HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Frau Dipl.-Ing.
Eva Nagamine-Jones

Erstellen eines Leitfadens für die Bewertung von Datensicherheits- und Cybersecurity-Risiken bei Medizinprodukten

Mittweida, 2023

Fakultät Angewandte Computer- und Biowissenschaften

BACHELORARBEIT

Erstellen eines Leitfadens für die Bewertung von Datensicherheits- und Cybersecurity-Risiken bei Medizinprodukten

Autor:
Frau Dipl.-Ing.

Eva Nagamine-Jones

Studiengang:
IT-Forensik/ Cybercrime

Seminargruppe:
CC18w1-B

Erstprüfer:
Prof. Ronny Bodach

Zweitprüfer:
Dipl.-Ing. (FH) Dirk Eisentraut

Einreichung:
Mittweida, 28.07.2023

Verteidigung/Bewertung:
Mittweida, 2023

Faculty Angewandte Computer- und Biowissen-
schaften

BACHELOR THESIS

Creation of a guideline for the assessment of data security and cybersecurity risks in medical devices

author:
Ms. Dipl.-Ing.

Eva Nagamine-Jones

course of studies:
IT-Forensik/ Cybercrime

seminar group:
CC18w1-B

first examiner:
Prof. Ronny Bodach

second examiner:
Dipl.-Ing. (FH) Dirk Eisentraut

submission:
Mittweida, 28.07.2023

defence/ evaluation:
Mittweida, 2023

Bibliografische Beschreibung:

Nagamine-Jones, Eva:
Erstellen eines Leitfadens für die Bewertung von Datensicherheits- und Cybersecurity-Risiken bei Medizinprodukten. - 2023. - 11, 92, 42 S.
Mittweida, Hochschule Mittweida, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2023

Referat:

Diese Arbeit beschäftigt sich mit der Erstellung eines Leitfadens für die Prüfung der Daten- und Cybersicherheitsrisiken für Medizinprodukte. Es werden die rechtlichen Grundlagen der Bewertung und die zugehörigen Empfehlungen dargestellt. Hierzu werden Empfehlungen aus Deutschland, der EU und der USA betrachtet und vergleichen. Die Umsetzung der Prüfung der Daten- und Cybersicherheitsrisiken wird mit Hilfe eines Beispiels erläutert und in der Folge daraus der zur Konformitätsprüfung wünschenswerte Umfang einer Dokumentation ermittelt. Für die Prüfung der technischen Angaben zur Risikobehandlung für Medizinprodukte, entsprechend der Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik, wurde zudem eine Einteilung in Schwierigkeitsgrade der Beurteilung vorgenommen.

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AFAP	As Far As Possible
ALARP	As Low As Reasonably Possible
BSI	Bundesamt für Sicherheit in der Informationstechnik
BZ	Blutzucker
CGM	Continuous Glucose Monitoring
DSGVO	Datenschutz-Grundverordnung
EMC	Electromagnetic Compatibility
ENISA	European Union Agency for Cybersecurity
FDA	Food and Drug Administration
GDNG	Gesetz zur verbesserten Nutzung von Gesundheitsdaten
GTHF	Globale Harmonisierungs-Task-Force
IP	Internet Protocol (Adresse)
JTAG	Joint Test Action Group - Synonym für IEEE-Standard 11491
MAC	Media Access Control
MDCG	Medical Device Coordination Group
MDR	Verordnung 2017/745 des Europäischen Parlamentes und des Rates
MDS2	Manufacturer Disclosure Statement for Medical Device Security
MPAMIV	Medizinprodukte-Anwendemelde- und Informationsverordnung
NEMA	National Electrical Manufacturers Association
NIS2	Richtlinie der Europäischen Union zur Netz- und Informationssicherheit
NIST	National Institute of Standards and Technology
OS	Operating System
SBOM	Software Bill of Materials
TCP	Transmission Control Protocol
UART	Universal Asynchronous Reiceiver and Transmitter
UDI	Unique Device Indentification
USB	Universal Serial Bus
WLAN	Wireless Local Area Network

Danksagung

Mein Dank gilt der SLG Prüf- und Zertifizierungs GmbH, insbesondere Herrn Eisentraut, welcher mir einen Einblick in seine Arbeit gab und mich mit den ihm verfügbaren Informationen unterstützte.

1 Einleitung

Die Bachelorarbeit hat das Ziel, einen Leitfaden zu erstellen, welcher die Beurteilung dokumentierter Lösungen und Nachweise zur Cybersicherheit von Medizinprodukten erleichtert. Die Arbeit soll eine Unterstützung für die Konformitätsbewertung bezüglich der Cybersicherheit sein.

1.1 Aufgabenstellung, Grundlagen und Notwendigkeit

Mit der Verordnung 2017/745 (MDR EU) Anhang I, Kapitel 2, Abs. 17 des Europäischen Parlamentes und des Rates vom 5. April 2017 wurden zusätzliche Anforderungen an Medizinprodukte mit IT-Bauteilen eingeführt.

Damit haben die Hersteller Schutzmaßnahmen für die das Medizinprodukt betreffende Software und des IT-Netzes mittels IT-Sicherheitsmaßnahmen zu treffen.
Die Regelung trat zum 26. Mai 2021 in Kraft und muss mit unterschiedlichen Übergangsfristen, bis spätestens 26.Mai 2024, umgesetzt werden.

Aus dieser im Sinne der Patientensicherheit geänderten Anforderung an den Zertifizierungsprozess hat sich die Aufgabenstellung ergeben, welche mit der SLG Prüf- und Zertifizierungs GmbH als Betreuerin der Bachelorarbeit gemeinsam umgesetzt wird.
Die SLG Prüf- und Zertifizierungs GmbH ist eine nach Verordnung (EU) 2017/745, Kapitel IV benannte Stelle, welche die Konformität von Medizinprodukten bewertet.
Die (EU) 2017/745, Artikel 51 und Anhang VIII bestimmt die Klassifizierung von Medizinprodukten auf Grundlage des Risikoniveaus der Produkte.
Entsprechend der Klassifizierung der Produkte erfolgt die Beteiligung einer Benannten Stelle als Kontrollinstanz, festgelegt in Artikel 52 der Verordnung, Klasse I keine oder nur beschränkte Beteiligung, Klasse IIa und IIb Beteiligung einer Benannten Stelle bis auf Ausnahmen, Klasse III immer mit Beteiligung einer Benannten Stelle.

Eine gute Grundlage für den Prüfprozess erleichtert nicht nur der SLG Prüf- und Zertifizierungs GmbH die Arbeit, sondern unterstützt auch die Umsetzung der Patientensicherheit

bezüglich physischer und nicht physischer Gefährdungen, welche durch Cybersecurity-Angriffe auf das Medizinprodukt entstehen können.

Da Risiken von den Anwendern der Medizinprodukte fern zu halten sind, ist es zunächst notwendig, die relevanten Vorschriften und Empfehlungen bezüglich der Ermittlung des aktuellen Stands der Technik auszuwerten.
Damit ist eine Hilfestellung zur systematischen Erkennung von Gefahrenursachen gegeben.

Schwieriger ist es, die Gefahren bezüglich der Cybersicherheit für ein spezielles Produkt vollumfänglich abzubilden und zu bewerten. Die Einschätzung obliegt dem Hersteller, jedoch hat dieser in seiner zur Prüfung vorzulegenden Dokumentation die notwendigen Informationen und eigenen Einschätzungen dem Prüfinstitut zu überlassen.

Das Prüfinstitut kann nun eine Einschätzung der vom Hersteller getroffenen Schutzmaßnahmen vornehmen und bei Feststellung des Einhaltens der Vorschriften dieses, als Teil der Konformitätsbescheinigung, als erfüllt betrachten.
„Diese Internationale Norm (DIN EN ISO 14971, Anm.d.Verf.) legt einen Prozess für einen Medizinproduktehersteller fest zur Identifizierung der mit Medizinprodukten verbundenen Gefährdungen“ [1]
Sie hat für Medizingeräte den Zweck, Schaden abzuwenden.

Die Risiken entstehen für
- Patienten,
- Anwender,
- weitere Personen,
- sonstige Ausstattungen und die
- Umwelt. [2]

Das Risiko wird aus zwei Faktoren bestimmt:
- Wahrscheinlichkeit des Auftretens eines Schadens
- Auswirkungen dieses Schadens (Schwere)

[1] DIN EN ISO 14971:2013-04 Medizinprodukte – Anwendung des Risikomanagements auf Medizinprodukte; 1 Anwendungsbereich
[2] ebenda; Einleitung

Die Einschätzung des Risikos ist für Medizinprodukte ein komplexer Prozess, da es eine Vielzahl an Beteiligten gibt:

- praktizierende Ärzte
- Dienstleister des Gesundheitswesens
- Behörden
- Industrie
- Patienten
- Öffentlichkeit

Jeder Beteiligte schätzt die Wahrscheinlichkeit und Schwere unterschiedlich ein. [3]
Für die Betrachtung der Sicherheit muss neben dem bestimmungsgemäßen Gebrauch des Medizinprodukts auch die missbräuchliche Nutzung betrachtet werden. Missbräuchliche Nutzung kann zufällig, aber auch vorsätzlich erfolgen.

[3] DIN EN ISO 14971

1.2 Definitionen

Die in dieser Arbeit verwendeten Begriffe wurden in verschiedenen Vorschriften definiert. Die wichtigsten Begriffe werden daher in den folgenden Unterkapiteln aufgeführt.
Für die ISO 14971 wurden einige Begriffe mit der Überarbeitung dieser Vorschrift mit Ausgabe 2019 geändert. Daher wurden die Definitionen aus den Ausgaben 2013 und 2019, erkennbar an der Fußnote, hier zusammengetragen.

1.2.1 Definitionen aus DIN EN ISO 14971, Auszug

Schaden
Verletzung oder Schädigung der Gesundheit von Menschen oder Schädigung von Gütern oder der Umwelt[4]

Gefährdung
potentielle Schadensquelle

Gefährdungssituation
Umstände, unter denen Menschen, Güter oder die Umwelt einer oder mehreren Gefährdungen ausgesetzt sind

Lebenszyklus
Abfolge alle Phasen im Leben eines Medizinprodukts von einer anfänglichen Konzeption bis zur endgültigen Außerbetriebnahme und Entsorgung[5]

Hersteller
natürliche oder juristische Person, die für das Design und/oder die Herstellung eines Medizinprodukts verantwortlich ist in der Absicht, das Medizinprodukt unter ihrem Namen für den Gebrauch bereitzustellen, unabhängig davon, ob dieses Medizinprodukt von dieser Person selbst und/oder in deren Auftrag von (einer) anderen Person(en) entwickelt oder hergestellt worden ist[6]

[4] neu definiert in EN ISO 14971:2019
[5] ebenda
[6] ebenda

Medizinprodukt

Instrument, Apparat, Werkzeug, Maschine, Gerät, Implantat, Reagens für die In-vitro-Anwendung, Software, Material oder anderer gleichartiger oder verwandter Gegenstand, das/der/die vom Hersteller für die Anwendung, alleine oder in Kombination, am Menschen für einen oder mehrere der spezifischen medizinischen Zwecke

- Erkennung, Verhütung, Überwachung, Behandlung oder Linderung einer Krankheit;
- Erkennung, Überwachung, Behandlung, Linderung oder Kompensierung von Verletzungen;
- Untersuchung, Ersatz, Veränderung oder Unterstützung des anatomischen Aufbaus oder eines physiologischen Prozesses;
- Unterstützung oder Erhaltung des Lebens;
- Empfängnisregelung;
- Desinfektion von Medizinprodukten;
- Bereitstellung von Informationen mittels In-vitro-Untersuchung von aus dem menschlichen Körper stammenden Proben;

vorgesehen ist und dessen/deren bestimmungsgemäße Hauptwirkung weder durch pharmakologische, immunologische noch metabolische Mittel, im oder am menschlichen Körper, erreicht wird, dessen/deren Wirkungsweise aber durch solche Mittel unterstützt werden kann.[7]

Verfahren

festgelegte Art und Weise, eine Tätigkeit oder einen Prozess auszuführen

Prozess

Satz zusammenhängender oder sich gegenseitig beeinflussender Tätigkeiten, der Eingaben zum Erzielen eines vorgesehenen Ergebnisses verwendet[8]

Aufzeichnung

Dokument, das erreichte Ergebnisse angibt oder einen Nachweis ausgeführter Tätigkeiten bereitstellt[9]

---

[7] neu definiert in EN ISO 14971:2019
[8] ebenda
[9] ebenda

Risiko

Kombination der Wahrscheinlichkeit des Auftretens eines Schadens und des Schweregrades[10]

Risikoanalyse

systematische Verwendung von verfügbaren Informationen zur Identifizierung von Gefährdungen und Einschätzung des Risikos[11]

Risikobeurteilung

Gesamtheit des Prozesses, der eine Risikoanalyse und eine Risikobewertung umfasst[12]

Risikoeinschätzung

Prozess, in dem der Wahrscheinlichkeit des Auftretens eines Schadens und dem Schweregrad dieses Schadens Werte zugeordnet werden[13]

Risikobewertung

Prozess des Vergleichens des eingeschätzten Risikos mit gegebenen Risikokriterien, um die Akzeptanz des Risikos zu bestimmen[14]

Schweregrad

Maß der möglichen Auswirkungen einer Gefährdung

1.2.2 Definitionen nach BSI (Bundesamt für Sicherheit in der Informationstechnik) IT-Grundschutz-Kompendium, Glossar[15]

Cyber-Sicherheit

Cyber-Sicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der Informationssicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende

[10] neu definiert in EN ISO 14971:2019
[11] ebenda
[12] ebenda
[13] ebenda
[14] ebenda
[15] BSI-Standard 200-3, Risikoanalyse auf der Basis von IT-Grundschutz, www.bsi.bund.de/grundschutz; Abrufdatum 04.06.2023

Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. Häufig wird bei der Betrachtung von Cyber-Sicherheit auch ein spezieller Fokus auf Angriffe aus dem Cyber-Raum gelegt.

Grundwerte der Informationssicherheit

Der IT-Grundschutz betrachtet die drei Grundwerte der Informationssicherheit: Vertraulichkeit, Verfügbarkeit und Integrität.

Jedem Anwendenden des IT-Grundschutzes steht es natürlich frei, bei der Schutzbedarfsfeststellung weitere Grundwerte zu betrachten, wenn dies in seinem oder ihrem individuellen Anwendungsfall hilfreich ist. Weitere generische Oberbegriffe der Informationssicherheit sind zum Beispiel Authentizität, Verbindlichkeit, Zuverlässigkeit und Nichtabstreitbarkeit.

Informationsverbund

Unter einem Informationsverbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund kann dabei als Ausprägung die gesamte Institution oder auch einzelne Bereiche, die durch organisatorische Strukturen (z. B. Abteilungen) oder gemeinsame Geschäftsprozesse bzw. Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen.

Kern-Absicherung

Im Fokus der Kern-Absicherung stehen zunächst die besonders gefährdeten Geschäftsprozesse und Assets.

Netzplan

Ein Netzplan ist eine graphische Übersicht über die Komponenten eines Netzes und ihrer Verbindungen.

Risiko

Risiko wird häufig definiert als die Kombination (also dem Produkt) aus der Häufigkeit, mit der ein Schaden auftritt und dem Ausmaß dieses Schadens. Der Schaden wird häufig als Differenz zwischen einem geplanten und ungeplanten Ergebnis dargestellt. Risiko ist eine spezielle Form der Unsicherheit oder besser Unwägbarkeit. In der ISO wird Risiko auch als das Ergebnis von Unwägbarkeiten auf Zielobjekte definiert. In diesem Sinne wird daher auch von Konsequenzen statt von Schaden gesprochen, wenn Ereignisse anders eintreten

als erwartet. Hierbei kann eine Konsequenz negativ (Schaden) oder positiv (Chance) sein. Die obige Definition hat sich allerdings als gängiger in der Praxis durchgesetzt. Im Unterschied zu „Gefährdung“ umfasst der Begriff „Risiko“ bereits eine Bewertung, inwieweit ein bestimmtes Schadensszenario im jeweils vorliegenden Fall relevant ist.

Risikoanalyse

Als Risikoanalyse wird der komplette Prozess bezeichnet, um Risiken zu beurteilen (identifizieren, einschätzen und bewerten) sowie zu behandeln. Risikoanalyse bezeichnet nach den einschlägigen ISO-Normen ISO 31000 und ISO 27005 nur einen Schritt im Rahmen der Risikobeurteilung, die aus den folgenden Schritten besteht:

- Identifikation von Risiken (Risk Identification)
- Analyse von Risiken (Risk Analysis)
- Evaluation oder Bewertung von Risiken (Risk Evaluation)

Im deutschen Sprachgebrauch hat sich allerdings der Begriff Risikoanalyse für den kompletten Prozess der Risikobeurteilung und Risikobehandlung etabliert. Daher wird auch in den Dokumenten zum IT-Grundschutz weiter der Begriff Risikoanalyse für den umfassenden Prozess benutzt.

Risikobehandlungsplan

Die vollständige Erfüllung der im IT-Grundschutz geforderten Basis- und Standard-Anforderungen und gegebenenfalls die Anforderungen bei erhöhtem Schutzbedarf ist ein hoher Anspruch an jede Institution. In der Praxis lassen sich nicht alle Anforderungen erfüllen, sei es, dass Umstande vorliegen, die eine Erfüllung nicht sinnvoll erscheinen lassen (Neubeschaffung von Informationstechnik, Umzugspläne oder Ähnliches) oder dass eine Anforderung aus organisatorischen oder technischen Rahmenbedingungen nicht möglich ist (IT-System oder Anwendung werden nicht eingesetzt oder Ähnliches). Bestehende Defizite bei der Umsetzung von Sicherheitsmaßnahmen, die aus den Sicherheitsanforderungen resultieren und die damit verbundenen Risiken müssen in Form eines Managementberichtes dokumentiert werden, einschließlich einer Umsetzungsplanung für die weitere Behandlung der bestehen- den Risiken. Der Risikobehandlungsplan sollte eine Beschreibung der geplanten Ressourcen und zeitliche Vorgaben enthalten. Er wird durch Unterschrift der Institutionsleitung genehmigt.

Die einzelnen Anforderungen aus dem Risikobehandlungsplan sollten mindestens einmal pro Jahr überprüft werden. Eine dauerhafte und unbefristete Übernahme von Risiken durch die Institutionsleitung muss vermieden werden, da sich im Bereich der

Informationssicherheit die Risiken in kurzer Zeit verändern können. Eine unbefristete Übernahme von Risiken birgt die Gefahr, dass diese Risiken nur zu einem Stichtag geprüft und bewertet werden und eine erneute Betrachtung ausgeschlossen bleibt.

Risikomanagement

Als Risikomanagement werden alle Aktivitäten mit Bezug auf die strategische und operative Behandlung von Risiken bezeichnet, also alle Tätigkeiten, um Risiken für eine Institution zu identifizieren, zu steuern und zu kontrollieren.

Das strategische Risikomanagement beschreibt die wesentlichen Rahmenbedingungen, wie die Behandlung von Risiken innerhalb einer Institution, die Kultur zum Umgang mit Risiken und die Methodik ausgestaltet sind. Diese Grundsätze für die Behandlung von Risiken innerhalb eines ISMS müssen mit den Rahmenbedingungen des organisationsweiten Risikomanagements übereinstimmen bzw. aufeinander abgestimmt sein.

Die Rahmenbedingungen des operativen Risikomanagements umfassen den Regelprozess aus

- Identifikation von Risiken,
- Einschätzung und Bewertung von Risiken,
- Behandlung von Risiken,
- Überwachung von Risiken und
- Risikokommunikation.

Schaden / Konsequenz

Eine Abweichung von einem erwarteten Ergebnis führt zu einer Konsequenz (häufig „Schaden“ genannt). Hierbei kann es sich grundsätzlich um eine positive oder negative Abweichung handeln.

Eine positive Konsequenz beziehungsweise positiver Schaden im Sinne der Chancen- und Risikoanalyse wird auch als Chance bezeichnet. Meistens werden in der Risikoanalyse jedoch die negativen Konsequenzen, also die Schäden, betrachtet.

Das Ausmaß eines Schadens wird als Schadenshöhe definiert und kann als bezifferbar oder nicht direkt bezifferbar betitelt werden. Die bezifferbaren Schäden können in der Regel mit direkten Aufwänden (z. B. finanzieller Art) dar- gestellt werden. Zu den nicht direkt bezifferbaren Schäden gehören z. B. Imageschäden oder Opportunitätskosten. Bei diesen lässt sich die tatsächliche Schadenshöhe häufig nur vermuten oder schätzen. Alle Angaben werden in der Regel aufgrund von Erfahrungs- oder Branchenwerten in Kategorien klassifiziert.

Schwachstelle (englisch „vulnerability“)

Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.

Standard-Absicherung

Die Standard-Absicherung entspricht im Wesentlichen der klassischen IT-Grundschutz-Vorgehensweise des BSI- Standards 100-2. Mit der Standard-Absicherung kann der oder die ISB die Assets und Prozesse einer Institution sowohl umfassend als auch in der Tiefe absichern.

Strukturanalyse

In einer Strukturanalyse werden die erforderlichen Informationen über den ausgewählten Informationsverbund, die Geschäftsprozesse, Anwendungen, IT-Systeme, Netze, Räume, Gebäude und Verbindungen erfasst und so aufbereitet, dass sie die weiteren Schritte gemäß IT-Grundschutz unterstützen.

Verbindlichkeit

Unter Verbindlichkeit werden die Sicherheitsziele Authentizität und Nichtabstreitbarkeit zusammengefasst. Bei der Übertragung von Informationen bedeutet dies, dass die Informationsquelle ihre Identität bewiesen hat und der Empfang der Nachricht nicht in Abrede gestellt werden kann.

Verfügbarkeit

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendenden stets wie vorgesehen genutzt werden können.

Vertraulichkeit

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

Wert (englisch „asset“)

Werte sind alles, was wichtig für eine Institution ist (Vermögen, Wissen, Gegenstände, Gesundheit).[16]

1.2.3 Definitionen nach Verordnung (EU) 2017/745 des Europäischen Parlamentes und des Rates[17]

Zubehör eines Medizinprodukts

bezeichnet einen Gegenstand der zwar an sich kein Medizinprodukt ist, aber vom Hersteller dazu bestimmt ist, zusammen mit einem oder mehreren bestimmten Medizinprodukten verwendet zu werden, und der speziell dessen / deren Verwendung gemäß seiner / ihrer Zweckbestimmung(en) ermöglicht oder mit dem die medizinische Funktion des Medizinprodukts bzw. der Medizinprodukte im Hinblick auf dessen / deren Zweckbestimmung(en) gezielt und unmittelbar unterstützt werden soll.

aktives Produkt

bezeichnet ein Produkt, dessen Betrieb von einer Energiequelle mit Ausnahme der für diesen Zweck durch den menschlichen Körper oder durch Schwerkraft erzeugten Energie abhängig ist und das mittels Änderung der Dichte oder Umwandlung dieser Energie wirkt. Ein Produkt, das zur Übertragung von Energie, Stoffen oder anderen Elementen zwischen einem aktiven Produkt und dem Patienten eingesetzt wird, ohne dass dabei eine wesentiche Veränderung von Energie, Stoffen oder Parametern eintritt, gilt nicht als aktives Produkt.

Software

gilt ebenfalls als aktives Produkt.

Kompatibilität

bezeichnet die Fähigkeit eines Produkts – einschließlich Software -, bei Verwendung zusammen mit einem oder mehreren anderen Produkten gemäß seiner Zweckbestimmung

a) seine Leistung zu erbringen, ohne dass seine bestimmungsgemäße Leistungsfähigkeit verloren geht oder beeinträchtigt wird, und / oder

[16] BSI-Standard 200-3, Risikoanalyse auf der Basis von IT-Grundschutz
[17] Verordnung (EU) 2017/745 des Europäischen Parlamentes und des Rates; https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32017R0745; Abrufbar: 04.06.2023

b) integriert zu werden und / oder seine Funktion zu erfüllen, ohne dass eine Veränderung oder Anpassung von Teilen der kombinierten Produkte erforderlich ist, und / oder
c) konfliktfrei und ohne Interferenzen oder nachteilige Wirkungen in dieser Kombination verwendet zu werden.

Konformitätsbewertung
bezeichnet das Verfahren, nachdem festgestellt wird, ob die Anforderungen dieser Verordnung an ein Produkt erfüllt worden sind.

Benannte Stelle
bezeichnet eine Konformitätsbewertungsstelle, die gemäß dieser Verordnung benannt wurde.

Scherwiegendes Vorkommnis
Vorkommnis, das direkt oder indirekt eine der nachstehenden Folgen hatte, hätte haben können oder haben könnte:
a) den Tod eines Patienten, Anwenders oder einer anderen Person,
b) die vorübergehende oder dauerhafte schwerwiegende Verschlechterung des Gesundheitszustands eines Patienten, Anwenders oder anderer Personen,
c) eine schwerwiegende Gefahr für die öffentliche Gesundheit.

Schwerwiegende Gefahr für die öffentliche Gesundheit
bezeichnet ein Ereignis, das unmittelbare Risiko des Todes, einer schwerwiegenden Verschlechterung des Gesundheitszustands einer Person oder einer schweren Erkrankung, die sofortige Abhilfemaßnahmen erfordert, bergen könnte, und das eine signifikante Morbidität oder Mortalität bei Menschen verursachen kann oder das für einen bestimmten Ort und eine bestimmte Zeit ungewöhnlich oder unerwartet ist.

Korrekturmaßnahme
bezeichnet eine Maßnahme zur Beseitigung der Ursache eines potentiellen oder vorhandenen Mangels an Konformität oder einer sonstigen unerwünschten Situation.[18]

[18] Verordnung (EU) 2017/745

1.2.4 Weitere Definitionen und Erklärungen

Die Planung der Sicherheit startet sinnvoll mit der Planung des Produktes und umfasst die Betrachtung aller Lebensphasen des Medizinproduktes. Ein früher Start der Sicherheitsplanung ermöglicht eine größere Sicherheit mit geringerem Aufwand, als wenn die notwendigen Sicherheitsmaßnahmen als Änderungen des Produktes im Nachhinein ergänzt werden müssen. Der Lebenszyklus, vgl. Abbildung 1, ermöglicht eine stetige Anpassung des Produktes an neue Erkenntnisse oder Herausforderungen.

