy And Technology* 10.3 (2021), S. 100549. DOI: https://doi.org/10.1016/j.hlpt.2021.100549.

[78] D. Truxius u. a. *Cyber-Sicherheitsbetrachtung vernetzter Medizinprodukte*. BSI-Projekt 392: Manipulation von Medizinprodukten (ManiMed). 2020. URL: https://www.bsi.bund.de.

[79] P. Upendra. "Selecting a Passive Network Monitoring Solution for Medical Device Cybersecurity Management". In: *Biomedical Instrumentation Technology* 55.4 (2021), S. 121–130. DOI: https://doi.org/10.2345/0890-8205-55.4.121.

[80] *VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)*. EUROPÄISCHES PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION, 2016.

[81] *Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates*. EUROPÄISCHES PARLAMENT UND DES RAT DER EUROPÄISCHEN UNION, 2017.

[82] *Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates vom 5. April 2017 über In-vitro-Diagnostika und zur Aufhebung der Richtlinie 98/79/EG und des Beschlusses 2010/227/EU der Kommission*. EUROPÄISCHES PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION, 2017.

[83] *VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit)*. EUROPÄISCHES PARLAMENT UND EUROPÄISCHE UNION, 2019.

[84] P. Williams und A. Woodward. "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem". In: *Medical Devices: Evidence and Research* (2015), S. 305. DOI: https://doi.org/10.2147/mder.s50048.

[85] A. Wirth. "Cybercrimes Pose Growing Threat to Medical Devices". In: *Biomedical Instrumentation Technology* 45.1 (2011), S. 26–34. DOI: https://doi.org/10.2345/0899-8205-45.1.26.

[86] F. Wu und S. Eagles. "Cybersecurity for Medical Device Manufacturers: Ensuring Safety and Functionality". In: *Biomedical Instrumentation Technology* 50.1 (2016), S. 23–34. DOI: https://doi.org/10.2345/0899-8205-50.1.23.