Phasen des Lebenszyklus des Medizinproduktes

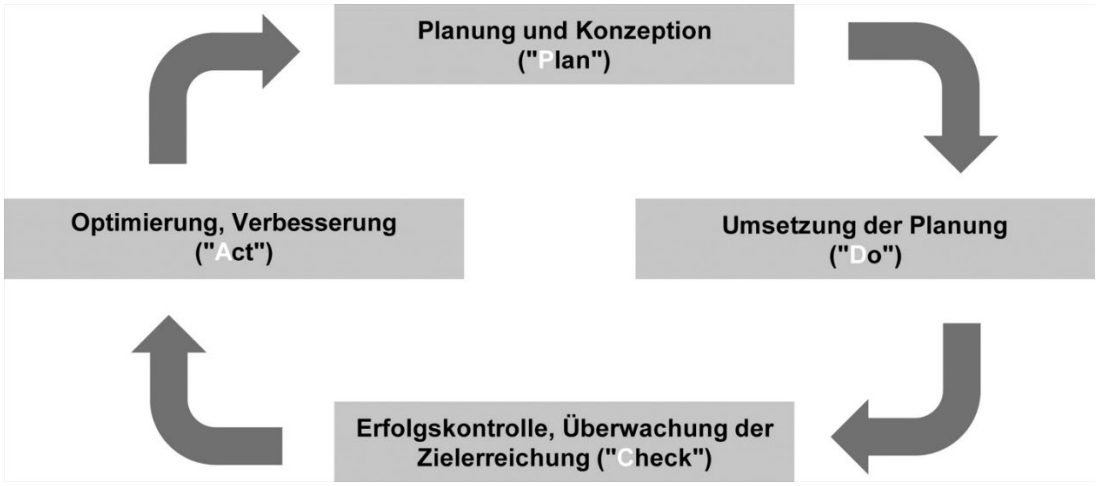

Abbildung 1: Lebenszyklus des Medizinprodukts[19]

Bei Medizinprodukten hatten Hersteller, Aufsichtsbehörden und die Dienstleister des Gesundheitswesens erkannt, dass eine „absolute Sicherheit“ für Medizinprodukte nicht erreicht werden kann. Deshalb muss neben der Risikobewertung auch eine Abwägung von Risiken und Nutzen erfolgen.

Einige Beurteilungen können nur vom qualifizierten medizinischen Praktiker unter Beachtung von Gesundheitszustand und Meinung des Patienten vorgenommen werden.[20] Dies bedeutet, dass bei einem nicht weiter abminderbaren Restrisikos der Behandler über die Anwendung des Medizinproduktes anhand des Einzelfalles die Anwendung entscheidet.

---

[19] BSI-Standard 200-1, Version 1.0, Abbildung 5 (www.bsi-bund.de/grundschutz); Abrufdatum 20.06.2023

[20] DIN EN ISO 14971

Diese Entscheidung basiert auf der Einschätzung von Chancen und Risiken für den jeweiligen Patienten. Dies könnte bei einem Einsatz von computergestützten oder robotergesteuerten Operationssystemen der Fall sein.

Risikomanagement-Prozess

Der Risikomanagement-Prozess ist vom Hersteller für den gesamten Lebenszyklus festzulegen, zu dokumentieren und aufrecht zu erhalten, um die Gefährdungen zu identifizieren, Risiken einzuschätzen und zu bewerten. Die festgestellten Risiken sind zu beherrschen und die Wirksamkeit zu überwachen.
Dafür sind nachfolgende Vorgänge notwendig:

- Risikoanalyse
- Risikobewertung
- Risikobeherrschung
- Informationen aus der Herstellung und den nachgelagerten Phasen.

Es ist eine Risikomanagementakte zu führen.

Der Hersteller muss eine Dokumentation zusammenstellen, die

- bekannte Gefährdungen
- vorhersehbare Gefährdungen

beinhaltet und sowohl

- Normalbedienung als auch
- Fehlbedienung

berücksichtigt.

2 Geltungsbereiche und Normen

Normen, Richtlinien und Empfehlungen haben Geltungsbereiche. Diese kann man in allgemeingültige, ohne geographischen Bezug und solche mit festgelegtem geographischem Bereich unterscheiden.

„DIN-Normen sind das Ergebnis nationaler, europäischer oder internationaler Normungsarbeit. Jeder kann die Erstellung einer Norm beantragen. Normen werden von Ausschüssen bei DIN, bei den europäischen Normungsorganisationen CEN/CENELEC oder bei den internationalen Normungsorganisationen ISO/IEC nach festgelegten Grundsätzen, Verfahrens- und Gestaltungsregeln erarbeitet. Die Verfahrens- und Gestaltungsregeln für die nationale Normung sind in der Normenreihe DIN 820 vom DIN-Normenausschuss Grundlagen der Normungsarbeit (NAGLN) definiert…Die Erarbeitung Europäischer Normen findet auf europäischer Ebene unter dem Dach der Normungsorganisationen CEN, CENELEC und ETSI statt. Bei CEN und CENELEC gilt das nationale Delegationsprinzip. Sogenannte Spiegelgremien erarbeiten in jedem Mitgliedsland die nationale Stellungnahme, in Deutschland bei DIN… Für die Annahme sind eine einfache Mehrheit und mindestens 71 Prozent der gewichteten Stimmen der CEN/CENELEC-Mitglieder nötig… Nach einem positiven Abstimmungsergebnis wird eine Europäische Norm formal ratifiziert. Sie muss danach von den nationalen Normungsorganisationen unverändert als nationale Norm übernommen werden. Abweichende nationale Normen sind zurückzuziehen. Jede angenommene Europäische Norm wird in Deutschland mit einem nationalen Vorwort als DIN-EN-Norm veröffentlicht. Auf internationaler Ebene erarbeitete Normen können durch parallele Erarbeitungs- und Abstimmverfahren gleichzeitig auch als Europäische Norm eingeführt werden und werden damit automatisch von den nationalen Normungsorganisationen übernommen.“[21]

Für diese Ausarbeitung wurden allgemeingültige Normen, Normen und Empfehlungen mit Geltungsbereich Europäische Union, United States of America und Empfehlungen deutscher Behörden betrachtet.
Diese Auswahl wurde getroffen, weil die Benannte Stelle ihren Sitz in Deutschland hat, aber Konformitätsbescheinigungen bezüglich des geltenden Rechts der EU ausgestellt werden.

Die Normen und Empfehlungen bezüglich des US-Amerikanischen Raumes wurden aus dem Grunde mit einbezogen, da Hersteller mitunter bereits eine Zulassung in diesem

[21] https://www.din.de/de/ueber-normen-und-standards/din-norm; Abrufdatum: 04.07.2023

Rechtsraum erlangt haben, deren Normen teilweise in ihrer Ausführung detaillierter sind. Es gibt augenscheinlich deutliche Bemühungen der Behörden (FDA – Food and Drug Administration), eine Standardisierung der Mindestanforderungen an einzureichende Unterlagen für den Zulassungsprozess, insbesondere auch bezüglich der Cybersicherheit, voran zu bringen. Wahrscheinlich wird noch in 2023 eine Richtlinie dazu veröffentlicht werden.[22]
Die FDA hat aktiv an der Entwicklung international harmonisierter Dokumente teilgenommen, einschließlich der Entwicklung einer Richtlinie der Globalen Harmonisierungs-Task Force (GHTF) „Implementierung der Risikobehandlungsprinzipien und Aktivitäten innerhalb eines Qualitätsmanagementsystems“, welches zu einer Integration der Risikobehandlung in das Qualitätsmanagementsystem zur Folge hatte.[23]
Die FDA bringt sich auch aktiv in den globalen Harmonisierungsprozess ein, so dass auch deshalb Neurungen und Hinweise von dieser Seite zu erwarten sind.
Damit hätten Hersteller und benannte Stellen schon etwas wie einen Stand der Technik, an welchen sich Hersteller und benannte Stellen bei Entwicklung, Zulassung und Betreuung nach Markteinführung halten könnten.
Diese Entwicklungen im Auge zu behalten, wäre auf jeden Fall lohnenswert.

2.1 Normen und Empfehlungen ohne territorialen Bezug

Mit Normen ohne territorialen Bezug sind hier Normen bezeichnet, welche zu den internationalen Standards gehören und sowohl in der Europäischen Union als auch im US-Amerikanischen Raum und anderen Gebieten der Welt Anwendung finden.
Hierzu zählen im Wesentlichen die ISO-Standards, welche von der International Organization for Standardization herausgegeben werden. In dieser Organisation sind mit Stand September 2022 167 Länder vertreten.[24]
Insbesondere die ISO EN 14971 zählt zu diesen Normen.

[22] https://www.federalregister.gov/documents/2022/04/08/2022-07614/cybersecurity-in-medical-devices-quality-system-considerations-and-content-of-premarket-submissions; Abrufdatum 04.07.2023
[23] https://www.meddeviceonline.com/doc/the-intersection-of-iso-and-iso-under-the-proposed-fda-qmsr-0001; Abrufdatum: 04.07.2023
[24] https://de.wikipedia.org/wiki/Internationale_Organisation_f%C3%BCr_Normung; Abrufdatum 04.07.2023

2.2 Normen und Empfehlungen mit territorialem Bezug

Zu diesen Normen zählen beispielsweise die Vorschriften der

- Europäischen Union, wie die Verordnung (EU) 2017/745 (MDR),
- Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder
- Food and Drug Administration (FDA) für die USA.

2.3 Graphische Übersicht

In der erstellten Übersicht werden einige betrachtete Normen und Empfehlungen bezüglich ihrer Geltungsbereiche aufgeführt.
Die Übersicht, Abbildung 2, ist nicht vollständig, da Medizinprodukte aus sehr vielen, sehr unterschiedlichen Komponenten bestehen können, für welche es spezielle Normen geben kann. Die für die Bewertung der Cybersicherheit wichtigsten Normen werden dargestellt.

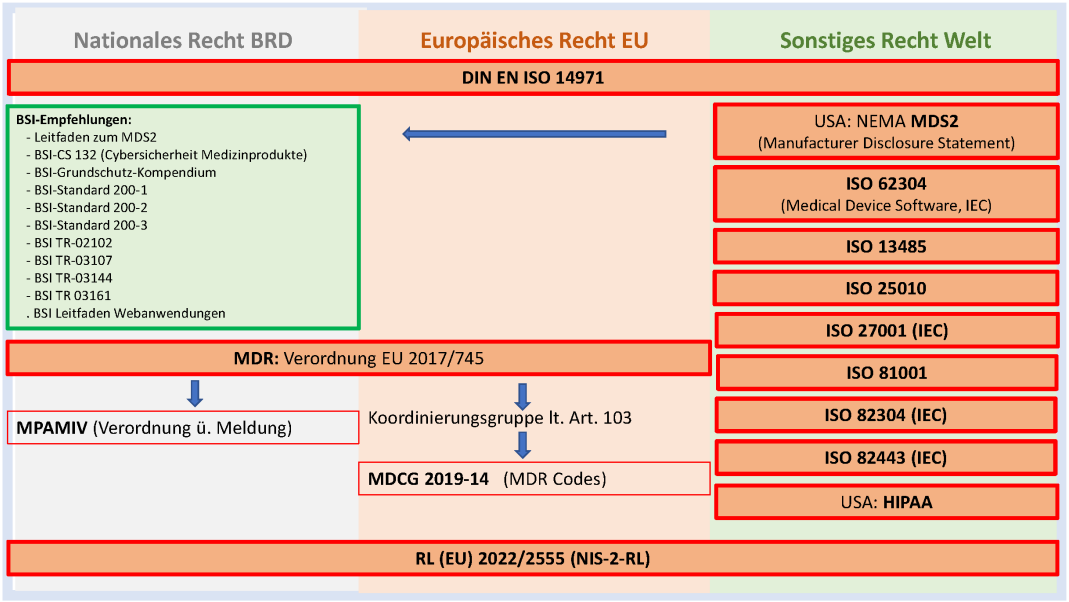

Abbildung 2: Standards und Empfehlungen mit zugehörigem territorialem Bezug

3 Technische Dokumentation

Der technischen Dokumentation des Medizinprodukts kommt eine besondere Bedeutung zu. Sie ist die Voraussetzung für einen sicheren Einsatz des Produktes, der sicheren Installation und Konfiguration, wie auch für die sichere Eingliederung des Produktes in seine Einsatzumgebung.
Darüber hinaus spielt die Dokumentation eine wichtige Rolle für die Überprüfung der Konformitätserklärung des Medizinprodukts.
Die Dokumentation wird in der Verordnung (EU) 2017/745 Anhang II „TECHNISCHE DOKUMENTATION“ und Anhang III „TECHNISCHE DOKUMENTATION ÜBER DIE ÜBERWACHUNG NACH DEM INVERKEHRBRINGEN“ festgelegt.

Das BSI hat in seiner Empfehlung zu den Anforderungen an netzwerkfähige Medizinprodukte Prüffragen zusammengestellt, deren Beantwortung eine wichtige Orientierungshilfe für die cybersicherheitstechnische Bewertung des Produktes bietet.[25]

Damit sollte die Dokumentation des Herstellers auf das Vorhandensein und die Erfüllung der folgenden Punkte geprüft werden:

- Verständliche Dokumentation für IT-Kräfte der Anwender zur sicheren Anwendung des Gerätes
- Benennung von Zielgruppen, welche technische Informationen bzgl. Cybersicherheit erhalten sollten
- Ausreichende Informationen, um ein IT-Sicherheitskonzept kundenseitig zu erstellen:
  - Dokumentation sämtlicher
    - Schnittstellen
    - Zugänge
    - Funktionen
  - Beschreibung der Cyber-Sicherheitsfunktionen der Komponenten
  - Beschreibung, welche Risiken / Bedrohungen durch die jeweilige Komponente selbst abgedeckt sind
  - Dokumentation, welche Bedrohungen im Cyber-Sicherheitsmanagement und -bewertung zu beachten sind

[25] BSI-CS 132; Version 1.0 vom 02.05.2018; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/CS-E-132_Medizinprodukte.pdf; Abrufdatum: 20.05.2023

  - Dokumentation, wie den Bedrohungen entgegengewirkt werden soll
  - Dokumentation, welche Dienste nicht abgesichert werden konnten und ergänzender technische oder organisatorische Cybersicherheitsmaßnahmen bedürfen
- Empfehlungen für eine sichere Konfiguration (Systemhärtung)
  - Hinweise zur Änderung von Standard-Passwörtern, Deaktivierung unnötiger Accounts
  - Checkliste zur Konfiguration und cyber-sicherheitstechnische Implikation, Hinweise zu Cyber-Sicherheitsauswirkungen der einzelnen Optionen oder Alternativen, mit Hinweis, welche Einstellungen als kritisch einzustufen sind
  - Referenzen für weiterführende Information und zum sicheren Betrieb

Zur Umsetzung dieser Empfehlungen wird von der Expertengruppe CyberMed, Allianz für Cyber-Sicherheit, die vermehrte Anwendung des Fragebogens: „Sicherheit von Medizinprodukten – Leitfaden zur Nutzung des MDS2 aus 2019“ empfohlen.
Mit der zunehmenden Anwendung des Fragebogens sollen die Informationen der Hersteller zu (cyber-)sicherheitsrelevanten Merkmalen strukturierter und vergleichbarer werden.
Der Fragebogen beinhaltet auch Informationen zum Schutz von sensiblen Daten und soll den Hersteller bei der Erfüllung anwendbarer Standards und regulatorischer Vorgaben unterstützen. [26]
Dieser Fragebogen soll eine umfangreiche, standardisierte Informations- und Kommunikationsgrundlage bilden und wird daher durch den Expertenkreis empfohlen. Er soll als Unterstützung verstanden werden.
Nach Meinung des Expertenkreises können die Hersteller mit der Anwendung des MDS2 deutlich machen, dass sie Transparenz gewährleisten und sichere Lösungen nach Industriestandards entwickeln, da sie alle notwendigen Informationen teilen.
Das MDS2 entstand aus der Überarbeitung des US-amerikanischen Standards HN 1-2008 und wurde von der NEMA (National Electrical Manufacturers Association) veröffentlicht.
Die NEMA stellt auf ihren Internetseiten als Hilfe eine ausfüllbare, englischsprachige Version dieses Fragebogens zur Verfügung.

Da keine Veröffentlichung des Fragebogens in gleichartig ausfüllbarer Form in deutscher Sprache gefunden werden konnte, wird eine Version des Fragebogens in Form einer Excel-Tabelle als Datei und in Form einer gedruckten Version, ist als Anlage, Teil 1 angefühgt.

---

[26] Expertenkreis CyberMed, Leitfaden zur Nutzung des MDS2 aus 2019, 1 Präambel; https://www.bsi.bund.de/SharedDocs/Downloads/Webs/ACS/DE/downloads/Expertenkreis_CyberMed_MDS2.pdf; Abrufdatum: 20.05.2023

4 Empfehlungen des BSI für sicheres Design

Die Empfehlungen des BSI[27] wurden in Zusammenarbeit mit dem ZVEI-Fachverband Elektromedizinische Technik und dem Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) erstellt.
Es handelt sich hierbei um Empfehlungen, ohne Gesetzescharakter. Bei der Sicherheitsbewertung von Medizinprodukten ist jedoch eine maximal mögliche Verringerung des Gefährdungsrisikos verlangt, wie auch der Einsatz des aktuellen Standes der Technik, um diesen zu erreichen.
In diesem Zusammenhang kann davon ausgegangen werden, dass die Empfehlungen den zum Zeitpunkt der Veröffentlichung aktuellen Stand der Technik darstellen und damit im Regelfalle diese Anwendung finden sollen.
Diese Empfehlungen bieten eine gute Übersicht zu gefährdeten Komponenten und Prozessen, sie wurden daher in die Grundlagen der Bewertung der Cybersicherheitsrisiken einbezogen. Damit sind sie eine wesentliche Hilfestellung zur Umsetzung der europäischen Normen, insbesondere der Verordnung (EU) 2017/745, welche die Regeln für das Inverkehrbringen, Bereitstellung und Inbetriebnahme von Medizinprodukten und deren Zubehör in der Europäischen Union festlegt. In dieser Verordnung werden die Grundanforderungen nur relativ kurz benannt, was deren Umsetzung nicht exakt festlegt.

In vorstehender Verordnung wurde in Artikel 103 das Einsetzen einer „Koordinierungsgruppe Medizinprodukte“ veranlasst. Diese hat u.a. die Entwicklung von Leitlinien für die wirksame und harmonisierte Durchführung dieser Verordnung zur Aufgabe. In Erfüllung dieser Aufgabe wurde durch diese Koordinierungsgruppe (Medical Device Coordination Group MDCG) das Dokument MDCG 2019-14 Explanatory note on MDR codes im Dezember 2019 herausgegeben. Dieses Dokument legt die Grundlage für die Einordnung von Medizinprodukten und bildet auch die Basis für den Zulassungsbereich der Benannten Stellen. Auch dieses Dokument ist keine praktische Hilfe für die Einschätzung von Cybersicherheits-Risiken von Medizinprodukte, sondern setzt administrative Rahmenbedingungen.

Eine Empfehlung des BSI ist die vermehrte Anwendung des MDS2 (Manufacturer Disclosure Statement for Medical Device Security), um Schwachstellen und Risiken von vernetzten Medizingeräten schneller zu identifizieren.

[27] BSI-CS 132; Version 1.0 vom 02.05.2018; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/CS-E-132_Medizinprodukte.pdf

Die Anwendung ist freiwillig, jedoch verbindlich für die Teilnahme am Beschaffungsprozess vieler Krankenhäuser des amerikanischen Marktes.
Somit stehen für den Rechtsraum der Europäischen Union derzeit nur die Rahmenbedingungen, bzw. Anforderungen, fest. Die Empfehlungen des BSI bilden daher eine gute Arbeitsgrundlage für die Umsetzungen der Anforderungen aus den Verordnungen der EU bezüglich der Cybersicherheit.

4.1 Betriebsarten

Unterscheidung folgender Betriebsarten kann getroffen werden:
- Medizinischer Betrieb nach Zweckbestimmung
- Konfiguration des Produktes
- Technischer Servicebetrieb

Oft sind diese nicht voneinander trennbar, daher gelten die Empfehlungen für alle Betriebsarten.

4.2 Umsetzung des Standes der Technik und Grenzen

Wenn nicht alle nach dem Stand der Technik möglichen Vorkehrungen aufgrund des Einflusses auf den Patienten möglich sind, dann muss gut begründet eine Alternativmaßnahme getroffen werden. Sie dürfen keinen störenden Einfluss auf die Safety-Funktionen der Geräte und damit auf das Leben der Patienten haben.

4.3 Entwicklungsschritte und Lebenszyklus des Produkts (Product Lifecycle)

Das BSI hat die Betrachtung unterschiedlicher Phasen eines Lebenszyklus für Produkte etabliert, um dazu passend gezielte Maßnahmen zu empfehlen.

4.3.1 Allgemeine Empfehlungen zur Entwicklung

Empfohlen wird das Etablieren eines sicheren Entwicklungszyklus (Secure Software Development Lifecycle) zur Verbesserung der Sicherheit.

Folgende Fragestellungen sollten Beachtung finden: [28]

- einheitliche, verbindliche, dem aktuellen Stand der Technik entsprechende Vorgaben zur Implementierung (Development Policies) z.B.:
  - Auswahl und Einrichtung vertrauenswürdiger Werkzeuge
  - Trennung von Software-Units
  - sichere Programmiertechniken und -werkzeuge
- Durchführung von Cyber-Sicherheitsanalysen zu Bedrohungen und Risiken
  - an Systemgrenzen
  - der Zweckbestimmung
  - der vorgesehenen Betriebsumgebung
- Verbindliche Prüfabschnitte (Security Gates) z.B: mit Review der Software bzw. ganzheitliche Cybersicherheitsbetrachtung
- sind automatisierte Codeanalysen fester Bestandteildes Entwicklungszyklus
- gezielte Suche nach bekannten Schwachstellen während des gesamten Entwicklungsprozesses alles Softwarekomponenten, wie buffer overflow, unhandled exceptions? Welche flankierenden Maßnahmen verhindern, dass beispielsweise innerhalb von unvorgesehenen Speicherbereichen Code ausgeführt wird?
- Wurde für das Produkt eine technische Sicherheitsanalyse (Penetrationstest) unterzogen? Wurde nach unbekannten Verwundbarkeiten oder alternativen Zugriffsmöglichkeiten gesucht, beispielsweise Auslesen und Analysieren von gespeicherten Daten?
- abschließende Reinigung des entwickelten Produkts von Testcode oder undokumentierten (nicht erforderlichen) Zugängen
- Etablierung von Prozessen (Routinen) für Behandlung von Schwachstellen von Betriebssystem, Drittkomponenten, Eigenentwicklungen
  - Bewertung und ihrer Auswirkung auf das Produkt
  - Festlegung Gegenmaßnahme
  - Behebung Schwachstelle
- welche Cybersicherheitsmechanismen gibt es? (Whitelisting, Antivirensysteme, …) Wurden diese ab Entwicklungsbeginn eingebunden?
- wie ist die Regelung zum Umgang mit Schwachstellen? Welche Reaktionszeiten und Notfallprozeduren gibt es? (siehe auch BSI-Empfehlung „Handhabung von Schwachstellen“)
- ist ein hinreichend langer Zeitraum für Updates, Patches vorgesehen und wie kundenfreundlich ist dieses für die Anwender?

[28] BSI-CS 132; Version 1.

- Werden Updates, Patches etc. vor Bereitstellung ausreichend getestet und die korrekte Funktion des Gerätes gesichert?
- Wie werden Updates, Patches etc. ausgeliefert und wie sicher ist die Auslieferungskette? (Portal auf Cybersicherheit getestet?)
- Werden Logdaten erhoben, analysiert und wurden notwendige Maßnahmen für irreguläre Einträge vorgesehen?

4.3.2 Korrektive Maßnahmen im Lifecycle

Die Hersteller sind gemäß Verordnung (EU) 2017/745 Artikel 87 zur Meldung von schwerwiegenden Vorkommnissen und Sicherheitskorrekturmaßnahmen verpflichtet.
Die Verpflichtung zu entsprechenden Korrekturmaßnahmen ergibt sich aus Artikel 10, Abs. 12 der Verordnung.
Die dafür zu schaffenden Voraussetzungen werden in o.g. Verordnung und für Deutschland in der MPAMIV[29] festgelegt.

Sie sind daher zu einer Überwachung nach Inverkehrbringung verpflichtet, die gebotenen korrektiven Maßnahmen durchzuführen und diese gegenüber ihren Anwendern mittels einer Maßnahmenempfehlung nachvollziehbar und effektiv mitzuteilen.

Dazu braucht es:
- offene Kommunikation bezüglich Cybersicherheit – wie wurde diese implementiert?
- definierte Prozesse der Kommunikation mit Drittanbietern bei Schwachstellen in deren Produkten,
- Ansprechpartner / Kontaktmöglichkeiten bzgl. Cybersicherheit,
- Erkennungsprozesse für potentielle Vorkommnisse im Bereich der Cybersicherheit und zugehörige Meldewege,
- Erkennungsprozesse für tatsächliche Vorkommnisse im Bereich der Cybersicheheit, Meldung und Bewertung gegenüber der zuständigen Behörde

[29] Verordnung über die Meldung von mutmaßlichen schwerwiegenden Vorkommnissen bei Medizinprodukten sowie zum Informationsaustausch der zuständigen Behörden (Medizinprodukte-Anwendermelde- und Informationsverordnung – MPAMIV), Ausfertigung vom 21.04.2021; https://www.gesetze-im-internet.de/mpamiv/MPAMIV.pdf, Abrufdatum 05.06.2023

- konsolidiertes Trackingsystem zur Zusammenführung von Hinweisen aus unterschiedlichen Kommunikationskanälen zu meldepflichtigen Ereignissen und sonstigen, auch potentiellen Vorfällen aus dem Bereich der Cybersicherheit,
- Information der Kunden über die Kritikalität jeweiliger Patches.

4.3.3 Empfehlungen für netzwerkfähige Medizinprodukte

Das BSI hat in der Veröffentlichung zu Cyber-Sicherheitsanforderungen für netzwerkfähige Medizinprodukte für alle Betriebsarten konkrete Empfehlungen verfasst, welche als Hinweise auf zu überprüfende Eigenschaften und Angaben der Dokumentation betrachtet werden können.

Für alle Betriebsarten:[30]

a. Identifizierung
   i. Dokumentation aller Schnittstellen
   ii. Bestimmung des maximal möglichen Schadens, der durch Angriffe auf diese Schnittstelle entstehen kann

b. Klärung der Fragen
   i. Welche Schnittstellen gibt es und was passiert, wenn unerwartete Signale auf diese gegeben werden?
   ii. Welche anderen Komponenten sind anschließbar und was kann dadurch passieren?
   iii. Wie werden die Komponenten angeschlossen (physischer Verbindungstyp) und welches Risiko geht von dieser Technologie aus?
   iv. In welche Richtung geht der Signalfluss/ Datenfluss und kann dieser auch in eine andere Richtung gehen?
   v. Welche Daten / Signale fließen, können sie geändert, gelöscht oder zugefügt werden, wie sind sie vor Zugriff Unberechtigter geschützt?
   vi. Welche Risiken können daraus für die Beteiligten erwachsen, sind diese im akzeptablen Bereich oder braucht es risikomindernde Maßnahmen?

c. Cybersicherheitsspezifische Produkteigenschaften zur Minderung der zuvor identifizierten Gefahren

[30] BSI-CS-E 132; Version 1.

i. Schutz von Daten und Signalen
   1. Ist eine Systemhärtung des Betriebssystems und aller Anwendungen erfolgt? Sind für den Betrieb nicht benötigte Anwendungen abgeschaltet oder wird der Anwender auf eine Abschaltung hingewiesen? Werden sichere Protokollalternativen verwendet (z.B: https statt http)?
   2. Werden nach Stand der Technik nur absicherbare Technologien verwendet?
   3. Wurde die Implementierung der grundlegenden Kommunikationsprotokolle einer Testung auf Toleranz und Robustheit unterzogen?
   4. Standardimplementierung oder Eigenentwicklung von Diensten und Protokollen?
   5. Sensible Daten geschützt gespeichert und übertragen?
      a. Standardimplementierung und anerkannte Algorithmen der Kryptographie oder Eigenentwicklung?
      b. Wird die Vorschrift TR-02102 des BSI zu Kryptoverfahren eingehalten?
      c. Sind Integritätschecks bzgl. sicherheitsrelevanter Daten vorhanden?
      d. Sind die Schnittstellen mit Eingabevalidierung ausgestattet (Verhinderung Manipulation)?
   6. Kann das Netzwerk gehärtet betrieben werden?
      a. Segmentierung des Netzwerks vorhanden oder Hinweise dazu für den Anwender? Ist eine Trennung der Konfigurationsdaten vom medizinischen Betrieb vorhanden?
      b. Abschalten von nicht benötigten Diensten und Technologien möglich, wenn diese vom Anwender nicht benötigt werden?
      c. Wurden Dienste und Technologien nach Stand der Technik bestmöglich gehärtet oder sind Hinweise zur Umsetzung für den Anwender vorhanden?
   7. Client-Server-Betrieb abgesichert?
      a. Werden die Parameter für die Cybersicherheit (wie Cookies) serverseitig berechnet und geprüft?
      b. Werden alle Eingaben des Clients serverseitig validiert?
   8. feingranulare Zugriffskontrolle (Login/ Authentifizierung) zum Schutz sensibler Daten vorhanden und ist die Benutzerverwaltung hinreichend?
      a. Zugangsdaten (z.B. Passwörter) kryptografisch gespeichert?
      b. Bei fehlerhaftem Login eine Fehlermeldung, welche keinen Hinweis auf die Art des Fehlers des Logins ermöglicht (z.B. kein Hinweis, dass Passwort oder Anmeldename falsch)
      c. kann der Netzwerkzugriff auf bestimmte MAC-Adressen, IP-Adressen oder Adressbereiche beschränkt werden?

   d. ergänzende Maßnahmen zur Absicherung eines Zugriffs
   e. Welche Software oder Prozesse laufen mit System-Privilegien und wie sind diese geschützt?
9. Gibt es für Mehrnutzeranwendung ein abgesichertes Session-Management?
   a. Verhinderung der Ausführung kritischer Aktionen ohne die dazu notwendigen Rechte?
   b. Sessions untereinander geschützt?
   c. Gibt es ein Timeout (Abbruchzeitpunkt) der Sessions und ist dieser konfigurierbar?
   d. Kann ein Angriff auf die Verfügbarkeit, welcher durch zu viele offene Verbindungen realisiert werden könnte, mit entsprechenden Vorkehrungen verhindert oder mindestens erschwert werden?
10. Sonstige Cybersicherheitsfunktionen:
   a. Erkennung und Schutz vor Schadprogrammen notwendig und möglich?
   b. Denial-of-Service: bleibt Funktionalität erhalten und wird der normale Betrieb automatisch wieder aufgenommen?
   c. Update-Mechanismen (Firmware) ausreichend abgesichert? Integritätsprüfung über Prüfsumme, Authentifizierung und Absicherung über Signaturen?
   d. Standardverfahren oder nutzerfreundliche Mechanismen für Backups und Wiederherstellung vorhanden?
11. Cybersicherheit zur Erkennung von Angriffen
   a. Logging
      i. Logdaten kritischer Aktionen (geänderte Konfiguration, fehlerhafte Logins, Konnektierung und Trennung von Speichern oder USB-Geräten etc.)?
      ii. Wird ein Zugriff auf geschützte Daten über die Logdaten verhindert?
   b. Auswertung der Logdaten
      i. Möglichkeit automatisierter Alarmierung bei kritischen Ereignissen vorhanden?
      ii. Warnmeldung bei Brute-Force-Angriff auf den Login-Prozess vorhanden?

Für die Konfiguration:

- Konfiguration nur nach vorheriger Authentifizierung
- sichere Standardkonfiguration bei Auslieferung
- Passwörter, Zertifikate für alle Dienste austauschbar
- geschützte Konfiguration gegen unautorisierte Manipulation (Prüfsumme, Signatur)

- Bei Standard-IT für Konfiguration:
  - ausreichend abgesichert?
  - Empfehlungen und technische Richtlinien sauber implementiert?
  - Bei Verwendung einer Weboberfläche ausschließlich verschlüsselte Verbindung
  - Einhaltung der technischen Mindestanforderungen des BSI TLS
  - Webserver nach Cyber-Sicherheitsempfehlungen nach BSI-Empfehlung „Entwicklung sicherer Webanwendungen“, insbesondere Abschnitt „Entwicklungsphase“.
  - Logoff-Prozess, der bei vergessener Abmeldung eine Konfiguration durch unberechtigte Personen verhindert.

Für den Servicebetrieb:

- Verwendete Schnittstellen gegen unberechtigten Zugriff geschützt?
- Fernwartung: die verwendeten Komponenten dürfen den Betrieb nicht beeinträchtigen
- Fernwartung (Schreibzugriff) auf Produkt / Komponente nur bei expliziter Aktivierung der Komponente, expliziter Willenserklärung und zeitlich beschränkt.[31]

[31] Auszug aus BSI CS-E 132

5 Weitere Ansätze der Systematisierung

Neben dem BSI gibt es auch andere Institutionen, welche sich bemühen, Hilfestellung zu geben, um Medizinprodukte sicherer zu machen und hierzu konkrete Maßnahmen in Umfang und Ausführung vorschlagen.
Hierzu zählen das Johner-Institut in Zusammenarbeit mit dem TÜV Süd, die Allianz für Cybersicherheit (dem BSI angeschlossen) und in den USA die FDA.

5.1 Johner-Institut, Konstanz

Das Johner-Institut beschäftigt sich mit der Sicherheit insbesondere von Medizinprodukten und hat mehr als 150 Mitarbeiter und Forschende für dieses Thema beschäftigt.
Es wurde festgestellt: „Es fehlt in Deutschland die ‚Regulatory Science' für Medizinprodukte, wie sie die USA z.B. mit dem Harvard MIT Center for Regulatory Science hat."[32]
Das Institut hat es sich zur Aufgabe gemacht, hier maßgebliche Arbeit zu leisten, um dieses abzuändern und sich zu einer Regulierung Gedanken zu machen.
In diesem Rahmen wurden Guidelines sowohl zur Cybersicherheit von Medizinprodukten, als auch zur Anwendung von KI in der Medizin veröffentlicht.

Zur Cybersicherheit von Medizinprodukten hat sich auch das Johner-Institut gemeinsam mit dem TÜV-Süd umfangreich Gedanken gemacht.
Das Johner-Institut geht, lt. seiner Einlassungen, davon aus, dass die Hersteller von Medizinprodukten noch unzureichend die Anforderungen an die Cybersicherheit erfüllen. Daher hat es sich zur Zielsetzung gemacht, eine Hilfestellung zu einfachen ersten Verbesserungen zu geben. Es wäre wünschenswert, wenn zunächst die einfach abzuhelfenden Schwächen beseitigt werden und dann schrittweise die schwierigen Aufgaben bewältigt werden.
Weiter geht das Johner-Institut davon aus, dass künftig die Normen zur IT-Sicherheit von Medizinprodukten weiterentwickelt und harmonisiert werden, was jedoch noch Jahre in Anspruch nehmen kann. Daher bemühte man sich, einen Leitfaden für ein allgemein akzeptiertes Niveau zu erstellen. [33]

---

[32] https://www.johner-institut.de/unternehmen/mission/; Abrufdatum: 28.06.2023
[33] https://github.com/johner-institut/it-security-guideline/blob/master/Konzept-Leitfaden-IT-Sicherheit.md; Abrufdatum: 28.06.2023

Der Leitfaden richtet sich sowohl an die Hersteller, als auch an diejenigen Organisationen, welche die Cybersicherheit der Produkte bewerten müssen.
So hat das Institut auf Github beispielsweise ausgearbeitete Fragebögen veröffentlicht.
Ein großer Teil der Fragen / Empfehlungen ist auf den Prozess der Herstellung, insbesondere Programmierung gerichtet, siehe „Anforderungen an die Prozesse“, und gibt Hinweise auf einen möglichst sicheren Ablauf der Erstellung der Software und Auswahl der Komponenten. Dazu gibt es einen weiteren Teil „Anforderungen an das Produkt“, welcher viele Anforderungen aus den Empfehlungen des BSI für medizinische Produkte abdeckt.
Das Johner-Institut hat dabei vier Reifegradstufen vergeben, welche von Laien-Niveau, Stufe 0, bis Experten-Niveau, Stufe 3 reichen, wobei die Stufe 3 „über das hinaus, was ein Auditor in der Regel bei Medizinprodukten erwarten darf“[34], geht.
Daneben schließt die Auflistung des Johner-Instituts eine Forderung der FDA (U.S: Food and Drug Administration) nach Ablehnung per Default für alle eingehenden Datenverbindungen ein.
Die Empfehlungen sind teils spezifischer, als die des BSI, so beispielsweise, dass Passwörter als „salted hash“ gespeichert werden sollen, eine gegenüber der normalen kryptographischen Hashfunktion um eine weitere Komponente (salt) erweiterte und damit noch sicherere Variante.
Ein Teil der Forderungen betrifft eher die Produktsicherheit, als die Cybersicherheit, z.B. die Forderung nach Verzicht von kabellosen Datenverbindungen bei zeitkritischen Daten zugunsten der Patientensicherheit.
Trotz der hohen Nützlichkeit dieser Arbeiten sind auch diese nicht verbindlich und bringen noch keine Fortschritte im Sinne der Standardisierung von Angaben in der Dokumentation zum jeweiligen Medizinprodukt. Sie sind jedoch für Hersteller ein gute Grundlage, die Entwicklung von sichereren Produkten umzusetzen und die Entwicklungsprozesse bereits mit kleinem Aufwand, so bisher nicht getan, schon um eine höhere Cybersicherheit zu bereichern.

5.2 Allianz für Cybersicherheit

Die Allianz für Cybersicherheit ist ein Teil des BSI. Hier können Unternehmen, die sich mit Cybersicherheit beschäftigen, Mitglied werden, Informationen erhalten und an Schulungen teilnehmen.

[34] https://github.com/johner-institut/it-security-guideline/blob/master/Guideline-IT-Security_DE.md; Abrufdatum: 28.06.2023

Die Allianz für Cybersicherheit hat sich deshalb u.a. auch mit Medizinprodukten beschäftigt. So wurde die bereits erwähnte Empfehlung „Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte“[35] durch die Allianz für Cybersicherheit veröffentlicht.
Auch wurde die in den USA als weit verbreiteter Standard betrachtete Tabelle für den Leitfaden zur Nutzung des MDS2 empfohlen und veröffentlicht. [36]
Eine um die Ausfüllbarkeit erweiterte Form dieser Tabelle ist in den Anlagen, Teil 1 zu finden.
Diese Tabelle ist z.B. in den USA bei Ausschreibungen für Medizinprodukte ein Standard in der gängigen Praxis der Ausschreibung, da sie aufgrund des Ausfüllens durch den Hersteller eine Vergleichbarkeit und Beurteilbarkeit der Medizinprodukte erlaubt.

5.3 Food and Drug Administration (FDA)

Die FDA (Food and Drug Administration der Vereinigten Staaten) hat am 08. April 2022 einen Entwurf einer Richtlinie für Cybersicherheit von Medizinprodukten veröffentlicht.[37]
Die FDA ist die zuständige Zulassungsbehörde der USA.
Für den Entwurf der Richtlinie hat man sich umfassend Gedanken gemacht, welche Bestandteile einer Dokumentation notwendig sind, um die Cybersicherheit von Medizinprodukten darzustellen und nachprüfbar zu machen. Noch hat das Dokument keine Rechtsbindung und ist lediglich ein Entwurf mit Empfehlungen und Wünschen der Behörde, es hat jedoch das Potential eine Basis für ein standardisierteres Vorgehen bei der Planung, Beantragung und Genehmigung von Medizinprodukten im Hinblick auf die Cybersicherheit zu werden.
Diese Empfehlungen des Entwurfes sind umfangreicher und detaillierter als die bisher für den Europäischen Markt geltenden, insbesondere wird hier eine erste konkrete Ausgestaltung der für das Genehmigungsverfahren erwünschten Unterlagen gefertigt. Dieser Entwurf hat bisher keine Rechtskraft, gibt aber Hinweise darauf, was künftig vom Hersteller eines netzwerkfähigen Medizinproduktes als Dokumentation zu fertigen und einzureichen ist.
Ziel des Entwurfs ist es, künftig die Gefahren zu mindern, die zum Ausfall von Medizingeräten oder ganzen Krankenhäusern führen könnten. Eine reale Gefahr, mit welcher leider

[35] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_132.html; Abrufdatum 28.06.2023
[36] https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Netzwerk-Formate/Veranstaltungen-und-Austausch/Expertenkreise/CyberMed/cybermed_node.html; Abrufdatum 28.06.2023
[37] https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions; Abrufdatum 30.06.2023

Krankenhäuser bereits Erfahrungen machen mussten, welche zu Verzögerungen bei Diagnosestellungen und Behandlungen und damit letztlich zur Gefährdung von Menschenleben führen könnte.

Im Kapitel Einführung wird daher ausgeführt, dass die Sicherheit von Medizinprodukten sowohl für des Produkt selber, als auch für die weitere Anwendungsumgebung gesichert sein muss. Daher sollten die Empfehlungen nicht nur für genehmigungspflichtige Geräte, sondern auch für nach MDR genehmigungsfreie Geräte Berücksichtigung finden.

Ähnlich wie die Empfehlungen vom Johner-Institut werden auch hier ein starkes Augenmerk auf eine sicherheitsorientierte Produktentwicklung gelegt.

Entwicklung für Sicherheit

Es werden fünf Schutzziele benannt: Echtheit, einschließlich Integrität, Autorisierung, Verfügbarkeit, Vertraulichkeit und eine sichere, zeitnahe Möglichkeit für Updates und Patches. Diese Schutzziele sollten bei der Entwicklung beachtet werden, damit die Zahl du Schwere von möglichen Schwachstellen reduziert wird.

Transparenz

Es wird für wichtig erachtet, dass die Nutzer Zugang zu Informationen bezüglich der Cybersicherheit erhalten, damit sie über Kenntnisse zu möglichen Risiken und andere relevante Informationen verfügen.

Einzureichende Dokumentation

Auf die für die Zulassung notwendige Dokumentation wird in den Empfehlungen näher eingegangen. Diese sollte im Umfang dem Risiko angepasst sein. Die Hersteller sollten bei der Bewertung der Risiken das Gesamtsystem, in welches das Produkt voraussichtlich integriert wird, mit betrachten.

Risikomanagement

Da sich die Gefährdungen mit der Zeit verändern und entwickeln, kann man nicht von einer kompletten Sicherheit ausgehen. Daher gehört das Risikomanagement zur Qualitätssicherung des Herstellers, welches, nicht nur im Hinblick auf die Sicherheit der Patienten, die es gilt vor Schaden zu bewahren, sondern auch für den Hersteller und seinen Ruf wichtig ist. Hier wird auf die ISO 14971:2019 verwiesen.

Die Bewertung von Bedrohungen sollte nicht nur auf Wahrscheinlichkeit bezogen werden, sie basiert auf einer möglichen Ausnutzung von Schwachstellen des Medizingerätes oder des Systems, in welchem es angewendet wird.

So ist es nicht nur wichtig, den aktuellen Stand der Bedrohungen zu untersuchen, sondern auch sicher zu stellen, dass sich im Verlaufe des Betriebs des Medizingerätes entstehende Möglichkeiten der Ausnutzung von Schwachstellen entweder bereits verhindert werden oder mittels geplanter Maßnahmen nach Markteinführung unter Kontrolle gehalten werden.

Daher sind die Hersteller angehalten, sowohl eine Risikobewertung nach ISO 14971, als auch eine begleitende Risikobewertung durchzuführen, um Gefährdungen für Patienten zu erkennen und unter Kontrolle zu halten.
Insbesondere für Risiken, die nur teilweise oder nicht gemindert werden konnten, sollten diese als vorhersehbare Risiken weiter bewertet und zusätzliche Kontrollmechanismen oder Risikotransfers eingeplant werden.

Threat Modeling

Threat Modeling beinhaltet den Prozess, Sicherheitsziele zu benennen, Risiken und Schwachstellen im System zu identifizieren und folglich Gegenmaßnahmen zum Schutz festzulegen oder die Folgen zu minimieren, welche durch die Gefahren während des gesamten Lebenszyklus entstehen können.
Die FDA empfiehlt das Threat Modeling, um hierdurch für die Risikoanalyse zu gewinnen und diese zu unterstützen.
Das Modell sollte:

- Systemrisiken und Minderungsmöglichkeiten identifizieren, das Risiko als Teil der Risikoanalyse vor und nach Minderung ermitteln,
- Feststellungen zum geplanten Nutzungssystem darlegen und
- Risiken erkennen, welche durch die Lieferkette, Herstellung, Einbau oder Zusammenspiel mit anderen Geräten, Wartung oder Updates und die Außerbetriebnahme entstehen, welche anderenfalls in der herkömmlichen Risikoanalyse übersehen werden könnten.

Die FDA empfiehlt, dass die Antragsunterlagen eine Dokumentation des Threat Modeling beinhalten, welche zeigen, wie Risiken bewertet werden und welche Mechanismen zur Risikokontrolle eingesetzt wurden. Für diese sollten Sicherheit und Effektivität nachgewiesen werden.

Fremde Softwarekomponenten

Die FDA hat bereits Richtlinien für die Nutzung von Softwarekomponenten, die von Dritten bezogen werden, erstellt.
Als Teil des Qualitätsnachweises, dass die Regeln eines sicheren Designs eingehalten wurden und das Risikobehandlung aus Lieferketten, eigener Softwareentwicklung und für erworbene Software erfolgt ist, sollte das Cybersicherheitsrisiko bewertet und dargelegt werden.
Außerdem haben die Hersteller entsprechend der bestehenden Richtlinien einen Kontrollprozess einzurichten, welcher den Nachweis ermöglicht, dass Zulieferer die Anforderungen des Herstellers erfüllen.

Als Teil des Ausstattungsmanagements sollten die Hersteller Nutzungsrechte am Sourcecode durch Hinterlegung oder Backups besitzen.

Software Bill of Materials (SBOM)

„Eine Software Bill of Materials ist eine formale, strukturierte Aufzeichnung, die die

- Komponenten eines Softwareprodukts und
- ihre Beziehungen innerhalb der Softwarelieferkette

beschreibt. Eine SBOM gibt also einerseits an, welche Pakete und Bibliotheken in Ihre Anwendung eingeflossen sind, andererseits auch die Beziehung zwischen diesen Paketen und Bibliotheken und anderen vorgelagerten Projekten.“[38]

Eine robuste SBOM beinhaltet sowohl die durch den Hersteller entwickelten Komponenten, als auch die von Dritten entwickelten. Daneben beinhaltet sie auch die Abhängigkeiten voneinander für Eigenentwicklungen, gekaufter / lizenzierter oder open-source Software.

Die SBOM kann darüber hinaus ein gutes Mittel für die Transparenz bezüglich möglicher Risiken gegenüber den Nutzern.

unterstützende Dokumentation der SBOM

Die Dokumentation sollte folgende Punkte beinhalten:

- Das Element, in welchem die Software installiert wurde
- Name der Software-Komponente
- Version der Software-Komponente
- Hersteller der Software-Komponente
- Level of Support, welcher mittels Überwachung und Wartung durch den Hersteller der Software-Komponente gewährleistet wird,
- Das End-of-Support-Datum der Software-Komponente
- Jegliche bekannte Schwachstellen

Dazu gehören weiter:

- Bewertungen der Sicherheitsrisiken jeder bekannten Schwachstelle und
- Angaben zur Risikobehandlung bezüglich der Schwachstellen. Wenn Risikobehandlungen Gegenmaßnahmen beinhalten, so sind sie in angemessener Detailtiefe zu beschreiben.

Gegenmaßnahmen (compensating controls) werden eingesetzt, wenn eine Risikobehandlung nicht sinnvoll oder nur mit unverhältnismäßigem Aufwand durchgeführt werden

.[38] https://www.csoonline.com/de/a/was-ist-eine-software-bill-of-materials,3674040; Abrufdatum: 01.07.2023

können. Im Gegensatz zur Risikobehandlung, welche von permanentem Character ist, ist die Gegenmaßnahme temporärer Natur.

Sicherheitsbewertung und unbehandelte Anomalien

Die FDA empfiehlt, dass die Hersteller eine Liste mit Software-Anomalien, welche zum Antragszeitpunkt für das Produkt existieren, zur Verfügung stellen.

Dokumentation der Risikobewertung

Die Dokumentation, welche die Sicherheit des Produktes darlegen soll, sollte den Plan der Risikobehandlung und den Bericht der Risikobehandlung beinhalten (AAMI TIR57). Diese sollen das Threat Modeling für das System, die SBOM und Bewertungen von unbehandelten Anomalien beinhalten.

Risikobeobachtung des gesamten Lebenszyklus des Medizinproduktes

Hersteller sollen ihre Risikobewertung überarbeiten, sobald es neue Informationen gibt, wenn neue Angriffe, Schwachstellen, Komponenten oder nachteilige Einflüsse während der Entwicklung oder nach Freigabe bekannt werden.

Sicherheits-Architektur

Hersteller sind verantwortlich, Cybersicherheits-Risiken für ihre Geräte und die Systeme in denen diese eigesetzt werden zu erkennen und entsprechende Maßnahmen der Risikobehandlung und -minimierung einzurichten.

Die Zulassungsanträge haben daher die Sicherheits-Architektur zu dokumentieren.

Die Erfassung von sicherheitsrelevanten Abhängigkeiten, Schnittstellen, Verbindungen mit der Außengrenzen des Systems im Detail ermöglicht die Erkennung der Teile des Systems, über welche ein Angriff ausgeführt werden könnte.

Eine solche Analyse des gesamten Systems sollte durchgeführt werden, um die gesamte Umgebung und den Kontext zu verstehen, in welchem das Gerät erwartungsgemäß eigesetzt werden wird.

Es wird empfohlen, dies in Form von Diagrammen durchzuführen. Diese sollten in die Unterlagen, welche die Sicherheit und Effektivität des Gerätes belegen sollen, integriert sein und keine separat zu erstellenden Dokumente werden.

Einzubauende Sicherheitsmaßnahmen

Die FDA betrachtet die Art, in der ein Gerät die Cybersicherheit angeht und die Art, auf welche es auf einen Cyberangriff, wenn es diesem ausgesetzt wird, beantwortet, als Funktionen der Gestaltung des Gerätes. Effektive Cyber-Sicherheit beruht auf der eingebauten Sicherheit und nicht auf einer nachträglich aufgesetzten.

Die Sicherheitsmaßnahmen entstammen hauptsächlich, jedoch nicht beschränkt auf diese, den folgenden Kategorien:

- Authentifizierung
- Autorisierung
- Kryptographie
- Integrität von Code, Daten und Ausführung,
- Vertraulichkeit,
- Angriffserkennung und Logging,
- Resilienz und Wiederherstellung und
- Updatebarkeit und Patchfähigkeit.

Die FDA empfiehlt die Aufführung von Anforderungs- und Akzeptanzkriterien für jede der vorstehenden Kategorien in den Antragsunterlagen.

Wenn Gegenmaßnahmen getroffen werden, welche hier nicht aufgelistet wurden, dann sollte der Hersteller eine Dokumentation mit Nachvollziehbarkeit der spezifischen Eigenschaften und Sicherheitsfunktion zur Verfügung stellen.

Diagramme der Sicherheits-Architektur

Anzahl und Umfang der Architekturdiagramme, welche den Antragsunterlagen beigefügt werden, hängen von der Angriffsoberfläche(n) ab, welche durch das Threat Modeling und Risiko erkannt wurden.

Diese Diagramme sind ein effektiver Weg, das Threat Modeling zu übermitteln.

Es wird empfohlen, mindestens folgende Diagramme zu erstellen:

- Diagramm des Gesamtsystems
- Diagramm der Mehrpatienten-Gefährdung
- Diagramm Updatebarkeit und Patchfähigkeit
- Diagramm des Anwendungsfalles Sicherheit

Diese Dokumente beinhalten die Diagramme und die textliche Erläuterung.

Die Diagramme sollten

- sicherheitsrelevante Systemelemente und deren Schnittstellen benennen,
- Sicherheitskontext, Bereiche, Grenzen und Außenschnittstellen des Systems definieren,
- Abstimmung der Systemarchitektur mit a) den Sicherheitszielen des Systems und b) den Charakteristika der Sicherheitsgestaltung und
- eine Nachvollziehbarkeit der Architektur-Elemente für Nutzer und Erfordernisse des Sicherheitssystems herzustellen.

Beispielsweise werden Systeme mit Netz- oder Cloudzugang erwartungsgemäß mehr Anwendungsfalldiagramme haben, als ein System mit lediglich einem USB-Anschluss.

Diagramm des Gesamtsystems

Das Diagramm sollte das umfassende System, einschließlich des Medizinproduktes selbst mit allen inneren und äußeren Schnittstellen umfassen.

Es sollte für alle eingebundenen und Netzwerkgeräte sollte das Diagramm alle eingebundenen Elemente, einschließlich der Softwareupdate-Infrastruktur, Einflüsse aus dem Netzwerk der medizinischen Ausstattung, Zwischenverbindungen oder -geräte, Cloudverbindungen etc. benennen.

Abhängig vom Umfang des Systems kann es sinnvoll sein, die Daten anstatt in einem Diagramm in mehreren Diagrammen darzustellen.

Diagramm der Mehrpatienten-Gefährdung

Wenn es möglich ist, dass die Geräte, über Kabel oder drahtlos, mit anderen medizinischen oder nichtmedizinischen Geräten, einem Netzwerk oder dem Internet verbunden werden könnten, kann das zu einer Kompromittierung von mehreren Geräten gleichzeitig führen. Daher kann dies ein Sicherheitsrisiko für Patienten darstellen, weil es die beabsichtigte Funktion des Gerätes verändern kann. Über eine nichtmedizinische Anwendung kann die medizinische Anwendung des Gerätes verändert werden und dadurch letztlich den Patienten gefährden.

Wenn mehrere Geräte kompromittiert werden, kann dies mehrere Patienten durch das Gerät selbst oder die Störung des medizinischen Ablaufs betreffen.

Die FDA empfiehlt, dass der Hersteller darlegt, wie sein Gerät oder System solche Angriffe abwehrt und darauf reagiert. Dazu dient das Diagramm der Mehrpatienten-Gefährdung. Diese Risiken müssen separat in der Risikobewertung behandelt werden, da sie ein Risiko von anderer Natur sind.

Diagramm der Updatebarkeit und Patchfähigkeit

Aufgrund der Notwendigkeit, dass zeitnah und verlässlich eine Versorgung der Geräte mit Updates stattfindet, um neu auftretenden Sicherheitsrisiken entgegen wirken zu können, wird empfohlen, auch dafür ein Diagramm zu erstellen. Es soll den Ende-zu-Ende-Prozess beschreiben, der es ermöglicht, Updates und Patches zur Verfügung zu stellen. Die erforderlichen Details sind im Anhang der Richtlinie der FDA ausgeführt.

Diagramm des Anwendungsfalls Sicherheit

Dieses sollte alle Systemfunktionen darstellen, durch welche die Sicherheit oder Effektivität beeinträchtigt werden könnte. Es sollte mehrere Operationszustände der Systemelemente beinhalten und den zugehörigen klinischen Status des Systems benennen, wie beispielsweise die Anzeige von Diagnoseberichten etc..

Die Anzahl der Diagramme sollte adäquat zum Umfang des Systems erstellt werden. Die einzuarbeitenden Informationen sind ebenfalls dem Anhang der Empfehlung der FDA zu entnehmen.

Cybersicherheitstests

Die Dokumentation von Sicherheitstests und zugehörige Berichte und Bewertungen sollten mit den Antragsunterlagen eingereicht werden.

Anforderungen

- Hersteller sollten beweisen, dass sie die Anforderungen an den Aufbau für Eingaben erfolgreich umgesetzt haben.
- Hersteller sollten beweisen, dass sie die Grenzflächenanalyse durchgeführt haben und welche Erkenntnisse für die Schlussfolgerungen angewandt wurden.

Gefährdungsminderung

- Hersteller sollten beweisen und die Testung detailliert darlegen, wie effektiv die Maßnahmen der Risikobehandlung entsprechend den vorbenannten Anwendungsfall- und Ablaufdiagrammen sind.
- Die Hersteller sollten die Angemessenheit jeder Risikobehandlungsmaßnahme zusichern können.

Schwachstellentestung

- Hersteller sollten detailliert beweisen, dass folgende bekannte Schwachstellen getestet wurden:
  - missbrächliche, fehlerhafte oder unerwartete Eingaben
    - Robustheit
    - Fuzz-testing (= Test mit Zufallsdaten)
  - Angriffsvektoren
  - Schwachstellen-Kombinationen
  - Closed-Box-Testung (=Testung ohne Kenntnis des Codes) bezüglich bekannter Schwachstellen
  - Software Composition Analysis (= Testung zur Erkennung von Open-Source Code und dessen Aktualität) für ausführbare Dateien
  - Statische und dynamische Code-Analyse, einschließlich Suche nach Credentials (= Suche nach Klartextpasswörtern und anderen Geheimnissen in Codes), welche als Standard (default) implementiert sind, leicht abgeleitet oder leicht kompromittiert werden könnten.

Penetrationstestung

- Dieser Test sollte durch Entdeckung und Nutzung von Schwachstellen der Sicherheit sicherheitsrelevante Gegebenheiten des Produktes identifizieren und charakterisieren.
- Der Bericht des Penetrationstests sollte folgendes enthalten:
  - Unabhängigkeit und technische Expertise des Testers
  - Umfang der Testung
  - Dauer der Testung
  - Angewandte Testmethoden
  - Testergebnisse, Entdeckungen und Beobachtungen

Transparenz der Cybersicherheit

Damit die Nutzer das Cybersicherheitsrisiko beachten können, ist die Transparenz die kritische Komponente, um die sichere und effektive Nutzung bei Integration des Gerätes in seine Umgebung gewährleisten zu können.
Verschiedene Nutzer haben verschiedene Fähigkeiten, eine Rolle in der Risikobehandlung zu übernehmen. Daher sollten die notwendigen Maßnahmen für die Gewährleistung der Sicherheit dem Nutzertyp angepasst sein.

Kennzeichnung

Die Kennzeichnung kann ein wichtiger Teil des Qualitätsmanagements sein. Sie sollte die relevanten Sicherheitsinformationen beinhalten. Die FDA empfiehlt dazu

- Anleitungen und Datenblätter bezüglich Risikobehandlungsmaßnahmen angemessen für die geplante Anwendungsumgebung (z.B. Virenschutz, Nutzung einer Firewall, Passwortanforderungen) zu erstellen.
- Ausreichend detaillierte Diagramme, welche den Nutzern ermöglichen, die empfohlenen Sicherheitsmaßnahmen auszuführen.
- Liste der Netzwerkschnittstellen (Ports) und anderer Schnittstellen, welche erwartungsgemäß Daten senden oder empfangen können. Die Liste sollte die Funktionen der Schnittstellen, Datenflussrichtungen und zulässige Endpunkte des Datenflusses enthalten.
- Spezielle Richtlinien für Nutzer mit den Anforderungen an die Infrastruktur, in welcher das Medizingerät zum Einsatz vorgesehen ist.
- SBOM, wie im Entwurf beschrieben oder in üblichem Format, um die Komponenten effektiv zu betreiben und die möglichen Einflüsse der bekannten Schwachstellen zu verstehen. SBOM-Informationen sollten kontinuierlich und maschinenlesbar zur Verfügung gestellt werden, beispielsweise mittels eines stets auf den neusten Stand bezogenen Link für Onlineinformationen.

- Beschreibung von systematischem Vorgehen für Nutzer, um versionsbezogene und herstellergenehmigte Software oder Firmware herunterzuladen, einschließlich einer Beschreibung dessen, wie Nutzer über neue Softwareupdates informiert werden.
- Beschreibung der Reaktion des Gerätes auf Anomalien, um die Sicherheit zu gewährleisten.
- Ausführliche Beschreibung der Geräteeigenschaften, welche kritische Funktionen schützen.
- Beschreibung von Backup, Wiederherstellungseigenschaften und -verfahren, um eine authentifizierte Konfiguration wiederherzustellen.
- Beschreibung von Methoden zur Aufbewahrung und Wiederherstellung der Konfiguration durch einen authentifizierten und autorisierten Nutzer.
- Beschreibung der sicheren Auslieferungskonfiguration und von Nachteilen, welche durch eingesetzte Möglichkeiten der Härtung des Systems entstanden und Anleitung für Konfigurationsänderungen durch den Nutzer.
- Wenn für den geplanten Einsatz angemessen, eine Beschreibung, wie forensische Beweise gesichert werden können, einschließlich, jedoch nicht beschränkt auf Logfiles, welche aufgrund von Sicherheitsvorfällen entstanden.
- Wenn angemessen, technische Anleitungen zum sicheren Einsatz im Netzwerk und Anleitungen für die Reaktion im Fall von Entdeckung von Vorfällen oder Schwachstellen.
- Informationen zur Gerätesicherheit im Falle der Beendung des Supports und der Außerbetriebnahme.
- Informationen, wie im Falle der Außerbetriebnahme das Produkt von sensiblen, vertraulichen, nichtöffentlichen Daten und Software gereinigt werden kann.

Plan der Schwachstellenbehandlung

Die FDA empfiehlt, dass den Antragsunterlagen ein Plan zu Mitteilungen bezügich Schwachstellen beigefügt wird, damit eingeschätzt werden kann, ob der Hersteller nach Marktzulassung ausreichend Vorsorge getan hat, um nach Zulassung die Sicherheit und Effektivität weiter zu gewährleisten.

Die Kategorien der Sicherheitsmaßnahmen und zugehörige Empfehlungen.

Neben Erklärungen zu den Kategorien, welche bereits unter Punkt „Einzubauende Sicherheitsmaßnahmen“ erwähnt wurden, werden Empfehlungen zur Implementation gegeben. Diese sind besonders nützlich, da hier gezielt effektive Maßnahmen benannt werden, die nach aktuellem Stand der Technik Anwendung finden sollten. Nach diesen Vorgaben kann auch eine Benannte Stelle bei positivem Abgleich von einer Einhaltung der Erfordernisse an die Sicherheit ausgehen. Daher wird hier als Auszug die Maßnahmenliste eingearbeitet,

für die Anwendung ist es dennoch sehr informativ, die Empfehlungen als Gesamtheit im Originaldokument einzusehen, da hier nicht der gesamte Umfang wiedergegeben werden kann.

Authentifizierung:

- Nutzung starker kryptographischer Authentifizierung (hier sei angemerkt, dass es dazu sowohl für den europäischen, als auch den US-amerikanischen Markt bereits Standards gibt) für Personal, Nachrichten, Befehlsupdates und soweit zutreffend für alle anderen Kommunikationswege. Hardwarebasierte Sicherheitslösungen, wenn anwendbar, sollten gewählt werden.
- Authentifizierung externer Verbindungen mit einer Wiederholungsrate, dem Risiko angemessen. Beispielsweise Verbindung zu einem Server außerhalb des Systems sollten Gerät und Server sich stets gegenseitig bei jeder Session authentifizieren und die Dauer der Session auch dann begrenzen, wenn die Verbindung über eine oder mehrere sichere Verbindungen erfolgt.
- Angemessene Nutzerauthentifizierung, beispielsweise Mehrfaktorauthentifizierung, um priviligierten Zugang zum Gerät für Administratoren, Servicetechniker oder Wartungspersonal u.a. zu gewähren.
- Authentifizierung anfordern und Genehmigung in bestimmten Fällen, bevor Softwareupdates oder Firmwareupdates, einschließlich der für das Betriebssystem, Viren- oder Malwareschutz oder Anwendungen aufgespielt werden können.
- Starker Passwortschutz. Es sollten keine Passwörter Anwendung finden, die hardcoded (im Code implementiert), Default-Passwörter oder leicht zu erratende Passwörter sind. Auch leicht kompromittierbare Passwörter, wie solche, welche für jedes Gerät benutzt werden, sollten nicht genutzt werden. Passwörter sollten nicht als Default genutzt werden, sollten nicht schwer zu ändern sein oder Gefahr laufen, dass sie öffentlich bekannt werden.
- Anti-Replay-Mittel sollten in kritischer Kommunikation eingesetzt werden, beispielsweise wenn möglicherweise gefährdende Befehle übermittelt werden. Hierzu können kryptographische Nonces (Number used once) benutzt werden.
- Bereitstellung von Mechanismen, welche die Authentizität von Informationen, welche vom Gerät gesandt werden, bestätigen, beispielsweise Telemetrie. Das gilt insbesondere für Daten, welche, wenn manipuliert, Patienten gefährden können.
- Man sollte sich nicht auf zyklische Redundanzprüfungen als Sicherheitsmaßnahme verlassen, da sie weder Integrität, noch Authentizität schützen. Zyklische Redundanzprüfungen dienen der Erkennung von Fehlern und schützen vor Umwelteinflüssen (noise, EMC), können jedoch nicht vor beabsichtigtem oder bösartigem Einfluss schützen.

- Angaben machen, wie das Gerät oder System bei missglückter Authentifizierung reagiert.

Autorisation

- Beschränkung des autorisierten Zugriffs auf Geräte mittels Authentifizierung von Nutzern mittels ID, Passwort, Smartcard, Biometrie, Zertifikaten etc.,
- Automatisierte, zeitbasierte Beendigung von Sessions innerhalb des Systems, wo es für die Nutzungsumgebung angemessen ist,
- Autorisierungsmodell unter Einsatz des Prinzips der geringsten Rechte basierend auf der Rolle der Nutzer (Patient, Systemadministrator etc.) oder der Gerätefunktion,
- Einrichtung des Gerätes auf „deny by default“ (Ablehnung ist Standard), so dass alles, was nicht ausdrücklich erlaubt ist, abgelehnt wird. Damit sollte das Gerät generell alle Verbindungen (Eingang TCP, USB, Bluetooth, Serielle Schnittstellen etc.) ablehnen. Das Ignorieren von Anfragen ist eine Form der Ablehnung.

Kryptographie

- Auswahl kryptographischer Algorithmen und Protokollen, die dem Industriestandard entsprechen, Auswahl einer angemessenen Schlüsselgenerierung, -zuteilung und -verwaltung und des Schutzes der Schlüssel, Einsatz von robusten Nonce-Algorithmen.
- Anwendung des aktuellen NIST-Standards für Kryptographie oder gleich starken kryptographischen Schutz während des gesamten Lebenszyklus des Produktes.
- Der Aufbau der Systemarchitektur und die eingesetzten Sicherheitsmechanismen sollten verhindern, dass die Kompromittierung eines einzelnen Gerätes dazu führen kann, dass dadurch die Schlüssel zu anderen Geräten ermittelt werden können:
  - keine Anwendung von Genrealschlüsseln, welche auf Geräten gespeichert werden, keine Schlüsselerzeugung, welche einzig auf Geräte-IDs oder anderen leicht herauszufindenden Informationen beruht.
  - keine Anwendung von Seriennummern als Schlüssel oder Teil des Schlüssels, da diese Patienten bei der Suche nach Informationen zur Kenntnis gelangen können, oder beim Rückruf von Geräten zur Identifizierung von betroffenen Geräten veröffentlicht werden. Public-Key-Kryptographie kann helfen, dieses umzusetzen.
- Anwendung von kryptographischen Protokollen, welche Verhandlung von Parametern / Versionen erlauben, damit aktuelle und sichere Einstellungen genutzt werden, sofern nicht anders notwendig.
- Verhinderung von Downgrades oder Rollbacks von Versionen, wenn nicht zwingend erforderlich, da diese es Angreifern ermöglichen, Schwachstellen der Vorversion oder weniger geschützte Versionen auszunutzen.

Integrität von Code, Daten und Ausführung

Code:

- Firmware und Software soll authentifiziert werden durch Prüfung von Tags, wie Signaturen oder „Message Authentication Codes MACs“ im Software- oder Firmwareinhalt, Versionsnummern oder Metadaten. Die Versionsnummern, welche installiert werden sollen, sollten signiert sein oder MACs besitzen. Geräte sollten elektronisch und sichtbar identifizierbar sein (UDI, Modellnummer, Seriennummer)
- Installation sollte für kryptographisch authentifizierte Firmware möglich sein, jedoch nicht wenn diese fehlt oder nicht korrekt erfolgt. Diese sollte kryptographisch signiert sein, um das Schutzniveau nicht durch Downgrade oder Rollback zu senken.
  - Downgrade, wenn zwingend erforderlich, kann durch Signatur und neue Metadaten ermöglicht werden.
- Die Authentifizierung sollte vor Installation erfolgen.
- Verhinderung oder Beschränkung von ungenehmigtem Zugang zu Debug-Ports (JTAG, UART etc.) bevor das Produkt ausgeliefert wird.
- Anbringung von Originalitätsverschluss-Siegeln an den Verschlüssen des Geräts und an empfindlichen Kommunikationsschnittstellen, um die physische Integrität nachzuweisen.

Daten

- Sicherstellung der Integrität aller eingehenden Daten, dass sie auf dem Transport nicht verändert wurden. Dazu kann kryptographische Authentifizierung verwendet werden. Damit kann die Integrität, jedoch nicht die Korrektheit gewährleistet werden.
- Überprüfung aller eigehenden Daten, dass diese in Form den erwarteten Protokollen und Spezifikationen entsprechen. Wenn angebracht, dann sollte man überprüfen, dass die Daten innerhalb eines für den Patienten sicheren Bereiches liegen.
- Die Integrität sollte für alle Daten geprüft sein, welche die Sicherheit und Effektivität des Gerätes beeinflussen können, wie Konfigurationseinstellungen oder Energieabgaben.

Ausführung

- Anwendung der Best Practice - Standards der Industrie, um die Integrität des Codes zu erhalten und zu prüfen, während er auf dem Gerät ausgeführt wird. Dafür kann ein Host-Based Intrusion Detection oder Prevention System, auf dem Gerät eingerichtet und zur Kontrolle von Zugriffen, genutzt werden.
- Jeder Code, der die Syntaxkontrolle von eingehenden Daten durchführt, sollte sogfältig entworfen und geprüft werden. Dazu können automatisierte und manuelle Methoden angewandt werden.

Vertraulichkeit

Die Anwendung der unter Authentifizierung und Autorisation genannten Maßnahmen sollten in der Lage sein, die Vertraulichkeit zu gewährleisten.

Angriffserkennung und Logging

- Einrichtung von Entwurfseigenschaften, welche Kompromittierung der Sicherheit und verdächtige Versuche aufspüren, erkennen, loggen, zeitlich erfassen und während der normalen Benutzung reagieren. Dabei sollte man die Nutzen-Risiko-Bewertung benutzen, welche bestimmt, ob eine Reaktion während der Nutzung des Gerätes angebracht ist.
- Sicherstellen, dass die Ausführung eine forensische Beweissicherung ermöglicht. Das Gerät sollte Logfiles erstellen und speichern können, um Angriffsversuche nachvollziehen zu können. Die Dokumentation sollte angeben, wie und wo die Daten gespeichert wurden, ob sie wiederverwendet oder archiviert werden und wie sie durch automatisierte Analysesoftware verarbeitet werden können.
- Auswirkungen von Vorfällen an Schwachstellen sollten so eingeschränkt werden, dass eine sichere Konfiguration festgelegt wurde. Das kann einen Malware-Schutz, Firewall, Allow-Listening (IP-Überwachung), Festlegung von Sicherheitsparametern, Logging-Parametern oder physische Angriffskontrolle beinhalten.
- Das Gerät sollte so entworfen werden, dass es Malware-Schutz integrieren oder nutzen kann. Diese Fähigkeiten können vom Gerätetyp, der Software oder den Hardware-Komponenten abhängen.
    - Geräte, die Windows-Betriebssysteme nutzen:
        - Antivirus / Antimalware ist empfohlen, dabei sollten verschiedene Varianten zulässig sein, um die Vorlieben der Nutzer zu unterstützen.
    - Nutzung anderer handelsüblicher Betriebssysteme (Ubuntu, Linux, Unix, Apple ..)
        - Antivirus / Antimalware ist abhängig von der Umgebung empfohlen, es ist eine Fall-zu-Fall-Entscheidung notwendig, abhängig vom Netzzugang und Risiko
    - Nutzung von Embedded Betriebssystemen (Real-Time-OS, Windows embedded etc.)
        - Antivirus / Antimalware ist nicht generell erforderlich, es sei denn, ein spezifisches Risiko oder Gefährdung konnte festgestellt werden, was nicht durch andere Maßnahmen verhindert werden kann.
- Das Gerät sollte eine Konfigurationsverwaltung, Genehmigungsnachverfolgung und Kontrolle von Softwareänderungen ermöglichen, welche elektronisch gesichert wird und möglichst maschinenlesbar durch autorisierte Nutzer ermittelt werden kann.

- Die Geräte sollten Variationsanalyse ermöglichen, welche feststellen kann, ob gleiche Schwachstellen übergreifend auf den Gerätemodellen oder Produktionslinien festgestellt werden kann.
- Es sollte überdacht werden, ob es möglich ist, dass das Gerät eine SBOM in maschinenlesbarem Format auswerfen kann.

Resilienz und Wiederherstellung

- Es sollten Eigenschaften eingesetzt werden, welche kritische Funktionen und Daten auch dann schützen, wenn das Gerät teilweise kompromittiert wurde. Das könnte durch Prozessisolation, Virtualisierungstechniken, hardwaregestützte sichere Ausführungsumgebungen erfolgen. Dadurch sollen Mechanismen angewendet werden, welche die Auswirkungen eines erfolgreichen Eindringens in das Gerät beschränken.
- Die Ausführung des Gerätes sollte es ermöglichen, dass eine sichere Konfiguration abgelegt und durch eine autorisierte und authentifizierte Person wiederhergestellt werden kann.
- Die Ausführung sollte das Niveau der Resilienz festlegen oder eine unabhängige Fähigkeit zu funktionieren, die jede Komponenten des Systems besitzt, wenn ihre Kommunikation mit dem Rest des Systems unterbrochen wurde und dies auch eine maßgebliche Zeit so bleibt.
- Das Gerät sollte so konstruiert sein, dass es eine Resilienz bezüglich möglicher Cyberangriffe besitzt, beispielsweise Netzwerkausfälle, Denial-of-Service-Angriffe, exzessive Nutzung der Bandbreite durch andere Geräte, gestörte Qualität der Dienste oder exzessive Jitter (Störung durch Verzögerung eingehender Pakete).

Firmware- und Softwareupdates

- Die Ausführung des Gerätes sollte die Notwendigkeit von Software- oder Firmwarepatches berücksichtigen, damit auch künftig auftretende Schwachstellen beseitigt werden können. Das wird voraussichtlich zusätzlichen Speicher und Verarbeitungsressourcen benötigen.
- Es sollte die Zuverlässigkeit von Updates überdacht werden und wie der Prozess im Falle der Unterbrechung der Kommunikationsverbindung reagiert. Dabei sollte der Einfluss auf die Hardware und die Möglichkeiten der Unterbrechung in jeder Phase des Updates berücksichtigt werden.
- Die Sicherheitspatches und -updates sollten von den regulären Updatezyklen unabhängig sein.

- Es sollten Prozesse, Technologien und Sicherheitsarchitekturen eingerichtet sein, welche die schnelle Verifikation, Validierung und Auslieferung der Patches und Updates ermöglichen.
- Die Einrichtungen, welche während der Entwicklung und Testung des Originalproduktes eingerichtet wurden, wie die aufgebauten Umgebungen, virtuelle Maschinen, Regressionstestanlagen, Entwicklungswerkzeuge, Emulatoren, Debugger und andere Werkzeuge sollten aufbewahrt und erhalten werden, damit die Updates und Patches für das Produkt zeitnah und sicher angewendet werden können.
- Notwendige Drittpartei-Lizenzen sollten über die gesamte unterstützte Lebenszeit des Gerätes aufrechterhalten werden. Es sollten Ausweichplanungen gemacht werden, für den Fall, dass der Anbieter der Drittpartei-Lizenz nicht mehr verfügbar ist, oder die Unterstützung des lizenzierten Produktes einstellt. Modulares Design wäre eine Möglichkeit, damit die Drittpartei-Lösung verfügbar ersetzt werden kann.

Bei dem ausgewerteten Dokument handelt es sich um einen Entwurf. Jedoch beabsichtigt die FDA, dieses noch in diesem Jahr in eine gültige Richtlinie zu überführen.[39] Es ist offen, welche Änderungen diese Empfehlung dabei erfährt.

[39] https://www.fda.gov/medical-devices/guidance-documents-medical-devices-and-radiation-emitting-products/cdrh-proposed-guidances-fiscal-year-2023-fy2023; Abrufdatum: 03.07.2023

6 Risikoanalyse

Mit dem BSI-Standard 200-3 stellt das BSI ein leicht anzuwendendes und anerkanntes Vorgehen zur Verfügung, mit dem Institutionen ihre Informationssicherheitsrisiken angemessen und zielgerichtet steuern können. [40]

Das BSI empfiehlt, dass in bestimmten Fällen eine Risikoanalyse durchgeführt werden muss, u.a. wenn das Risiko mit den existierenden Bausteinen des IT-Grundschutzes nicht hinreichend abgebildet werden. Das ist insbesondere bei Medizinprodukten der Fall, da diese

- in Aufbau und Funktion sehr vielfältig und damit mit Standardbausteinen schlecht abzubilden sind,
- sich in der Anwendung von Medizinprodukten ein hohes Schadpotential entfalten kann,
- Medizinprodukte in Szenarien angewendet werden können, welche im Rahmen des IT-Grundschutzes nicht vorgesehen sind.

Daher ist zu prüfen, inwieweit sich ein über den Grundschutz hinaus gehender Schutzbedarf ergibt. Der BSI-Standard 200-3 stellt eine Anleitung zur Risikobewertung dar.

6.1 Grundlagen

Die Risikoanalyse beinhaltet das Identifizieren, Einschätzen und Bewerten des Risikos der Systemkomponenten.

Die Schritte der Risikoanalyse müssen hier an das System Medizinprodukt angepasst werden. In Anlehnung an Kapitel 2 des BSI-Standard 200-3 werden folgende Schritte empfohlen:

- Feststellung des bereits vorhandenen Sicherheitskonzeptes für das Produkt und die Komponenten, einschließlich der bereits vorhandenen Rollen und Hierarchien
- Festlegung des Geltungsbereiches des Sicherheitskonzeptes, der sogenannte Informationsverbund, insbesondere Festlegung der Außengrenzen des zu betrachtenden Systems
- Strukturanalyse des Informationsverbunds, der Komponenten, Prozesse und Darstellung in einem Flussdiagramm und Liste der Abhängigkeiten

[40] BSI-Standard 200-3, Risikoanalyse auf der Basis von IT-Grundschutz, www.bsi.bund.de/grundschutz

- Festlegung des Schutzbedarfes der Komponenten, Liste kritischer Kommunikationsverbindungen, mit Festlegung der Stufen des Schutzbedarfes für die drei Grundwerte (Vertraulichkeit, Integrität und Verfügbarkeit)
- Feststellung, ob es für die jeweilige Komponente einen passenden IT-Grundschutzbaustein gibt und wie dieser angewendet werden kann
- Feststellung welcher Grundschutz bereits vorhanden ist und wo Defizite bestehen

Aus diesen Erkenntnissen wird eine Liste der Komponenten (Zielobjekte) erstellt, für welche eine Risikoanalyse durchzuführen ist. Dieses sind regelmäßig diejenigen Komponenten, welche ein hohes bis sehr hohes Gefahrenpotential bilden oder besonders oft von Sicherheitsproblemen betroffen sein können. Komponenten können in geeigneten Gruppen zusammengefasst werden.

Auf die drei Grundwerte mit Schutzbedarf, Vertraulichkeit, Integrität und Verfügbarkeit wird auch im BSI-Standard 200-1 eingegangen.

Anhand dieser Erkenntnisse kann eine Priorisierung von Zielobjekten für die Risikoanalyse festgelegt werden. In diese Betrachtungen sollten nicht nur die Eigenschaften der Komponenten, sondern auch die im Medizinprodukt ausgeführten Prozesse mit betrachtet werden. Damit wird dem prozessabhängigen Risiko, welches nicht ausschließlich auf der physikalischen Struktur basiert, Rechnung getragen.
Für die Ausführung der Risikoanalyse muss eine geeignete Richtlinie geschaffen werden. Diese muss die folgenden Aspekte berücksichtigen:

- Voraussetzungen für die Notwendigkeit der Risikoanalyse
- Festlegung der Methodik zum Identifizieren, Einschätzen, Bewerten und Behandeln von Risiken
- Anpassung der Methodik auf die speziellen Belange des einzelnen Medizinprodukts
- Festlegung von Kriterien für Risikoakzeptanz
- Festlegung der Verantwortlichkeiten für die Risikoanalyse, hier ist nach DIN EN ISO 14971 Kapitel D.3.2 die Verantwortlichkeit des Herstellers zu beachten,
- Wie ist die Risikoanalyse in den Sicherheitsprozess integriert, sind Nachbesserungen erforderlich
- Wie werden Berichtspflichten umgesetzt
- Ist eine Aktualisierung der Risikobewertung vorgesehen

Zur Betrachtung der Risiken sollte ein Modell des Informationsverbundes erstellt sein, aus welchem die Komponenten und deren Eigenschaften, nebst zugehörigem Datenfluss, erkennbar sind.

Für die Risikoanalyse sind weiter die ISO 13485 und Iso 14971 von Bedeutung. „Die ISO 13485 referenziert die ISO 14971, was bedeutet, dass die Einhaltung der Vorgaben aus ISO 14971 notwendig ist, um die Vorgaben der ISO 13485 zu erfüllen.“[41]
Weiter heißt es in erwähntem Artikel: „Da das Risikomanagement als ein iterativer Prozess während des gesamten Lebenszyklus des Produktes betrachtet werden kann, können die Ausführungserfordernisse erneuert werden, sobald es neue Informationen während des Realisierungsprozess einfließen.“
Die graphische Darstellung des Prozesses, Abbildung 3, wurde in starker Anlehnung an die Darstellung des Autors, Edwin Bills, des hier zitierten Artikels erstellt. Sie stellt dar, dass in die Risikoanalyse nach ISO 14971 alle Risikoanalysen aller verfügbarer Werkzeuge eingehen sollen.

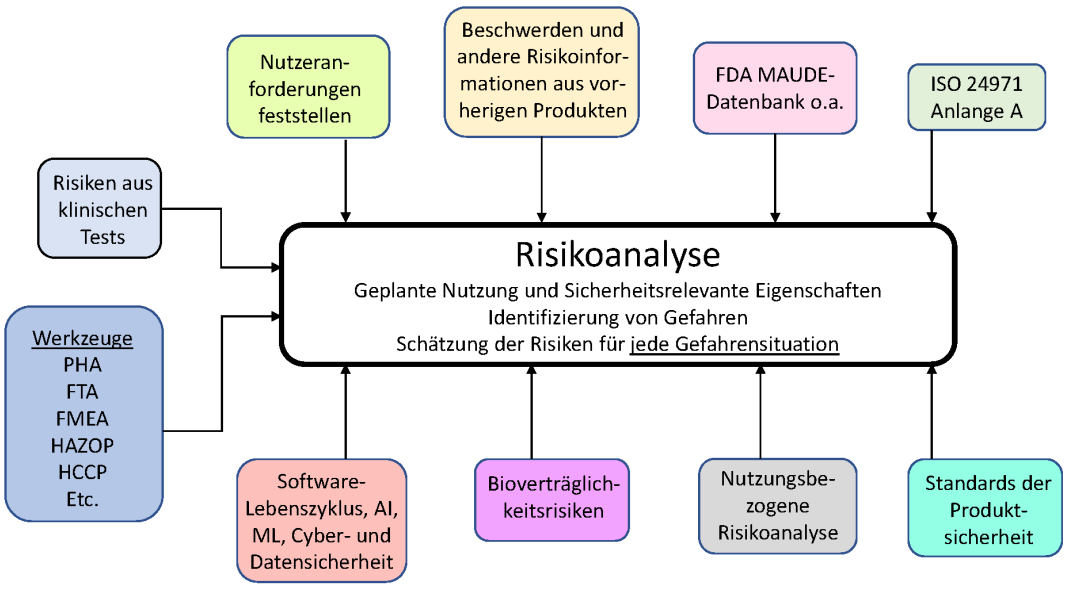

Abbildung 3: In die Risikoanalyse einfließende Risiken nach Edwin Bills[42]

[41] Edwin Bills, Christie Johnson; The Intersection of ISO 13485 And ISO 14971 Under The Proposed FDA QMSR; https://www.meddeviceonline.com/doc/the-intersection-of-iso-and-iso-under-the-proposed-fda-qmsr-0001; Abrufdatum: 04.07.2023
[42] ebenda

6.2 Elementare Gefährdungen

Durch das BSI wurde eine hilfreiche Übersicht der elementaren Gefährdungen gegeben. Es wird hier auch bereits angegeben, für welche der drei Grundwerte diese zutreffen. [43]

Für die Cybersicherheit sind dabei folgende Gefährdungen, vgl. Tabelle 1, von Belang:
Beschriftung:

A (Availability = Verfügbarkeit),
I (Integrity) = Integrität,
C (Confidentiality) = Vertraulichkeit

	Gefährdung	Grundwert
G.0.1	Feuer	A
G.0.2	Ungünstige klimatische Bedingungen	I, A
G.0.3	Wasser	I, A
G.0.4	Verschmutzung, Staub, Korrosion	I, A
G.0.5	Naturkatastrophen	A
G.0.6	Katastrophen im Umfeld	A
G.0.7	Großereignisse im Umfeld	C, I, A
G.0.8	Ausfall oder Störung der Stromversorgung	I, A
G.0.9	Ausfall oder Störung von Kommunikationsnetzen	I, A
G.0.10	Ausfall oder Störung von Versorgungsnetzen	A
G.0.11	Ausfall oder Störung von Dienstleistern	C, I, A
G.0.12	Elektromagnetische Störstrahlung	I, A
G.0.13	Abfangen kompromittierender Strahlung	C
G.0.14	Ausspähen von Informationen / Spionage	C
G.0.15	Abhören	C
G.0.16	Diebstahl von Geräten, Datenträgern und Dokumenten	C, A
G.0.17	Verlust von Geräten, Datenträgern und Dokumenten	C, A
G.0.18	Fehlplanung oder fehlende Anpassung	C, I, A
G.0.19	Offenlegung schützenswerter Informationen	C
G.0.20	Informationen aus unzuverlässiger Quelle	C, I, A

[43] BSI Standard 200-3, Risikoanalyse auf der Basis von IT-Grundschutz, Kapitel 3, www.bsi-bund.de/grund-schutz

G.0 21	Manipulation von Hard- und Software	C, I, A
G.0.22	Manipulation von Informationen	I
G.0.23	Unbefugtes Eindringen in IT-Systeme	C, I
G.0.24	Zerstörung von Geräten oder Datenträgern	A
G.0.25	Ausfall von Geräten oder Systemen	A
G.0.26	Fehlfunktion von Geräten oder Systemen	C, I, A
G.0.27	Ressourcenmangel	A
G.0.28	Softwareschwachstellen oder -fehler	C, I, A
G.0.29	Verstoß gegen Gesetze oder Regelungen	C, I, A
G.0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	C, I, A
G.0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	C, I, A
G.0.32	Missbrauch von Berechtigungen	C, I, A
G.0.33	Personalausfall	A
G.0.34	Anschlag	C, I, A
G.0.35	Nötigung, Erpressung oder Korruption	C, I, A
G.0.36	Identitätsdiebstahl	C, I, A
G.0.37	Abstreiten von Handlungen	C, I
G.0.38	Missbrauch personenbezogener Daten	C
G.0.39	Schadprogramme	C, I, A
G.0.40	Verhinderung von Diensten (Denial of Service)	A
G.0.41	Sabotage	A
G.0.42	Social Engineering	C, I
G.0.43	Einspielen von Nachrichten	C, I
G.0.44	Unbefugtes Eindringen in Räumlichkeiten	C, I, A
G.0.45	Datenverlust	A
G.0.46	Integritätsverlust schützenswerter Informationen	I

Tabelle 1 : Übersicht über die elementaren Gefährdungen mit den jeweils betroffenen Grundwerten[44]

Diese elementaren Gefährdungen werden mit den nachfolgend erläuterten Gefährdungskategorien zur ersten Beurteilung zusammengebracht.

[44] BSI-Standard 200-3, Tabelle 1, www.BSI-Bund.de/grundschutz; Abrufdatum 25.05.2023

6.3 Gefährdungskategorien

Um die tatsächliche Gefährdung zu ermitteln, müssen die potentiellen Gefährdungen für das zu bewertende Zielobjekt einer der drei Kategorien, „direkt relevant“, „indirekt relevant“ oder „nicht relevant“, zugeordnet werden.

Die Kategorien sind im BSI-Standard 200-3 definiert mit:

„

- ‚direkt relevant‘ bedeutet hier, dass die jeweilige Gefährdung auf das betrachtete Zielobjekt einwirken kann und deshalb im Rahmen der Risikoanalyse behandelt werden muss.
- „indirekt relevant“ meint hier, dass die jeweilige Gefährdung zwar auf das betrachtete Zielobjekt einwirken kann, in ihrer potentiellen Wirkung aber nicht über andere (allgemeinere) Gefährdungen hinausgeht. In diesem Fall muss die jeweilige Gefährdung für dieses Zielobjekt nicht gesondert im Rahmen der Risikoanalyse behandelt werden.
- „nicht relevant“ heißt hier, dass die jeweilige Gefährdung nicht auf das betrachtete Zielobjekt einwirken kann und deshalb für dieses Zielobjekt im Rahmen der Risikoanalyse nicht behandelt werden muss.“[45]

6.4 Zusammenführung von Gefährdungen und Gefährdungskategorien

Für jede einzelne der elementaren Gefährdungen kann nun festgestellt werden, ob

- dies für das aktuell betrachtete System relevant ist,
- welche der drei Grundwerte (Verfügbarkeit, Vertraulichkeit und Integrität) davon beeinträchtigt werden könnten,
- in welche Gefährdungskategorie sie gehört (direkt, indirekt, nicht relevant) und
- ob diese Gefährdung bereits in einer der anderen elementaren Gefährdungen eingeschlossen ist (beispielsweise Zerstörung durch *Feuer i*st gegebenenfalls mit der allgemeinen Gefährdung *Ausfall von Geräten oder Systemen* bereits abgedeckt).

[45] BSI Standard 200-3, Risikoanalyse auf der Basis von IT-Grundschutz, Kapitel 4.1; www.bsi-bund.de/grundschutz

6.4.1 Datenblatt einer Komponente mit Gefährdungen, Grundwerten und Relevanz

Für jedes Zielobjekt wird ein Datenblatt[46] erstellt, welches folgende Informationen bereitstellt:

- Name des Zielobjekts,
- Schutzbedarf der drei Grundwerte
- relevante elementare Gefährdungen
- Kommentar

Für die bessere Anschaulichkeit der nachfolgenden Schritte der Risikobewertung wird zur Hilfestellung ein modernes System einer automatischen Insulinpumpe mit Sensor zur Überwachung des Blutzuckers dargestellt.

Das System besteht aus

- Blutzuckersensor mit Transmitter
- Steuerungsgerät
- Insulinpumpe
- Smartphone-App
- Cloudserver-Anbindung

Das Zusammenspiel der Komponenten wurde mit Abbildung 4 grafisch dargestellt.

[46] BSI-Standard 200-3

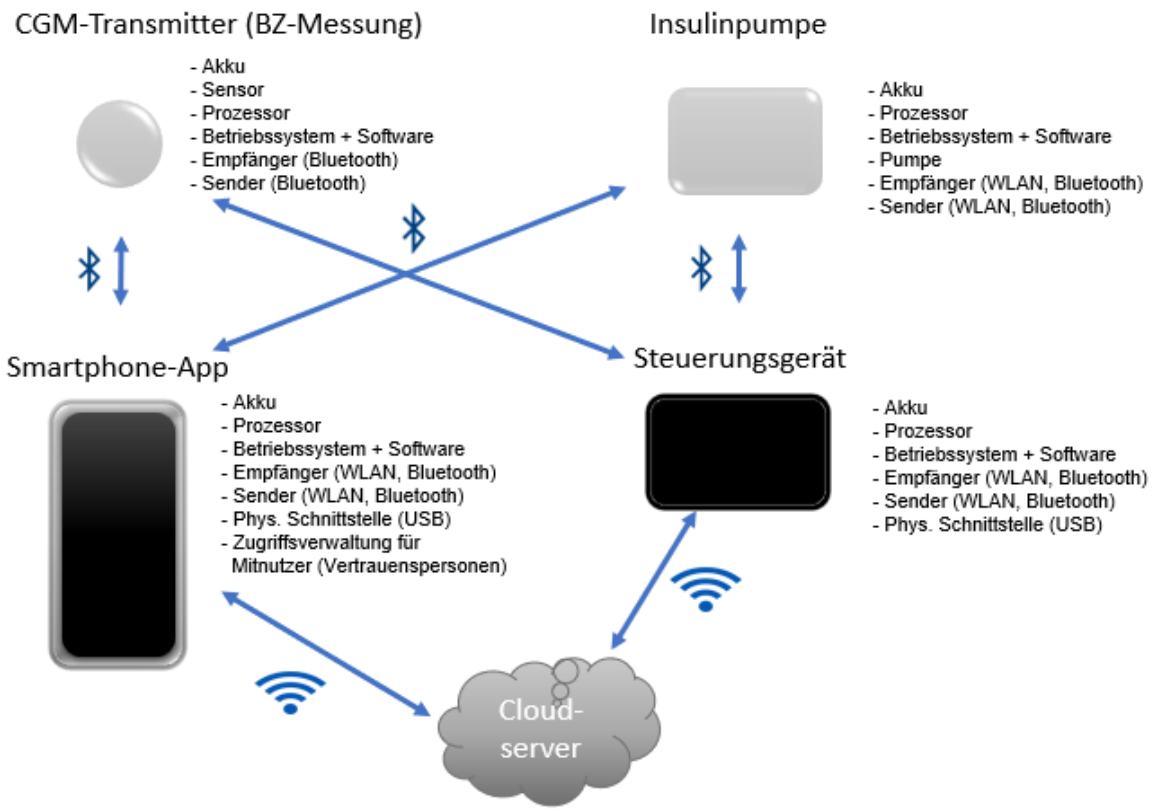

Abbildung 4: Vereinfachter Netzplan automatische Insulinpumpe

Für eine Insulinpumpe könnte das beispielsweise, wie in nachfolgender Tabelle unvollständig dargestellt, aussehen.

Die Tabelle, vgl. Tabelle 2, wurde nach dem Vorschlag in BSI-Standard 200-3, Tabelle 2 für ein Steuerungsmodul einer Insulinpumpe erstellt.

Gefährdung	Grundwerte	Wirkung / Relevanz	Kommentar
G.0.1 Feuer	Verfügbarkeit	Indirekte Wirkung, nicht relevant	Durch G.0.1 *Feuer* kommen, gegenüber G.0.25 *Ausfall von Geräten oder Systemen*, keine neuen sicherheitsrelevanten Gefährdungen hinzu. Daher keine spezifischen Maßnahmen zu treffen.
G.0.14 Ausspähen von	Vertraulichkeit	Indirekte Wirkung, nicht relevant	Die durch G.0.14 Ausspähen von Informationen / Spionage kommen, gegenüber G.0.32 Missbrauch von

Informationen / Spionage			Berechtigungen, keine neuen Gefährdungen hinzu. Daher sind keine spezifischen Maßnahmen zu treffen.
G.0.25	Verfügbarkeit	Direkte Wirkung, relevant	Die Gefährdung durch G.0.25 *Ausfall von Geräten oder Systemen* wirkt direkt auf die Funktion des Steuerungsmoduls der Insulinpumpe ein. Daher sind Maßnahmen gegen G.0.25 *Ausfall von Geräten oder Systemen* zu prüfen.
G.0.32 Missbrauch von Berechtigungen	Vertraulichkeit, Verfügbarkeit, Integrität	Direkte Wirkung, relevant	Die Gefährdung durch G.0.32 *Missbrauch von Berechtigungen* wirkt direkt auf die Funktion des Steuerungsmoduls der Insulinpumpe ein. Daher sind Maßnahmen gegen G.0.32 *Missbrauch von Berechtigungen* zu prüfen.

Tabelle 2: Zusammenstellung nach BSI-Standard 200-3, Tabelle 2; Beispiel Insulinpumpe

Für den Fall, dass die elementaren Gefährdungen nicht das gesamte Gefährdungspotential abdecken, sind diese zusätzlichen Gefährdungen ebenfalls zu ermitteln und aufzustellen, damit auch für diese Maßnahmen getroffen werden können.

6.4.2 Zuordnung von Grundschutzbausteinen nach BSI-Grundschutz zu allen Systemkomponenten

Für die einzelnen Zielobjekte (siehe vereinfachter Netzplan automatische Insulinpumpe) muss festgestellt werden, welche einen hohen oder sehr hohen Schutzbedarf in mindestens einem der Grundwerte (Vertraulichkeit, Integrität, Verfügbarkeit) haben.

Es werden hierzu die IT-Grundschutz-Bausteine des BSI Grundschutz-Kompendiums verwendet.[47]

Auswahl von im BSI IT-Grundschutz-Kompendium benannte Komponenten, welche für die Cybersicherheit von Medizinprodukten bedeutsam sein können:

Software-Entwicklung	CON.8
Informationsaustausch	CON.9
Entwicklung von Webanwendungen	CON.10
Patch- und Änderungsmanagement	OPS.1.1.3
Schutz vor Schadprogrammen	OPS.1.1.4
Protokollierung	OPS.1.1.5
Software-Tests und -Freigaben	OPS.1.1.6
Archivierung	OPS.1.2.2
Fernwartung	OPS.1.2.5
NTP-Zeitsynchronisation	OPS.1.2.6
Cloud-Nutzung	OPS.2.2
Detektion von sicherheitsrelevanten Ereignissen	DER.1
Behandlung von Sicherheitsvorfällen	DER.2.1
Vorsorge für die IT-Forensik	DER.2.2
Audits und Revisionen	DER.3.1
Notfallmanagement	DER.4
Webbrowser	APP.1.2
Mobile Anwendungen (Apps)	APP.1.4
Allgemeiner Verzeichnisdienst	APP.2.1
OpenLDAP	APP.2.3
Webserver	APP.3.2
Fileserver	APP.3.3
Relationale Datenbanken	APP.4.3
Kubernetes	APP.4.4
Microsoft Exchange und Outlook	APP.5.2
Allgemeiner E-Mail-Client und -Server	APP.5.3
Unified Communications und Collaboration (UCC)	APP.5.4
Allgemeine Software	APP.6

[47] BSI Grundschutz-Kompendium; https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html; Abrufdatum 29.05.2023

Entwicklung von Individualsoftware	APP.7
Allgemeiner Server	SYS.1.1
Windows Server 2012	SYS.1.2.2
Windows Server	SYS.1.2.3
Server unter Linux und Unix	SYS.1.3
Virtualisierung	SYS.1.5
Containerisierung	SYS.1.6
IBM Z	SYS.1.7
Speicherlösungen	SYS.1.8
Terminalserver	SYS.1.9
Allgemeiner Client	SYS.2.1
Clients unter Windows	SYS.2.2.3
Clients unter Linux und Unix	SYS.2.3
Clients unter macOS	SYS.2.4
Client-Virtualisierung	SYS.2.5
Virtual Desktop Infrastructure	SYS.2.6
Laptops	SYS.3.1
Allgemeine Smartphones und Tablets	SYS.3.2.1
Mobile Device Management (MDM)	SYS.3.2.2
iOS (for Enterprise)	SYS.3.2.3
Android	SYS.3.2.4
Mobiltelefon	SYS.3.3
Drucker, Kopierer und Multifunktionsgeräte	SYS.4.1
Eingebettete Systeme	SYS.4.3
Allgemeines IoT-Gerät	SYS.4.4
Wechseldatenträger	SYS.4.5
Prozessleit- und Automatisierungstechnik	IND.1
Allgemeine ICS-Komponente	IND.2.1
Speicherprogrammierbare Steuerung (SPS)	IND.2.2
Sensoren und Aktoren	IND.2.3
Maschine	IND.2.4
Safety Instrumented Systems	IND.2.7
Fernwartung im industriellen Umfeld	IND.3.2
Netzarchitektur und -design	NET.1.1
Netzmanagement	NET.1.2
WLAN-Betrieb	NET.2.1

WLAN-Nutzung	NET.2.2
Router und Switches	NET.3.1
Firewall	NET.3.2
VPN	NET.3.3
Network Access Control	NET.3.4
TK-Anlagen	NET.4.1
VoIP	NET.4.2
Faxgeräte und Faxserver	NET.4.3
Verkabelung	NF.12
Technisches Gebäudemanagement	INF.13
Gebäudeautomation	INF.14

Weitere Informationen zu ausgewählten Komponenten aus dem BSI-Grundschutz-Kompendium wurden in Anlage, Teil 2 zu dieser Arbeit angefügt.

Anwendung am Beispiel Insulinpumpe

Dieser hohe oder sehr hohe Schutzbedarf wurde für alle Komponenten des Systems Insulinpumpe festgestellt, vgl. Tabelle 3.

- Sensor mit Transmitter
- Steuergerät
- Insulinpumpe
- Smartphone-App
- Cloudserver

Nummer	Titel des Bausteins	Zielobjekt
IND.2.3	Sensoren und Aktoren	Sensor mit Transmitter
IND.1	Prozessleit- und Automatisierungstechnik	Steuergerät
IND.2.4	Maschine	Insulinpumpe
SYS.3.3	Mobiltelefon	Smartphone-App
OPS.2.2	Cloud-Nutzung	Cloudserver

Tabelle 3: Systemkomponenten mit hohem oder sehr hohem Schutzbedarf und zugehörige IT-Grundschutz-Bausteine, Beispiel Insulinpumpe

Anmerkung: Maschine ist die nach Ansicht des Verfassers passendste Komponente aus dem IT-Grundschutzkompendium mit ihrer Definition: „Eine Maschine ist eine technische Vorrichtung, die automatisierte Aufgaben durchführt.“[48]
Die Insulinpumpe gibt automatisiert (ohne Zutun des Patienten, auch unabhängig vom Kontakt zum Steuergerät) Insulin durch Pumpen in das Gewebe des Patienten.

6.4.3 Datenblatt von Systemkomponenten mit allen relevanten elementaren Gefährdungen

Zu jeder Komponente, für welche in vorstehender Tabelle ein hoher oder sehr hoher Schutzbedarf festgestellt wurde, wird nun mit einem neuen Datenblatt dargestellt, welcher Grundwert einen hohen Schutzbedarf hat und welche der elementaren Gefährdungen dabei eine Rolle spielen. Vgl. Tabelle 4

Steuergerät
Vertraulichkeit: hoch Integrität: hoch Verfügbarkeit: hoch
G 0.9 Ausfall oder Störung von Kommunikationsnetzen
G 0.12 Elektromagnetische Störstrahlung
G 0.14 Ausspähen von Informationen / Spionage
G 0.19 Offenlegung schützenswerter Informationen
G 0.21 Manipulation von Hard- und Software
G 0.22 Manipulation von Informationen
G 0.23 Unbefugtes Eindringen in IT-Systeme
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen
G 0.31 Missbrauch von Berechtigungen
G 0.38 Missbrauch personenbezogener Daten
G 0.39 Schadprogramme
G 0.40 Verhinderung von Diensten (Denial of Service)
G 0.41 Sabotage
G 0.45 Datenverlust

[48] BSI IT-Grundschutzkompendium, IND.2.4 Maschine, 1.1. Einleitung

G 0.46 Integritätsverlust schützenswerter Informationen
G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe

Tabelle 4; Datenblatt Schutzbedarf und elementaere Gefährdungen

Nun ist es möglich, dass alle Gefährdungen für die betrachtete Systemkomponente untersucht und geprüft werden können.

6.4.4 zusätzliche Gefährdungen

Es ist möglich, dass es für das betrachtete Medizinprodukt zusätzliche Gefährdungen gibt, welche nicht in den Richtlinien aufgeführt wurden. In dem Fall sind auch diese aufzulisten, wie die elementaren Gefährdungen zu untersuchen, zu bewerten und, wenn notwendig, zu behandeln.

Die Aufstellung könnte, in Anlehnung an BSI-Standard 200-3, für das Beispiel Sensor der Insulinpumpe, wie folgt, vgl. Tabelle 5, aussehen.

Sensor mit Transmitter
G.z.1 Manipulation der Kalibrierungseinstellungen
Kalibrierungen werden mittels Messflüssigkeiten durchgeführt. Durch fehlerhafte Anwendung oder vorsätzliche Änderung der Konzentration oder Zusammensetzung der zur Kalibrierung des Sensors verwendeten Chemikalien kann ein falscher Basiswert in die Software für die künftig auszuführenden Messungen eingetragen werden. Damit ist die Software mit einem falschen Basiswert versehen, welche alle künftigen Messungen bis zur erneuten Kalibrierung mit einem systemischen Fehler ausgibt. Diese zusätzliche Gefährdung ergänzt die elementaren Gefährdungen G.0.21 Manipulation von Hard- und Software und G.0.22 Manipulation von Informationen.
u.s.w.

Tabelle 5: zusätzliche elementare Gefährdungen, Beispiel[49]

[49] nach BSI-Standard 200-3

6.5 Risikoeinstufung

Für eine Risikoeinstufung bedarf es der Kenntnis zur möglichen Schadenshöhe und der Wahrscheinlichkeit / Häufigkeit, dass der Schaden eintritt.

Für IT-Anlagen ist die Schadenshöhe durch den Betreiber („Institution“) zu ermitteln. Bei Medizinprodukten ist diese Einschätzung schwieriger, da die Umgebung des künftigen Einsatzgebietes nur grob gefasst werden kann. Im Gegensatz zu den IT-Anlagen, wie sie im Regelfall zur Anwendung kommen, entstehen bei Medizinprodukten andere Schadenspotentiale, bis zur Gefährdung von Menschenleben. Diese sind in die Betrachtung einzubeziehen.

6.5.1 Grundlagen der Risikoeinstufung

Für die Schadenshäufigkeit darf die Einschätzung nur durch geeignetes Fachpersonal erfolgen. Sie ist zu schätzen. Dabei können Erfahrungen und Statistiken zur Unterstützung herangezogen werden. Da solche Erfahrungswerte oft fehlen, kann mit qualitativen Kategorien gearbeitet werden.

Neben den elementaren Gefährdungen sind auch Fehler als Ursache für Gefährdungssituationen zu berücksichtigen. [50]

Bei den Fehlern selber muss man zwischen
- Zufallsfehlern und
- systematischen Fehlern

unterscheiden.

Zur Feststellung der sicherheitsrelevanten Eigenschaften des Medizinprodukts sind nach DIN EN ISO 14971, Anhang C die Antworten auf folgende Fakten, reduziert auf die für die Cybersicherheit möglicherweise relevanten, wichtig:

[50] DIN EN ISO 14971, Kapitel D.2.2

1. Zweckbestimmung des Gerätes
   a. Krankheit
      - Erkennung
      - Verhütung
      - Überwachung
      - Behandlung
      - Linderung
   b. Kompensierung von Verletzung oder Behinderung
   c. Ersatz oder Veränderung des anatomischen Aufbaus
   d. Empfängnisregelung

2. Informationen zur Anwendung
   - Anwendung mit Kontakt zum Patienten, Dauer des Kontakts ist anzugeben
     - oberflächlicher Kontakt
     - invasiv
     - implantiert
   - Werkstoffe, Bauteile, die mit dem Medizinprodukt angewendet werden oder in Berührung kommen
     - Verträglichkeit mit Substanzen
     - Verträglichkeit mit Geweben und Körperflüssigkeit
     - sind sicherheitsrelevante Eigenschaften bekannt
     - Herstellung unter Verwendung von Stoffen tierischen Ursprungs
   - Wird dem Patienten Energie zugeführt oder entzogen
     - Energieart
     - Steuerung, Qualität, Quantität und Dauer energetischer Einflüsse
     - sind die Energieniveaus höher als bei aktuell ähnlichen Geräten
   - Werden dem Patienten Substanzen zugeführt oder entzogen
     - Stoffe, die zugeführt oder entzogen werden
     - Einzelsubstanz oder eine Reihe von Substanzen
     - Steuerung der Übertragung
     - maximale und minimale Übertragungsarten
   - Bearbeitet das Produkt biologische Substanzen zur anschließenden Wiederverwendung, Transfusion oder Transplantation
     - Art des Prozesses
     - zu bearbeitende Substanzen
   - Soll das Medizinprodukt die Umgebung des Patienten verändern

  - Temperatur
  - Feuchtigkeit
  - Zusammensetzung des atmosphärischen Gases
  - Luftdruck
  - Lichtverhältnisse
- Werden Messungen vorgenommen
  - gemessene Variablen
  - Genauigkeit / Präzision der Messergebnisse
- liefert das Produkt interpretierbare Aussagen
  - liefert das Medizinprodukt Schlussfolgerungen aus eingegebenen oder erfassten Daten
  - Welche Algorithmen und Vertrauensbereich
  - Was passiert bei unbeabsichtigten Anwendungen von Daten oder Algorithmen
- Ist das Medizinprodukt für die Verwendung mit anderen Medizinprodukten, Medikamenten oder sonstiger Medizintechnik vorgesehen
  - Medizinprodukte
  - Medikamente
  - sonstige Produkte
  - mögliche Probleme oder Wechselwirkungen
- Unerwünschte Abgaben Stoffe/Energie
  - energetische Faktoren
    - Geräusche
    - Schwingungen
    - Wärme
    - Strahlungen (ionisierend, nichtionisierend)
    - UV-Strahlung, sichtbares Licht oder Infrarotstrahlung
    - Kontakttemperaturen
    - Leckströme
    - elektrische oder magnetische Felder
  - stoffliche Faktoren
    - Substanzen von Herstellung, Reinigung oder Prüfung, die im Produkt verbleiben und physiologische Auswirkungen
    - Freisetzung von Chemikalien, Abfallprodukten oder Körperflüssigkeiten
- Beeinflusst das Medizinprodukt die Umwelt
  - Auswirkung auf Strom- und Kühlmittelversorgung
  - Abgabe toxischer Substanzen

  - Erzeugung elektromagnetischer Störungen
- Wartung / Kalibrierung erforderlich
  - Wartung oder Kalibrierung durch
    - Bediener
    - Anwender
    - Fachmann
  - sind dazu besondere Substanzen oder Werkzeuge erforderlich
- Ist Software enthalten
  - Installation, Verifizierung, Änderung oder Austausch der Software durch
    - Bediener
    - Anwender
    - Fachmann
- Benötigt die Installation eine Spezialausbildung oder spezielle Fertigkeiten
- Wie werden die Angaben für eine sichere Verwendung zur Verfügung gestellt
  - Angaben direkt an Anwender oder über Dritte (Apotheker, Fachkräfte etc.)
  - Inbetriebnahme und Übergabe an Anwender und ob Installation ohne besondere Fähigkeiten durchgeführt werden kann
  - ist aufgrund der Lebensdauer eine erneute Ausbildung / Zertifizierung von Bedienern oder Wartungspersonal notwendig
- Neue Techniken oder Prozesse in der Herstellung erforderlich
- Hängt die erfolgreiche Anwendung von menschlichen Faktoren ab, z.B. Schnittstelle für den Anwender
- Können Gestaltungsmerkmale der Schnittstelle zum Anwender zu Fehlern bei der Anwendung beitragen
- Gibt es eine Schnittstelle für die Steuerung
  - Fehler durch Versehen in der Anwendung
  - Fehler durch falsche Gruppierung, Codierung, Einschaltrichtung etc.
- Zeigt das Gerät Informationen an
  - Sichtbarkeit, Anordnung
  - Klarheit der Angaben, Einheiten, Farbkodierungen, Zugänglichkeit
- Gibt es eine Menüsteuerung
  - Komplexität
  - Statusanzeige
  - Navigationsverfahren
  - Probleme bei Speicherung
  - Auswirkung bei Abweichung von der regelrechten Bedienung

- Anwendung durch Personen mit besonderen Bedürfnissen
  - Berücksichtigung geistiger und körperlicher Fähigkeiten
  - Ergonomie
  - Unterstützung notwendig
  - Berücksichtigung unterschiedlichen kulturellen Hintergrunds
- Kann die Schnittstelle Tätigkeiten des Anwenders einleiten
- Hat das Medizinprodukt ein Alarmsystem
- Wie kann das Produkt vorsätzlich falsch angewendet werden
- Speichert das Medizinprodukt Daten, die für die Versorgung des Patienten entscheidend sind[51]

6.5.2 Vorgehen bei schwer einzuschätzenden Wahrscheinlichkeiten

Insbesondere die Wahrscheinlichkeit des Auftretens systematischer Fehler ist schwierig einzuschätzen. Daher muss ein breiter Bereich für die Wahrscheinlichkeit angesetzt werden.

Weitere Beispiele für schwer einschätzbare Risiken sind:
- Versagen der Software
- Sabotage oder unbefugte Anwendung
- neue oder schwierig zu verstehende Gefährdungen (z.B. Übertragung neuer Erreger)
- toxikologische Gefährdungen mit Unmöglichkeit der Festlegung von Expositionsgrenzwerten.

Fehlen jegliche Daten zur Einschätzung der Wahrscheinlichkeit des Auftretens eines Schadens ist das Risiko allein auf der Grundlage der Art des Schadens zu bewerten.

Üblicherweise geht man von einer umgekehrten Beziehung von Exaktheit bei Gestaltung und Entwicklung zu Wahrscheinlichkeit eines unentdeckten Einschleppens von systematischen Fehlern aus.
Das bedeutet, dass je schlimmer die Auswirkungen, desto geringer sollte die Wahrscheinlichkeit sein und daher sollte die Exaktheit des Entwicklungsverfahrens umso höher sein.

[51] Auszug aus DIN EN ISO 14971, Anhang C

6.5.3 Bestimmung des Schweregrads

Für die Einschätzung des Schweregrads sind vom Hersteller geeignete Deskriptoren zu verwenden. Es sind sowohl verbale als auch symbolische Niveaustufen möglich, jedoch sind beide ausreichend zu definieren.
Dazu sind auch die Anwendungsbedingungen, für welche die Schweregrade gelten, zu wählen und zu begründen.

Wenn ein Schaden aufgrund eines auftretenden Fehlers entstehen kann, ist die Wahrscheinlichkeit des Auftreten des Fehlers nicht die des Eintritts des Schadens. Nicht jede Gefährdungssituation zieht zwingend den maximal möglichen Schaden nach sich. Daher kann es sinnvoll sein, beide Wahrscheinlichkeiten getrennt zu ermitteln und dann zusammen zu führen.

Auf den Vorgang der Risikoeinschätzung wird ausführlich im BSI-Standard 200-3 eingegangen, jedoch ist die in der DIN EN ISO 14971 vorgegebene Vorgehensweise für Medizinprodukte nicht nur vorgesehen, sondern auch passender.

In der DIN EN ISO 14971 wurde u.a. folgende geeignete Beispiele für die Schweregrade gegeben (vgl. Tabellen 6 und 7):

Qualitative Schweregrade:

Übliche Begriffe	**Mögliche Beschreibung**
Katastrophal	Führt zum Tod des Patienten
Kritisch	Führt zu dauernder Behinderung oder einer lebensbedrohlichen Schädigung
Ernst	Führt zu einer Schädigung oder Behinderung, die ein sachkundiges medizinisches Eingreifen erfordert
Gering	Führt zu einer zeitweiligen Schädigung oder Behinderung, die kein sachkundiges medizinisches Eingreifen erfordert
Vernächlässigbar	Unannehmlichkeiten oder zeitweilige Beschwerden

Tabelle 6: Beispiel von fünf qualitativen Schweregraden[52]

[52] nach DIN EN ISO 14971, Tabelle D.3

Halbquantitative Schweregrade:

Übliche Begriffe	Mögliche Beschreibung
Häufig	$\geq 10^{-3}$
Wahrscheinlich	$< 10^{-3}$ und $\geq 10^{-4}$
Gelegentlich	$< 10^{-4}$ und $\geq 10^{-5}$
Fernliegend	$< 10^{-5}$ und $\geq 10^{-6}$
Unwahrscheinlich	$< 10^{-6}$

Tabelle 7: Beispiel halbquantitativer Wahrscheinlichkeitsniveaus[53]

6.5.4 Risikomatrix

Risikomatrix: Pro Dimension sollten nicht mehr als fünf Kategorien gewählt werden[54]

„Bei der klassischen Risikoanalyse berechnet sich das Risiko aus der Schadenshöhe multipliziert mit der Eintrittswahrscheinlichkeit.“[55]

Die EN ISO 14971:2019 ermöglicht zusätzlich noch die Ermittlung einer Eintrittswahrscheinlichkeit (P) aus einer Kombination des Eintretens einer Gefährdungssituation (P_1) und einer Wahrscheinlichkeit, dass eine solche Situation auch zu einem Schaden (P_2) führt.
Diese Zerlegung ist nicht obligatorisch, kann im Einzelfalle jedoch hilfreich sein.

In der EN ISO 14971:2019 wurde dazu eine Grafik erstellt, welche bildhaft den Zusammenhang zwischen Gefährdung, Abfolge von Ereignissen, Gefährdungssituation und Schaden darstellt. Diese ist hier als Abbildung 5 in strenger Anlehnung an das Original abgebildet:

[53] nach DIN EN ISO 14971, Tabelle D.4
[54] BSI-Standard 200-1, 8.1 Erstellung des Sicherheitskonzepts
[55] BSI-Standard 200-1, 10.2.1 Integrierte Risikobewertung im IT-Grundschutz

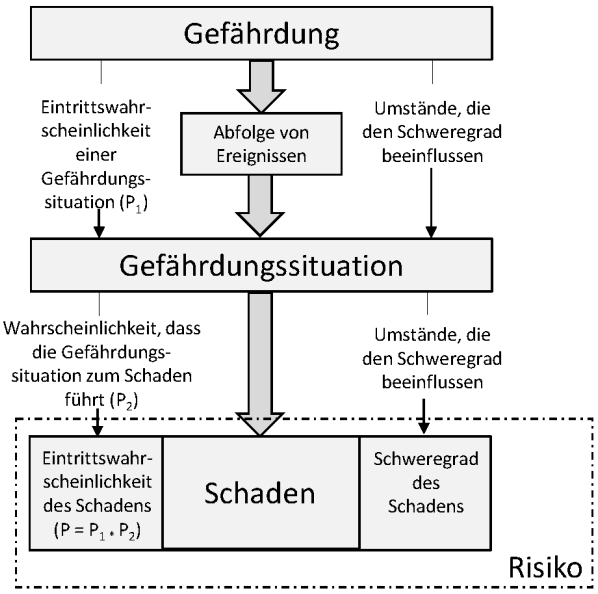

Abbildung 5: Zusammenhang zwischen Gefährdung, Abfolge von Ereignissen, Gefährdungssituation und Schaden[56]

Aus diesen Dimensionen Eintrittswahrscheinlichkeit und Schadenshöhe wird eine Risikomatrix erstellt, siehe Tabelle 8. Für diese Matrix ist dann festzulegen, welche Bereiche als niedriges, mittleres oder hohes Risiko einzuschätzen sind.

Für Medizinprodukte ergibt sich hier eine Abweichung von dieser Verfahrensweise dahingehend, dass nicht drei Risikostufen festgelegt werden, sondern nur zwei:

- vertretbares Risiko
- nicht vertretbares Risiko

	Vernachlässigbar	**Gering**	**Ernst**	**Kritisch**	**Katastrophal**
Häufig					
Wahrscheinlich	R_1	R_2			
Gelegentlich		R_4		R_5	R_6
Fernliegend					
Unwahrscheinlich			R_3		

Tabelle 8: Beispiel einer halbquantitativen Matrix zur Risikobewertung[57]

[56] nach EN ISO 14971:2019, Bild C.1
[57] nach DIN EN ISO 14971, Bild D.3

	Vernach-lässigbar 1	Gering 2	Ernst 3	Kritisch 4	Katastrophal 5
Häufig 5	5	10	15	20	25
Wahrscheinlich 4	4	8	12	16	20
Gelegentlich 3	3	6	9	12	15
Fernliegend 2	2	4	6	8	10
Unwahrscheinlich 1	1	2	3	4	5

Tabelle 9: Risikomatrix 5x5 mit Feldwerten

Diese anhand der Matrix ermittelte Risikowerte, vgl. Tabelle 9, gehen in die Übersicht für das jeweils zu betrachtende Zielobjekt ein.
Diese ist die Grundlage der Bewertung des Risikos und der zur Abwehr getroffenen Maßnahmen.

6.5.5 Risikobewertung und Risikoakzeptanz

Die DIN EN ISO 14971 legt keine vertretbaren Risiken fest. Diese Entscheidung wird dem Hersteller überlassen.

Dieses kann mit Hilfe von

- weitere Normen, deren Durchsetzung eine Akzeptanz bestimmter Risiken bedeutet
- Vergleich mit offenkundigen Risikograden von Medizinprodukten, welche bereits in Gebrauch sind
- Daten aus klinischen Studien, besonders bei neuen Techniken oder Zweckbestimmungen

erfolgen.

Dieses erfolgt unter Beachtung des Standes der Technik zum Zeitpunkt der Produktgestaltung. Dabei können unterschiedliche Verfahren zur Bestimmung verwendet werden. Geeignet sind beispielsweise:

- für das gleiche Produkt oder ähnliche Produkte verwendete Normen
- beste Praxis, wie bei Produkten gleichen oder ähnlichen Typs
- Ergebnisse anerkannter wissenschaftlicher Forschung

Nach ISO 14971, Kapitel D.4 werden Risiken in vertretbare und nicht vertretbare Risiken unterteilt. Dazu kann die Risikomatrix als ein Weg zur Darstellung gewählt werden.

	Vernach-lässigbar	**Gering**	**Ernst**	**Kritisch**	**Katastrophal**
Häufig					
Wahrscheinlich	R_1	R_2			
Gelegentlich		R_4		R_5	R_6
Fernliegend					
Unwahrscheinlich			R_3		

Tabelle 10: Qualitative Schweregrade[58]

Legende: Nicht vertretbares Risiko

Vertretbares Risiko

Bei diesem Matrix-Beispiel wurden alle Risiken, welche einen Feldwert < 10 haben, als akzeptabel eingestuft.

Diese Einstufung und Abschätzung hat in der Praxis durch den Hersteller zu erfolgen.

Es ist dennoch wichtig, dass eine Einschätzung getroffen wird, welche unvermeidbaren Risiken akzeptabel sind.

Für jede Komponente aus dem Netzplan des Medizingeräts kann nun für jede der elementaren Gefährdungen eine Auswertung erfolgen.

Dazu eignet sich das im BSI-Standard 200-3 vorgeschlagene Datenblatt zur Risikoeinstufung.

[58] nach DIN EN ISO 14971, Bild D.5

<table>
<tr><td colspan="3">Steuergerät
Vertraulichkeit: hoch
Verfügbarkeit: hoch
Integrität: hoch</td></tr>
<tr><td colspan="2">Gefährdung:
G 0.31 Missbrauch von Berechtigungen</td><td>Beeinträchtigte Grundwerte:
Vertraulichkeit, Verfügbarkeit, Integrität</td></tr>
<tr><td>Eintrittshäufigkeit ohne zusätzliche Maßnahmen: unwahrscheinlich</td><td>Auswirkungen ohne zusätzliche Maßnahmen:
Kritisch</td><td>Risiko ohne zusätzliche Maßnahmen:
Vertretbar</td></tr>
<tr><td colspan="3">Beschreibung:
Das Steuergerät kann sowohl direkt, als auch über die zugehörige Smartphone-App bedient werden. Dieses kann sowohl über eine WLAN-Schnittstelle, als auch über Bluetooth-Schnittstelle erfolgen.
Die Zuweisung der Berechtigungen für Nutzer kann über einen Administrator-Zugang eingerichtet werden. Dieses erfolgt über einen lizenzierten Händler des Medizinprodukts.
Das Nutzerkonto für den Patienten kann keine weiteren Nutzerkonten anlegen oder Berechtigungen ändern.
Der Login erfolgt über Patientennamen und Passwort, beides ist verschlüsselt abgelegt.
Vom Patienten sind notwendige persönliche Daten hinterlegt, wie Geburtsdatum, Geschlecht, Gewicht und Nutzungsdaten zur Analyse des Blutzuckerstoffwechsels für eine optimierte, automatisierte Anpassung der Parameter.
Einige Parameter des Nutzerkontos können über die Smartphone-App eingestellt werden, beispielsweise aktuelle Ernährung und geplante physische Aktivitäten.
Der Administrator-Login wird mit allen Aktivitäten, einschließlich der Identität der Konfigurierungssoftware, geloggt.
Die Bedienung durch die Nutzer-App ist von der Überwachungssoftware getrennt. Der Zugang erfolgt über Login und automatischen Logout nach festgelegter Zeit.
Ein Missbrauch von Berechtigungen ist an zwei Punkten möglich:
- Benutzung der Bedienwerkzeuge per Smartphone-App (auch bei den als Vertrauenspersonen eingestellten weiteren Smartphones, insgesamt 5 App-Zugänge) durch eine nicht autorisierte Person. Dadurch könnte beispielsweise eine geplante, aber nicht getätigte, über das Normalmaß zuckerhaltige Mahlzeit eingetragen werden, welche mit dem notwendigen Vorlauf eine zu hohe Insulinmenge freigibt, was zu einer gefährlichen Unterzuckerung führen kann.</td></tr>
</table>

- Missbräuchliche Nutzung des Administratorkontos und Änderung der hinterlegten Patientendaten. Dadurch kann eine zu hohe oder zu geringe Insulinausschüttung durch systemischen Fehler ausgelöst werden. **Bewertung:** Das Steuergerät ist vor missbräuchlichem Zugriff zu sichern. Dazu ist der Zugriff nur nach Authentifikation möglich. Für die Konfiguration bedarf es eines direkten physischen Zugangs, welcher nur über die Software des Herstellers und Authentifikation des Bedieners der Software möglich ist. Die Nutzereinstellungen können direkt am Gerät vorgenommen werden, dazu muss sich der Nutzer einloggen. Nach einer festgelegten Zeit wird der Nutzer ausgeloggt und das Konfigurationsmenü verlassen. Die Smartphone-Apps werden über den Server des Herstellers authentifiziert. Dazu müssen diese mit dem Internet und dem Server verbunden sein. Nur über diesen ist ein Einloggen in die Konfiguration möglich. Diese wird mitgeloggt. Die Apps empfangen auch Warnmeldungen zum Blutzuckerstand. Für die daraus resultierenden Notwendigkeiten sind feste Routinen hinterlegt, welche durch die App-Nutzer ausgelöst werden können. Pro Warnmeldung kann nur einmal eine Aktion ausgelöst werden. Damit konnte die Wahrscheinlichkeit für den Missbrauch von Berechtigungen für das Steuergerät als „unwahrscheinlich“ eingeschätzt werden. Trotz „kritischer“ Auswirkungen ist damit das Gesamtrisiko „vertretbar“.

Tabelle 11: Risikobehandlung für ein fiktives Steuergerät, mit Zusatztexten[59]

Die Texte für Beschreibung und Bewertung sind entsprechend BSI-Standard 200-3 optional, da mitunter sehr viele Komponenten darzustellen sind. Sie dienen dazu, das Ergebnis der Bewertung nachvollziehbar zu machen.

Wenn es sich bei den Maßnahmen der Absicherung um solche handelt, welche aus dem IT-Grundschutz-Kompendium abgeleitet wurden, ist eine Darstellung des Risikos ohne diese Zusatztexte, wie folgend in Tabelle 12 dargestellt, ausreichend.

[59] nach BSI-Standard 200-3

Steuergerät Vertraulichkeit: hoch Verfügbarkeit: hoch Integrität: hoch		
Gefährdung: G 0.31 Missbrauch von Berechtigungen	Beeinträchtigte Grundwerte: Vertraulichkeit, Verfügbarkeit, Integrität	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: unwahrscheinlich	Auswirkungen ohne zusätzliche Maßnahmen: Kritisch	Risiko ohne zusätzliche Maßnahmen: Vertretbar

Tabelle 12: Risikobehandlung für ein fiktives Steuergerät, Kurzform[60]

Auf diese Weise ist es möglich, die Risiken für Komponenten auch für mehrere elementare Gefährdungen in einer Tabelle zusammenzufassen.

Steuergerät Vertraulichkeit: hoch Verfügbarkeit: hoch Integrität: hoch		
Gefährdung: G 0.31 Missbrauch von Berechtigungen	Beeinträchtigte Grundwerte: Vertraulichkeit, Verfügbarkeit, Integrität	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: unwahrscheinlich	Auswirkungen ohne zusätzliche Maßnahmen: Kritisch	Risiko ohne zusätzliche Maßnahmen: **Vertretbar**
Gefährdung: G 0.19 Offenlegung schützenswerter Informationen	Beeinträchtigte Grundwerte: Vertraulichkeit	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: unwahrscheinlich	Auswirkungen ohne zusätzliche Maßnahmen: Gering	Risiko ohne zusätzliche Maßnahmen: **Vertretbar**
u.s.w.		

Tabelle 13: Datenblatt mit mehreren elementaren Gefährdungen[61]

[60] nach BSI-Standard 200-3
[61] ebenda

6.6 Risikobehandlung

Die Risikobehandlung wird durch den Hersteller durchgeführt und dokumentiert. Sie wird zwar nicht durch die Benannte Stelle ausgeführt, liefert aber die Grundlage für den Zertifizierungsprozess.
Die Risikobehandlung, welche zum Zeitpunkt der Antragstellung vorliegt, muss nach Verordnung (EU) 2017/745, Kapitel VII „ÜBERWACHUNG NACH DEM INVERKEHRBRINGEN, VIGILANZ UND MARKTÜBERWACHUNG“ weitergeführt werden (Risikobeobachtung).

Die Benannte Stelle hat zu überprüfen, ob die Risikobehandlung in notwendigem Maße stattgefunden hat und für das Produkt geeignete Maßnahmen etabliert wurden.
Die Herausforderung liegt in der Einschätzung der Maßnahmen.
Die Konformität bezieht sich immer auf den Zeitpunkt der Ausstellung der Bescheinigung und die zu diesem Zeitpunkt vorliegenden Dokumentationen zum Produkt, daher ist diese auch nur befristet zu vergeben und kann unter Umständen durch die Behörden auch entzogen werden.

In der ersten Risikoeinstufung kann es passieren, dass das Ergebnis „nicht vertretbar“ ausfällt.
Für ein solches Ergebnis ist für die entsprechende Komponente dann eine Risikobehandlungsoption auszuwählen:

- vermeiden
- reduzieren
- transferieren
- akzeptieren[62]

Das Akzeptieren eines Risikos ist dann sinnvoll, wenn in der Risiko-Nutzen-Bewertung der Nutzen das Risiko überwiegt und keine weitere Reduktion oder ein Vermeiden des Risikos möglich ist (Risiko-Nutzen-Analyse). Das wäre beispielsweise der Fall, wenn Patienten ohne das Medizingerät keine Überlebenschance hätten, jedoch mit dem Gerät eine Überlebenschance von 50 % entstehen würde. Damit ist das Risiko des Versterbens von Patienten akzeptabel.

[62] BSI-Standard 200-3

6.7 Risiko-Nutzen-Analyse

Eine Risiko-Nutzen-Analyse liefert die Berechtigung für ein Risiko, nachdem alle praktisch durchführbaren Maßnahmen zur Verringerung des Risikos angewendet wurden und das Risiko noch immer nicht als vertretbar eingestuft werden konnte.
Durch die Risiko-Nutzen-Analyse wird festgestellt, ob der Nutzen das Risiko überwiegt.
Es gibt keinen genormten Ansatz zur Bewertung des Nutzens.

6.8 Risikobeobachtung

Es ist generell sinnvoll, Risiken zu beobachten und dafür Register und Verzeichnisse anzulegen.
In der Verordnung (EU) 2017/745 [63] wurde die Pflicht geschaffen, bei Feststellung, dass eine Konformität im Sinne der Verordnung nicht (mehr) gegeben ist, die Konformität unverzüglich herzustellen oder das Produkt vom Markt zu nehmen.
Sollte von dem Produkt eine schwerwiegende Gefahr ausgehen, besteht eine unverzügliche Informationspflicht des Herstellers gegenüber Behörden und der Benannten Stelle, welche für das Produkt die Bescheinigung ausgestellt hat und informiert mit Angaben zur Nichtkonformität und den ergriffenen Korrekturmaßnahmen.
Weiter sind die Hersteller verpflichtet, ein Meldesystem zu Vorkommnissen und Sicherheitskorrekturmaßnahmen vorzuhalten.
Dazu hat der Hersteller jedes Gerät mit einer UDI, einem Kennzeichen zur eindeutigen Identifikation des Medizingeräts, auszustatten.
Die Informationspflicht gegenüber den Behörden ist in der Medizinprodukte-Anwendermelde- und Informationsverordnung MPAMIV vom 21.04.2021 festgelegt. [64]
Demnach ist jedes „mutmaßliches schwerwiegendes Vorkommnis“ den jeweils zuständigen Bundesoberbehörden zu melden.
Solche Vorkommnisse sind diejenigen, bei denen nicht ausgeschlossen ist, dass diese auf

- einer unerwünschten Nebenwirkung des Produkts,
- einer Fehlfunktion,

[63] Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017
[64] Verordnung, „Verordnung über die Meldung von mutmaßlichen schwerwiegenden Vorkommnissen bei Medizinprodukten sowie zum Informationsaustausch der zuständigen Behörden“, Ausfertigungsdatum 21.04.2021. [Online] https://www.gesetze-im-internet.de/mpamiv/MPAMIV.pdf (Abrufdatum 26.05.2023)

- einer Verschlechterung der Eigenschaften oder der Leistung eines Produkts,
- Anwendungsfehlern aufgrund ergonomischer Merkmale,
- Unzulänglichkeit der vom Hersteller bereitgestellten Informationen

beruhen und das direkt oder indirekt eine der nachstehenden Folgen hatte oder hätte haben können:

- Tod eines Patienten, Anwenders oder anderer Person,
- vorübergehende oder dauerhafte schwerwiegende Verschlechterung des Gesundheitszustandes eines Patienten, Anwenders oder anderen Person,
- schwerwiegende Gefahr für die öffentliche Gesundheit.

6.9 Relevanz der Risikoanalyse für das Konformitätsverfahren

In der DIN EN ISO 14971 Anhang ZA gibt es einen Absatz „Verfahren zur Konformitätserklärung“.

Diese besagt, dass die Norm zur Unterstützung der folgenden Verfahrensbestandteile verwendet werden kann.

- einer angemessenen Beschreibung der Ergebnisse der Risikoanalyse
- dem Vorhaben des Herstellers, ein systematisches Verfahren einzurichten und auf den neusten Stand zu halten. Das ermöglicht, Erfahrungen in den der Herstellung nachgelagerten Phasen und dem Produkt selber auszuwerten und ermöglicht erforderliche Korrekturen.

Damit sind die Unterlagen der Risikoanalyse für die Konformitätsbewertung notwendig und folglich dem Antrag auf Konformitätsprüfung beizulegen.

7 Datenschutz

Der Datenschutz sollte bei der Gesamtbetrachtung der Sicherheit eines Medizingeräts nicht unbeachtet bleiben.
Datenschutzverstöße (beabsichtigt oder nicht) sind Verletzungen des Grundwertes Vertraulichkeit.
Datenschutzverstöße können durch Missbrauch, durch Schwachstellen oder unbeabsichtigte Aktionen entstehen.
Das regulierende Gesetz für Deutschland und die Europäische Union ist die DSGVO (Datenschutz-Grundverordnung), Verordnung (EZ) 2016/679 des Europäischen Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten[65]
Entsprechend dieser Verordnung, Artikel 9 ist die Verarbeitung von Gesundheitsdaten erst einmal grundsätzlich untersagt. Die Person hat demnach ausdrücklich und zweckbezogen in die Datenverarbeitung einzuwilligen, um eine solche zu ermöglichen.
Die Verarbeitung von gesundheitsbezogenen Daten darf entsprechend dieser Verordnung nur durch Fachpersonal oder im Auftrag von Fachpersonal erfolgen.
Das zeigt den hohen Stellenwert der Vertraulichkeit von personenbezogen Gesundheitsdaten, was sich in der Risikoanalyse wiederspiegeln sollte. Es besteht hier nicht nur eine Gefahr für den Patienten als Anwender, sondern auch für Ärzte und sonstige Betreiber der Geräte. Nicht zuletzt sollte auch der Hersteller zugunsten seiner Reputation diese Hervorhebung von Gesundheitsdaten nie aus dem Blick verlieren.

7.1 Datenschutz am Beispiel Insulinpumpe

Für das fiktive Medizinprodukt Insulinpumpe ist eine Speicherung von gesundheitsbezogenen Daten außerhalb des Verfügungsbereiches des Anwenders an zwei Stellen notwendig.

[65] Datenschutz-Grundverordnung (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); https://dejure.org/gesetze/DSGVO; Abrufdatum: 28.06.2023

1. Während der Konfiguration und Inbetriebnahme werden die Gesundheitsdaten für die Grundeinstellung des Gerätes notwendig. Das betrifft beispielsweise die Schwere des Diabetes unter Betrachtung einer eventuellen Restleistung der Bauchspeicheldrüse, Essgewohnheiten, gewöhnliches Aktivitätsprofil, Körpermaße und Gewicht zur Berechnung des Grundbedarfes für das zu installierende Grundprogramm der Pumpe. Dieses Programm läuft als Standard und wird nach Ablauf von temporären Änderungen durch das Steuergerät wieder aufgenommen. Auch fällt die Pumpe bei eventuellen Störungen immer wieder in diesen Grundmodus zurück, um die Sicherheit des Patienten zu gewährleisten. Damit müssen die Datenverarbeitung und Absicherung an dieser Stelle in die Betrachtung einbezogen werden.

2. Messdaten, Verbrauchsdaten und Störungsmeldungen werden automatisch auf den Server des Herstellers geladen, um diese dem behandelnden Arzt zur Verfügung stellen zu können. Der Hersteller muss die Absicherung des Datenflusses und der Speicherung der personenbezogenen Daten auf seinem Server für die Prüfung dokumentieren. Wichtig ist es darzulegen, ob
   a. der Hersteller seine Aktivitäten bezüglich des zu prüfenden Produktes auf die EU beschränkt, was eine Verarbeitung nach DSGVO bedeutet.
   b. Nutzt der Hersteller für die Speicherung der Daten ausschließlich eigene Server oder Server von Diensten innerhalb der EU? Wenn nicht, ist nachzuweisen wie die Einhaltung der DSGVO erreicht wird.
   c. Sind Datenspenden für kommerzielle oder Forschungszwecke vorgesehen? Wenn ja, werden die Daten anonymisiert oder ausreichend pseudonymisiert weitergegeben? Werden die Patienten ausreichend hierüber aufgeklärt und gibt es eine Möglichkeit, der Nutzung der Daten zu widersprechen, ohne dass dadurch Einschränkungen des Service oder eine schlechtere medizinische Behandlung resultieren?

Nicht zuletzt sei angemerkt, dass das Speichern von Daten weitreichendere Konsequenzen, als man im ersten Moment betrachtet, haben kann. So wird beispielsweise in einem Artikel auf www.gelbe-liste.de folgendes berichtet: „Wie beim Symposium zu Diabetes im Straßenverkehr berichtet, können CGM-Systeme Betroffenen zum Nachteil gereichen, wenn sie aufgrund einer Hypoglykämie *(= Unterzuckerung, Anm. d. Verf.)* einen Unfall verursachen. Eigentlich sollten, berichtete Ebert, aufgrund von CGM-Systemen keine hypoglykämiebedingten Unfälle mehr möglich sein, denn die Systeme sollten rechtzeitig genug warnen, wenn Betroffene unterzuckern. Kam es trotzdem aufgrund einer Unterzuckerung zu einem Unfall, könnten Daten von CGM-Systemen theoretisch, wenn sie auf Servern von

Firmen liegen, beschlagnahmt werden. Daten in Arztpraxen sind zumeist durch die ärztliche Schweigepflicht abgedeckt.“[66]

Zu den o.g. Herausforderungen wird vermutlich das neue Gesetz zur verbesserten Nutzung von Gesundheitsdaten (GDNG) Klarheit bringen, welches sich derzeit jedoch noch im Stadium eines Referentenentwurfs (Stand 09.Juni 2023, lt. Webseite der AOK) befindet.[67]

[66] Sonja Klein, DDG 2023: Unsicherheit Digitalisierung – Regeln für Datenverarbeitung; www.gelbe-Liste.de/diabetologie/digitalisierung-datenschutz-schwerpunktpraxen; Abrufdatum: 30.05.2023
[67] https://www.aok-bv.de/hintergrund/gesetze/index_26432.html; Abrufdatum: 23.06.2023

8 Beispielbewertung der Cybersicherheit

Um die vorstehenden, sehr theoretisch gefassten Vorgehensweisen zu veranschaulichen, werden diese mittels eines fiktiven Medizinprodukts veranschaulicht.
Um ein bestmögliches Resultat zu erlangen, soll das Beispiel komplex genug sein, um gängige Gefahren abbilden zu können, welche durch Medizinprodukte entstehen können. Dazu gehören sowohl verschiedene Schnittstellen zu Komponenten, wie auch ein komplexer Datenfluss. Zudem sollte das Beispielprodukt ein Gefährdungspotential aufweisen, welches sowohl schwerwiegende physische Folgen, als auch schwerwiegende Verstöße des Datenschutzes darstellen kann.

8.1 Wahl des Beispiels Insulinpumpe

Für die Beispielbewertung ist ein sowohl allgemein bekanntes, als auch komplexes System eines Medizinproduktes sinnvoll.
Durch die allgemeine Bekanntheit (TV-Werbung, Verbreitung in der Bevölkerung) sind die Probleme für den Nutzer dieser Auswertung gut vorstellbar. Andererseits sind die neuen Systeme komplex genug, um das Gefährdungspotential sinnvoll darstellen zu können.
Ein weiteres Kriterium für die Wahl der Insulinpumpe ist, dass bei missbräuchlicher Anwendung oder Manipulation des Systems durch Unterzuckerung schwerwiegende Folgen für den Patienten, bis hin zum Tod, die Folge einer Fehlfunktion sein können.
Dieses zeigt, dass die Sicherheit eines solchen Produktes sowohl für den Patienten, als auch für den Hersteller, der aufgrund von Vorfällen seine Reputation verlieren könnte, von äußerster Wichtigkeit ist. So geschehen im Jahre 2019, als zwei Hacker den Nachweis brachten, dass sie mit Hilfe einer erstellten Smartphone-App Insulinpumpen des Herstellers Medtronic unabhängig vom Einsatzort fernsteuern können, welche potentiell tödliche Schwachstellen hatten. Dies führte zu einem Rückruf der Insulinpumpen. [68]

[68] https://www.wired.com/story/medtronic-insulin-pump-hack-app/; Abrufdatum: 10.07.2023

8.2 Aufbau und Funktion des Systems

Das Beispielsystem ist so zusammengestellt, dass die Blutzuckermessung mittels eines CGM-Moduls (Continuous Glucose Monitoring = Ständige Überwachung des Blutzuckers über Äquvalenzmessung mittels aufklebbarem Subkutansensor mit regelmäßiger Messung des Zuckergehalts im Unterhautgewebe) erfolgt.
Diese Messung wird dann per Bluetoothverbindung zum Steuergerät und, wenn gewünscht, zu einer App auf dem Smartphone übertragen. Diese Geräte sind über Internet mit dem Server des Herstellers verbunden. Das ist beispielsweise bei dem System von GlucoMen der Fall. Über den Server soll eine direkte Verbindung in die Arztpraxis zur Kontrolle der Patientendaten möglich sein.
Über die zugehörige App auf dem Smartphone können sowohl das Steuergerät, als auch der Messtransmitter konfiguriert werden. Man kann damit die Messfrequenz ändern oder auch bei Bedarf vor einer Mahlzeit mit höherem Insulinbedarf die Pumpleistung vorsorglich anpassen.
Letztlich ist auch die Pumpe selber mit dem Steuergerät verbunden, welche die mittels der Software von App und Steuergerät ermittelten Insulinbedarfe über eine Kanüle in das Gewebe des Patienten einbringt.

Damit haben wir vier physische Komponenten mit ihren spezifischen Eigenschaften und Datenverbindungen.

8.2.1 CGM-Transmitter

Abbildung 6: CGM-Transmitter[69]

Abbildung 7: CGM-Transmitter[70]

[69] https://amsldiabetes.com.au/wp-content/uploads/2019/05/stomach-g6-e1590972547690.jpg; Abrufdatum: 09.07.2023
[70] https://www.weavermedical.com/binary/shop_proprod_photos/original/113.png, 05.06.2023

Hauptkomponenten des Transmitters sind:

- Sensor mit Messeinheit (Subkutanmessung)
- Prozessor mit
  - Betriebssystem und
  - Software
  - Speicher
- eventuell physische Schnittstelle (USB) zur Programmierung und Kalibrierung
- Empfänger (Bluetooth)
- Sender (Bluetooth)
- Energieversorgung (Batterie oder Akku)

8.2.2 Insulinpumpe

Abbildung 8: Beispiel Patchpumpe[71]

Hauptkomponenten der Insulinpumpe (Patchpumpe) sind:

- Prozessor mit
  - Betriebssystem
  - Software
  - Speicher
  - Steuereinheit / Schnittstelle für Insulinpumpe
  - Schnittstelle zum Dateneingang vom Steuergerät (Bluetooth oder Kabel)

[71] *https://diatec-fortbildung.de/wordpress/wp-content/uploads/2023/01/a.m3-1-1024x301.jpg; Abruf-datum: 05.06.2023*

- Pumpe mit Kanüle und Insulinvorrat
- Sender (Bluetooth, WLAN)
- Empfänger (Bluetooth, WLAN)
- eventuell physische Schnittstelle (USB)
- Energieversorgung (Batterie, Akku)

8.2.3 Steuergerät

Abbildung 9: Steuergerät und CGD-Transmitter[72]

Hauptkomponenten des Steuergerätes sind:

- Display (Eingabe und Ausgabe)
- Prozessor mit
  - Betriebssystem
  - Software
  - Speicher
- Empfänger (Bluetooth, WLAN)
- Sender (Bluetooth, WLAN)
- physische Schnittstelle (USB)
- Energieversorgung (Batterie, Akku)

[72] https://imageio.forbes.com/specials-images/imageserve/1137686482/Children-of-the-90s-study/960x0.jpg; Abrufdatum 05.06.2023

8.2.4 App auf Smartphone / Smartwatch

Abbildung 10:Beispiel App auf Smartphone[73]

Hauptkomponenten:

- Software
  - Betriebssystem des Smartphones
  - Software der App mit Schnittstelle zum Smartphone
- Speicher (des Smartphones)
- Display des Smartphones (Eingabe und Ausgabe von Daten)
- Empfangseinheit des Smartphones (Bluetooth, WLAN)
- Sendeeinheit des Smartphones (Bluetooth, WLAN)
- Prozessor des Smartphones
- Datenverbindung Smartphone zur Cloud des Herstellers der Insulinpumpe
- Nutzerverwaltung in Abhängigkeit von App und Hersteller, z.B. CareLink-App hat Möglichkeit zur Einrichtung von 5 Vertrauenspersonen, welche Zugriff auf das System haben und im Falle einer Warnung durch das System reagieren können.
- Ausführung von Updates über die Datenverbindung zum Hersteller
- Weiterleitung der Nutzerdaten an den behandelnden Arzt über die Cloudinfrastruktur des Herstellers

[73] https://www.connectedinmotion.ca/wp-content/uploads/2019/12/CIM-DexcomG6-Apps.jpg

8.3 Allgemeines Schema des Aufbaus des Systems Insulinpumpe

Das Medizingerät Insulinpumpe besteht aus mehreren Komponenten, welche den an Diabetes erkrankten Menschen das Leben mit dieser Krankheit vereinfachen sollen.
Dieses System hat den Erkrankten viele Fortschritte gebracht und wird in der weiteren Entwicklung noch viele Vorteile mit sich bringen.
Die Entwicklung zu hochtechnisierten Möglichkeiten des Umgangs mit dieser Erkrankung hat in den letzten Jahrzehnten nicht nur Bequemlichkeit und eine bessere Möglichkeit der Gestaltung im Alltag ermöglicht, sie hat auch die Lebenserwartung, gerade für Menschen mit Typ I- Diabetes, der Autoimmundiabetes, welche schon Kinder betrifft, maßgeblich an eine normale Lebenserwartung gebracht. Auch die Langzeitfolgen durch diese schwere Erkrankung, wie zunehmende Erblindung der Patienten, sind heute kaum noch ein Thema.

Dieses Beispiel zeigt ganz besonders, dass eine Risiko-Nutzen-Abwägung im Bereich der Medizinprodukte zwingender Bestandteil für eine Evaluierung der Sicherheit durch den Hersteller ist.

Durch das Schema mit seinen vielfältigen Datenverbindungen ist erkennbar, dass gerade ein solch komplexes Produkt mit Anbindung an die häusliche IT-Infrastruktur (WLAN, Smartphone, etc.) viele natürliche Schwachstellen für die Datensicherheit und auch die Cybersicherheit birgt.

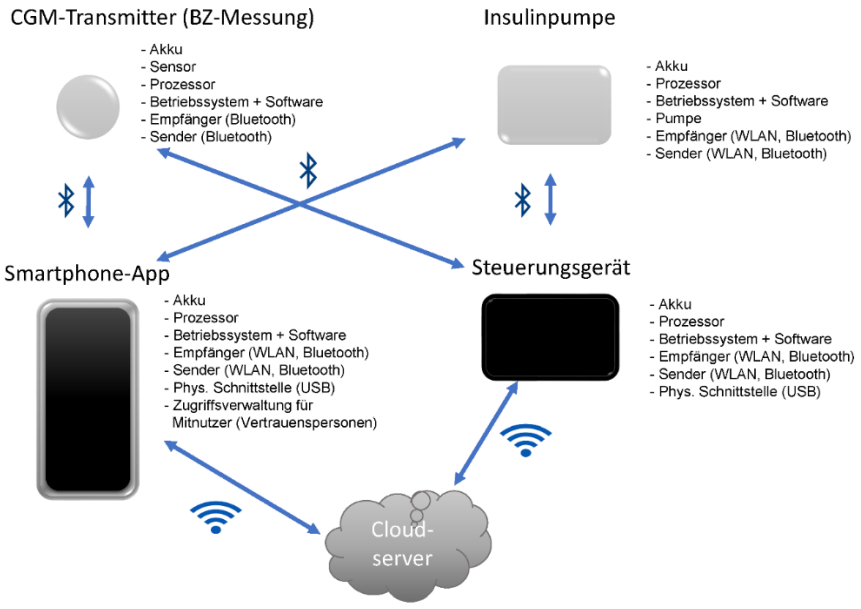

Abbildung 11: Netzplan des fiktiven Produktes Insulinpumpe

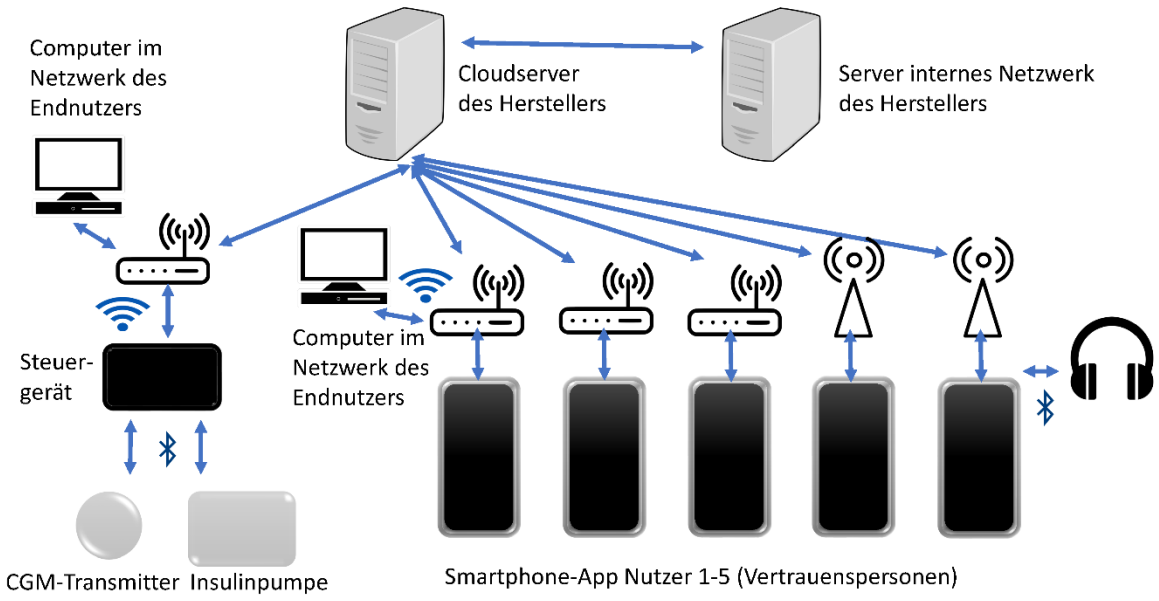

Abbildung 12: Mögliche Netzwerkverbindungen des fiktiven Produktes Insulinpumpe

8.4 Wichtige Dokumentationsinhalte

Es gibt drei zu betrachtende Bereiche der Sicherheit bei diesem Gerät:

1. Das zum Geräteservice gehörende Netzsystem mit Datenserver
2. Das Insulinpumpensystem selber
3. Einbindung in die Dateninfrastruktur der Nutzer (Patient, Arzt)

Für die ersten beiden Punkte ist der Hersteller allein verantwortlich, für Punkt 3 der Patient, bzw. der Arzt. Für das Netzsystem des Herstellers ist als erster Schritt ein Nachweis, dass dieses nach BSI-Grundschutz gehärtet ist, sinnvoll.
Als zweiter Schritt scheint die Sicherstellung der Anforderungen aus BSI CS-E 132 sinnvoll. Anschließend können die Risikoanalyse und Risikobehandlung für das Gerät, wie in den vorigen Kapiteln erläutert, ausgeführt werden.
Abschließend sollte das Risikopotential, welches aus Zusammenführung von Medizinprodukt und dem Datennetz des Herstellers entsteht, betrachtet werden, da durch die Kombination von Schwachstellen neue Risiken entstehen können. Dabei sind auch Risiken, welche sich aus der Anbindung der Dateninfrastruktur der behandelnden Ärzte ergeben können, zu betrachten.
Aus dieser Analyse können weitere Sicherheitsmaßnahmen notwendig werden, welche es umzusetzen gilt, wenn Risiken in einem nicht akzeptierbaren Bereich verbleiben. Das kann

auch Maßnahmen einschließen, welche seitens der Anwender, z.B. der Arztpraxen, umzusetzen sind. Diese Umsetzung ist sicherzustellen und ggf. Kontrollmechanismen darzulegen. Gleiches gilt für die App, welche durch die Patienten genutzt werden kann, insbesondere auch unter Berücksichtigung der geplanten Mehrfachzugänge für die sogenannten Vertrauenspersonen, da diese zum System gehören.

Daraus ergeben sich folgende Nachweisschritte der Konformität:

1. Nachweis des IT-Grundschutzes für die Anbindung an den Server, den Server und das zugehörige Netzwerk
2. Nachweis der Erfüllung der Anforderungen aus Empfehlung BSI CS-E 132, vgl. Anlagen, Teil 3
3. Nachweis des Einhaltens der Anforderungen aus BSI TR 03161 für die Smartphone-App
4. Risikoanalyse und Behandlung für das Gerät und seiner Komponenten, vgl. Abbildung 12
5. Risikoanalyse und Behandlung für das Zusammenspiel aus Gerät und der gewöhnlichen Netzwerkumgebung, vgl. Abbildung 13
6. Dokumentation der Sicherheit und ggf. der zusätzlichen Maßnahmen, welche durch die Anwender zu erfolgen haben.

Für die Punkte 4 und 5, Risikoanalysen, ist ein Vorgehen nach BSI-Standard 200-3, wie unter Kapitel 6 beschrieben, sinnvoll.
Eine Darstellung mit Risikobewertung vor Risikobehandlung ist möglich, jedoch nicht zwingend notwendig, solange

- im Ergebnis ein akzeptables Risiko erscheint
- Nach EU 2017/745 die maximal mögliche Minderung des Risikos nach Stand der Technik erfolgte.

9 Diskussion

Die Bewertung der Cybersicherheit von Medizinprodukten stellt für die Benannten Stellen eine große Herausforderung dar.
Diese liegt vor allem in folgenden Punkten begründet:

- Anforderungen an die Cybersicherheit im Konkreten haben überwiegend Empfehlungscharakter,
- Aus diesen Empfehlungen müssen sowohl Hersteller, als auch Benannte Stellen ableiten, was als Stand der Technik gilt,
- unterschiedliche territoriale Geltungsbereiche haben unterschiedliche Empfehlungen und Umsetzungsstandards formuliert,
- Die Produktvielfalt für medizinische Produkte ist enorm, sowohl bezogen auf die möglichen Komponenten des Produkts, aber auch bezüglich der Anwendung und damit der potentiellen Schadensmöglichkeiten für Patienten.

Während sich Hersteller auf ihre Produktpalette konzentrieren können, müssen die Benannten Stellen das gesamte mögliche Produktspektrum, zumindest aber das, für welche sie benannt wurden, in einem strengen, verglichen mit den Entwicklungszeitraum sehr kurzen Zeitfenster überprüfen können.

9.1 Herausforderungen und Herangehensweisen

Die Risikobewertung ist die Entscheidungsgrundlage dafür, ob ein Medizingerät eine Markteinführung erhält.

Die Konformitätsprüfung muss daher prüfen, ob die Ausführungen des Herstellers nachvollziehbar und den Vorschriften entsprechend umgesetzt wurden. Dieses ist aus der Dokumentation zu entnehmen.
Um hier eine Einschätzung zu ermöglichen, muss man zunächst wissen, wie die Risikobewertung im Ablauf funktioniert. Im Kapitel Risikobewertung wurde daher die Vorgehensweise nach den EU-Vorschriften und den Empfehlungen des BSI dargestellt, also eine Vorgehensweise, wie sie in diesem Rechtsraum möglich ist.

Durch die MDR ist das Prinzip, dass ein Risiko auszuschließen oder so weit wie möglich zu vermeiden ist, festgelegt. (Anhang I, Artikel 17.1)
Dieses hat Einfluss auf das Herangehen an die Risikobewertung.
Im Geltungsbereich der FDA ist das Prinzip, jedes einzelne Risiko so weit zu mindern, bis es akzeptabel ist, möglich.

Daraus ergibt sich, dass nach Ansatz der MDR erst alle Risiken nach dem Stand der Technik gemindert werden und dann eine Betrachtung der Einzelrisiken erfolgt. Es folgt die Einteilung in akzeptierbare und nicht akzeptierbare Risiken. Sollte es nicht akzeptierbare Risiken geben, dann müssen Maßnahmen getroffen werden, diese Risiken in akzeptierbare Risiken zu überführen, gelingt dieses nicht, ist zunächst eine Nutzen-Risiko-Analyse durchzuführen. Ist diese ebenfalls nicht positiv, ist die Konformität des Medizinproduktes nicht gegeben.
Das Prinzip der MDR ist die Risikoreduzierung „As Far As Possible“ (AFAP), während der Nutzen-Risiko bezogene Ansatz eine Risikoreduzierung „As Low As Reasonable Possible“ (ALARP) ist. [74]
Die Grenze zwischen akzeptierbaren und nichtakzeptierbaren Risiken wird in der Regel in der Matrix nach ALARP die Grenze zwischen akzeptierbaren und weiter zu behandelnden Risiken sein.

Der Unterschied beider Herangehensweisen wird bei der Betrachtung der Risikomatrices deutlich. Während nach MDR nur akzeptable und nichtakzeptable Risiken abgebildet werden, können nach dem Prinzip der Nutzen-Risikobewertung drei oder mehr Risikolevels abgebildet werden.

Umgekehrt bedeutet dies jedoch auch, dass ein im Rechtsgebiet zugelassenes Produkt nicht die mit diesem Prinzip geschaffenen strengeren Bedingungen der Konformität erfüllt. Es ist eine neue Risikobewertung durchzuführen und folglich ggf. weitergehende Maßnahmen zu implementieren.

[74] Edwin Bills; ISO TR 24971:2020 – Bringing Clarity To Risk Acceptability In ISO 14971; https://www.meddeviceonline.com/doc/iso-tr-bringing-clarity-to-risk-acceptability-in-iso-0001; Abrufdatum: 05.07.2023

Risikomatrix mit Akzeptanzgrad

	Vernach-lässigbar	Gering	Ernst	Kritisch	Katastrophal
Häufig					
Wahrscheinlich					
Gelegentlich					
Fernliegend					
Unwahrscheinlich					

Tabelle 14: Risikomatrix nach ALARP-Prinzip

Akzeptierbares Risiko

Weiter zu behandelndes Risiko

Nichtakzeptierbares Risiko

	Vernach-lässigbar	Gering	Ernst	Kritisch	Katastrophal
Häufig					
Wahrscheinlich					
Gelegentlich					
Fernliegend					
Unwahrscheinlich					

Tabelle 15: Risikomatrix nach ALAP-Prinzip

Akzeptierbares Risiko

Nichtakzeptierbares Risiko

Während dieses für eine Konformitätbewertung, welche in Deutschland stattfindet, zunächst keine Relevanz zu haben scheint, ist es gerade in Hinblick auf die Auswertungen von Dokumentationen von zuvor erfolgten FDA-Zulassungen wichtig, die möglicherweise unterschiedliche Ausgangsbasis für die durch den Hersteller getroffenen Feststellungen zu kennen. Der praktische Unterschied ist, dass nach ALARP Risikominderungen nur so weit getroffen werden, dass die Akzeptanz für das eine betrachtete Risiko akzeptabel wird, während nach ALAP zunächst eine Maximalminderungen aller Risiken erfolgt und danach eine Bewertung.

Das ALARP-Prinzip ist das, welches unter anderem auch im BSI-Grundschutz angewendet wird.

Bei der Konformitätsbewertung sind insgesamt drei Bereiche zu berücksichtigen:
1. Das IT-System der Umgebung des Medizinprodukts
2. Das Medizinprodukt selber mit seinem eigenen Cybersicherheits-Risiko
3. Die Kombination von Produkt und Einsatzumgebung unter Beachtung einer möglichen Kumulation von Ereignissen und Ausnutzung von Schwachstellen der einen Komponenten, um in die anderen Komponente eindringen zu können oder das Ausnutzen einer durch das Einbringen des Medizinproduktes in die geplante Umgebung erst geschaffenen Kombinationsmöglichkeit des Ausnutzens einer Kombination von Schwachstellen.

Alle drei Aspekte haben in der Dokumentation des Medizinproduktes Berücksichtigung zu finden.

9.2 Medizinprodukte und Datenschutz

Werden Gesundheitsdaten durch ein Medizinprodukt verarbeitet, was auch eine reine Speicherung der Daten umfasst, müssen diesen erhöhten Anforderungen Rechnung getragen werden.
Folglich muss eindeutig sein, in welchen Komponenten des Systems diese Daten verarbeitet oder gespeichert werden. Der Datenfluss zwischen den Komponenten muss betrachtet werden, um hier Risiken des Zugriffs von außen ausschließen zu können, oder das Risiko des Zugriffs mindestens minimieren zu können.
Geeignete Maßnahmen müssen getroffen werden, was beispielsweise durch Verschlüsselung des Datenflusses und verschlüsselter Speicherung erfolgen kann.

Letztlich ist es auch wichtig, dass Patienten der notwendigen Verarbeitung ihrer Daten wirksam zugestimmt haben.
Besonderes Augenmerk ist darauf zu richten, wenn Daten auf externen Servern gespeichert werden, dass Klarheit besteht, wer auf diese Systeme Zugriff erlangen kann. Dies spielt insbesondere dann eine Rolle, wenn Hersteller oder Betreiber entweder ihre Serverdienstleistung im Nicht-EU-Ausland beziehen oder vielleicht selbst ihren Sitz oder Datenverarbeitung außerhalb der EU haben.
Dann ist sicher zu stellen, dass Patienten in diesem speziellen Falle einer solchen Verarbeitung explizit und wirksam zustimmen oder optional diese Verarbeitung ausschließen können, da ein nicht durch Vereinbarung autorisierter Zugriff auf diese Daten eine Verletzung des Schutzzieles Vertraulichkeit bedeutet.
Es kann aufgrund dieser Zusammenhänge der Schluss gezogen werden, dass die Betrachtung der Datensicherheit im Netz im engen Rahmen der DSGVO ein Teil der Konformitätsprüfung sein sollte.
Der Hersteller sollte Angaben machen, ob die DSGVO eingehalten wird oder wenn Daten z.B. für Forschung gespendet werden sollen, wie dieses rechtssicher gestaltet werden kann.

9.3 Ausblick

Für eine Verbesserung der Cybersicherheit von Medizinprodukten wäre es wünschenswert, wenn es systematischere, verbindliche Abläufe der Umsetzung gäbe. Bisher ist man auf die Umsetzung von Empfehlungen angewiesen.
Es wird hier von Seiten des EU-Rechts und der nationalen Umsetzungen zukünftig weitere Schritte geben. Das Gesetz zur verbesserten Nutzung von Gesundheitsdaten (GDNG) wird verabschiedet werden und es werden damit sicher auch Vorgaben zur Sicherheit der Daten, wie Pseudonymisierung, sicherer Datenverkehr und sichere Speicherung bei Datenspende gemacht werden. Damit könnte man der Bewertung der Cybersicherheit in diesem Punkt eine rechtliche Grundlage der Konformität geben.
Weiter wird es im Rahmen der NIS2-RL[75] eine Überarbeitung der derzeitigen IT-Sicherheitsgesetzes geben müssen, die EU hat eine Umsetzung bis 17.10.2024 gefordert. Im Rahmen der Neugestaltung wird explizit das Gesundheitswesen auf Grundlage von EU

[75] Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie); https://eur-lex.europa.eu/eli/dir/2022/2555/oj, Abrufdatum: 23.06.2023

2022/2557[76] durch Artikel 2, Absatz 3 dieser Richtlinie einbezogen und auch im Anhang I als wesentliche Einrichtung im Sinne des Geltungsbereiches benannt.

Für die genaue Umsetzung der NIS2-RL wird eine Kooperationsgruppe mit der ENISA (European Union Agency for Cybersecurity) festlegen, welche Dienste, Systeme oder Produkte einer Risikobewertung von der Richtlinie erfasst werden. Davon hängt letztlich ab, ob nicht nur der Hersteller der Medizinprodukte mit seinen Anlagen, sondern auch die hergestellten Medizinprodukte diesen, noch zu schaffenden, Auflagen unterworfen sein werden. Artikel 24 der Richtlinie stellt Europäische Schemata für die Cybersicherheitszertifizierung in Aussicht. Das wäre im Sinne der Vereinheitlichung der Prozesse zugunsten der Sicherheit der Patienten und Anwender zu begrüßen. Damit würden auch die Anforderungen, welche derzeit für den deutschen Raum als Geltungsbereich als Empfehlungen bestehen, eine höhere Verpflichtung zur Einhaltung erfahren.

[76] Richtlinie (EU) 2022/2557; https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32022L2557; Abrufdatum 24.06.2023

Literatur

[AFC2023] Allianz für Cybersicherheit: <https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Netzwerk-Formate/Veranstaltungen-und-Austausch/Expertenkreise/CyberMed/cybermed_node.html>, verfügbar am 28.06.2023

[AOK2023] AOK: <https://www.aok-bv.de/hintergrund/gesetze/index_26432.html>, verfügbar am 23.06.2023

[BiJo2023] Bills, Johnson: The Intersection Of ISO 13485 AND ISO 14971 Under The Proposed FDA QMSR, <https://www.meddeviceonline.com/doc/the-intersection-of-iso-and-iso-under-the-proposed-fda-qmsr-0001>, verfügbar: 04.07.2023

[Bills2023] Bills, Edwin: Bringing Clarity TO Risk Acceptability IN ISO 14971, <https://www.meddeviceonline.com/doc/iso-tr-bringing-clarity-to-risk-acceptability-in-iso-0001>, verfügbar am 05.07.2023

[BSIGS2023] BSI: Grundschutz-Kompendium, <https://bsi.bund.de/DE/Themen/Untenehmen-und-Organsisationen/Standards-und-Zertifizierung/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html>, verfügbar am 29.05.2023

[BSICS2023] BSI: Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte (BSI CS-E 132), <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/CS-E-132_Medizinprodukte.pdf>, verfügbar am 10.05.2023

[BSISt2001] BSI: BSI-Standard 200-1, Version 1.0, <www.bsi.bund.de/grundschutz>; verfügbar am 20.06.2023

[BSISt2003] BSI: BSI-Standard 200-3, Risikoanalyse auf der Basis von IT-Grundschutz; <www.bsi.bund.de/grundschutz>, verfügbar am 04.06.2023

[CSO2023] CSO: Was ist eine Software-Bill-of-Materials, <https://www.csoonline.com/de/a/was-ist-eine-software-bill-of-materials,2674040>, verfügbar am 01.07.2023

[DIN2023] DIN.de:, Über Normen und Standards, <https://www.din.de/de/ueber-normen-und-standards/din-norm>, verfügbar am 04.07.2023

[DSGVO2023] Dejure.org: Datenschutz-Grundverordnung (Verordnung (EU) 2016/679des 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), <https://dejure.org/gesetze/DSGVO>, verfügbar am 28.06.2023

[ENISO2013] DIN EN ISO 14971: Medizinprodukte – Anwendung des Risikomanagements auf Medizinprodukte: DIN Deutsches Institut für Normung e.V., 2013

[ENISO2019] DIN EN ISO 14971: Medizinprodukte – Anwendung des Risikomanagements auf Medizinprodukte; OVE Österreichischer Verband für Elektrotechnik, 2019

[ExCM2023] Expertenkreis CyberMed: Leitfaden zur Nutzung des MDS2 aus 2019, 1 Präambel, <https://bsi.bund.de/SharedDocs/Downloads/Webs/ACS/DE/downlodow/Expertenkreis_CyberMed_MDS2.pdf>, verfügbar am 20.05.2023

[FedRe2023] Federalregister.gov: Cybersecurity in medical devices, <https://www.federalregister.gov/documents/2022/04/08/2022-07614/cybersecurity-in-medical-devices-quality-system-

considerations-and-content-of-premarket-subissions>, verfügbar am 04.07.2023

[Git2023] Johner-Institut: GitHub, <https://github.com/johner-institut/it-security-guideline/blob/master/Konzept-Leitfden-IT-Sicherheit.md>, verfügbar am 28.06.2023

[Git2023] Johner-Institut: GitHub, https://github.com/johner-institut/it-security-guideline/blob/master/Guideline-IT-Security_DE.md>, verfügbar am 28.06.2023

[JohIn2023] Johner-Institut: Mission, <https://www.johner-institut.de/unternehmen/mission/>, verfügbar: 28.06.2023

[Klein2023] Klein, Sonja: Unsicherheit Digitalisierung – Regeln für Datenverarbeitung, <https://www.gelbe-Liste.de/diabetologie/digitalisierung-datenschutz-schwerpunktpraxen>, verfügbar am 30.05.2023

[NIS22023] Europa.eu: Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie), <https://eur-lex.europa.eu/eli/dir/2022/2555oj>, verfügbar am 23.06.2023

[RLEU2023] Richtlinie (EU) 2022/2557, <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32022L2557>, verfügbar am 24.06.2023

[VerEU2017] Europa.eu: Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates, < https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32017R0745>, verfügbar am 04.06.2023

[VerDE2021] Gesetze im Internet: Verordnung über die Meldung von mutmaßlichen schwerwiegenden Vorkommnissen bei Medizinprodukten sowie zum Informationsaustausch der zuständigen Behörden (MPAMIV), Ausfertigung vom 21.04.2021, <https://www.gesetze-im-internet.de/mpamiv/MPAMIV.pdf>, verfügbar am 05.06.2023

[WIKI2023] Wikipedia: Internationale Organisation für Normung, <https://de.wikipedia.org/wiki/Internationale_Organisation%C3%BCr_Normung>, verfügbar am 04.07.2023

[Wired2023] Wired.com: <https://www.wired.com/story/medtronic-insulin-pump-hack-app/>, verfügbar am 10.07.2023

Anlagen

Anlagen, Teil 1: Fragenkatalog nach NEMA, MDS2

Fragenkatalog nach Leitfaden „Sicherheit von Medizinprodukten“ der Allianz für Cyber-Sicherheit auf Basis NEMA, MDS2:

Die Allianz für Cybersicherheit stellt online eine PDF-Variante in deutscher Sprache für den Fragebogen MDS2 zur Verfügung. Dieser wurde hier verwendet und um eine Spalte für Eintragungen erweitert.

Für eine weitere Verwendung wird dieser Arbeit die zugehörige Excel-Datei beigefügt, welche man interessierten Herstellern zur Verfügung stellen könnte.

Es wäre wünschenswert, wenn dieser Standard für Übermittlung von Eigenschaften des netzwerkfähigen Medizinprodukten, welcher umfangreich in den USA Anwendung findet, auch in Deutschland verstärkt Anwendung findet.

Die Allianz für Cybersicherheit scheint dies zu befürworten, es ist sinnvoll, da hiermit auf einen Blick wichtige sicherheitsrelevante Daten ermittelt werden könnten. Der Fragebogen ist darüber hinaus eine Möglichkeit, die Angaben zu den Produkten mehr zu standardisieren und vergleichbar zu machen.

Fragenkatalog nach Leitfaden „Sicherheit von Medizinprodukten“ der Allianz für Cyber-

9.4 1 Fragenkatalog DOC: Beschreibung des Medizinprodukts

FragenID	Frage	“yes”, “no” oder “n/a”	Antwort	Hinweise
DOC-1	Name des Herstellers/Legal manufacturer			
DOC-2	Beschreibung des Produkts			Bitte geben Sie hier die Produkt- und/oder Versionsinformationen an.
DOC-3	Modellnummer des Produkts			Hier ist es empfehlenswert, die Modellnummer, mit der das Produkt in Verkehr gebracht wurde, zu verwenden.
DOC-4	Dokumenten ID			Es wird empfohlen die Dokumentennummer dieses MDS2-Dokuments einzufügen, so dass klar ist, auf welches Dokument und welchen Versionsstand sich eventuelle Rückfragen beziehen.
DOC-5	Kontaktinformationen des Herstellers			Es wird empfohlen, einen Ansprechpartner, in Form einer Telefonnummer, Mailadresse oder durch persönlichen Kontakt zu nennen. Um den unterschiedlichen Firmenstrukturen gerecht zu werden, sollte bei Fragen zum Produkt das Produktmanagement angegeben werden, bei IT- Sicherheitsfragen sollte ein technischer Experte und bei Fragen zum Datenschutz eine entsprechend verantwortliche Person benannt werden.

DOC-6	Zweckbestimmung des Produkts in vernezten Umgebungen			Hier ist empfehlenswert, dass auf die Formulierungen im Benutzerhandbuch oder in anderen bestehenden Dokumenten verwiesen wird.
DOC-7	Veröffentlichungsdatum des Dokuments			Es wird empfohlen, dass neben dem Dokumentendatum auch das Datum des MDS2-Formulars angegeben wird.
DOC-8	Koordiniertes Offenlegungs-Programm des Herstellers			Gibt es ein herstellereigenes koordiniertes Offenlegungs-Programm (Disclosure-Programm) für Schwachstellen? Wo kann man dieses finden (Web)?
DOC-9	ISAO			ISAO steht für „Information Sharing and Analysis Organization“. Der Hersteller kann hier angeben, ob und in welcher ISAO er Mitglied ist. Die Allianz für Cyber-Sicherheit (ACS) kann durchaus als solche betrachtet werden.
DOC-10	Gibt es ein Netzwerk- oder Datenfluss-Diagramm, das die Verbindung zu anderen Systemkomponenten oder externen Ressourcen darstellt? Wenn ja, stellen Sie bitte Details oder entsprechende Referenzen im Freitextfeld zur Verfügung.			Hier ist zu empfehlen, dass ein Verweis z. B. auf ein Netzwerkdiagramm in der Kundendokumentation, aufgeführt wird.
DOC-11	Handelt es sich bei dem Produkt um Software as a Medical Device (SaMD)?			Hier ist zu empfehlen, dass wenn die Antwort „no“ lautet, bei den folgenden Fragen 11.1 bis 11.4 „n/a“ angegeben wird.

DOC-11.1	Beinhaltet die SaMD ein Betriebssystem? Wenn ja, stellen Sie bitte Details oder entsprechende Referenzen im Freitextfeld zur Verfügung.			
DOC-11.2	Läuft die SaMD auf einem vom Betreiber gestellten Betriebssystem? Wenn ja, stellen Sie bitte Details oder entsprechende Referenzen im Freitextfeld zur Verfügung.			
DOC-11.3	Wird die SaMD vom Hersteller betrieben? Wenn ja, stellen Sie bitte Details oder entsprechende Referenzen im Freitextfeld zur Verfügung.			
DOC-11.4	Wird die SaMD vom Kunden betrieben? Wenn ja, stellen Sie bitte Details oder entsprechende Referenzen im Freitextfeld zur Verfügung.			

Fragenkatalog nach Leitfaden „Sicherheit von Medizinprodukten“ der Allianz für Cyber-Sicherheit

9.5 2 Fragenkatalog MPII: Verwaltung von personenbezogenen Daten

FragenID	Frage	“yes”, “no” oder “”n/a”	Antwort	Hinweise
MPII-1	Kann das Produkt personenbezogene Daten anzeigen, übertragen, speichern oder verändern (inklusive elektronischer Akten)?			Hier ist die nationale/lokale Gesetzgebung bzw. Auslegung von PII (personenbezogene Daten) oder die Verarbeitung dieser Daten gemeint. Hierzu zählen beispielsweise: Patientenname, Krankenversicherung und Versicherungsnummer, biometrische Daten, etc.
MPII-2	Welche Arten von personenbezogenen Daten können von dem Produkt vorgehalten werden? Listen Sie diese bitte in einem Freitextfeld auf.			Hier ist es sinnvoll, dass alle Arten von personenbezogenen Daten aufgezählt werden oder auf deren Dokumentation verwiesen wird. Wenn bei MPII- 1 mit „no“ geantwortet wurde, so sollte auch hier mit „no“ geantwortet und das Kommentarfeld freigelassen
MPII-2.1	Werden im Produkt personenbezogenen Daten temporär oder in einem flüchtigen internen Speicher vorgehalten (z. B. bis zum Ausschalten oder Zurücksetzen des Produkts)?			Wenn bei MPII-1 mit „no“ geantwortet wurde, so sollte auch hier mit „no“ geantwortet und das Kommentarfeld freigelassen werden. Ansonsten sollte diese Frage mit „yes“ beantwortet und die Details, wie das Halten der Informationen bis zum Ausschalten des Produkts (embedded device) oder bis zum Beenden
MPII-2.2	Werden personenbezogene Daten dauerhaft in internem Speicher gesichert			Bitte geben Sie hier Informationen zur Art der Speicherung, z. B. Datenbank oder Dateisystem, an.

MPII-2.3	Werden personenbezogene Daten auf nicht flüchtigen Datenspeichern aufbewahrt, bis diese explizit gelöscht werden?			Bitte geben Sie hier Informationen zur Art des Auslösens der Löschung, z. B. automatisch oder manuell, an.
MPII-2.4	Werden personenbezogene Daten dauerhaft in Datenbanken gespeichert? Wenn ja, liefern Sie bitte Details zur Architektur der Datenbank im Freitextfeld.			Wenn bei MPII-1 mit „no“ geantwortet wurde, so sollte auch hier mit „no“ geantwortet und das Kommentarfeld freigelassen werden. Diese Frage sollte nur mit „yes“ beantwortet werden, wenn die Daten tatsächlich in einer Datenbank abgelegt werden. Geben Sie bitte an, ob die Daten in einer externen oder lokalen Datenbank gespeichert werden. Bei Informationen zur Datenbank sollte sich die Erklärung nur auf die für den Datenschutz relevanten Daten beschränken.
MPII-2.5	Boetet das Produkt die Möglichkeit, dass lokal gespeicherte, personenbezogene Daten nach deren Ablage auf einem Langzeitspeicher automatisch gelöscht werden?			
MPII-2.6	Können personenbezogene Daten von anderen Systemen importiert oder dorthin exportiert werden? Z. B. ein tragbares Überwachungsgerät könnte personenbezogene Daten an einen Server liefern.			Hier ist das Importieren und Exportieren von personenbezogenen Daten zur weiteren Verarbeitung, als Teil der Zweckbestimmung und des normalen Betriebs, gemeint. Die Frage bezieht sich nicht auf Backup-Lösungen.
MPII-2.7	Werden personenbezogene Daten vorgehalten, wenn das Produkt ausgeschaltet wird oder die Stromzufuhr unterbrochen wird?			

MPII-2.8	Können die internen Datenspeicher durch einen Wartungsmitarbeiter entfernt werden, z. B. um diese separat zu vernichten oder beim Kunden vorzuhalten?			Hier kann zusätzlich angegeben werden, ob es sich um einen Mitarbeiter des Kunden handelt oder ob nur ein Mitarbeiter des Herstellers berechtigt ist.
MPII-2.9	Können personenbezogene Daten auf einem separaten System, getrennt vom Betriebssystem des Produkts oder der Gerätesoftware, gespeichert werden? Z. B. auf einem zweiten internen Laufwerk, auf alternativen Partitionen auf der Festplatte oder auf einem externen Speicherplatz.			
MPII-3	Erlaubt die Zweckbestimmung des Produkts, dass Mechanismen für die Übertragung			Bitte geben Sie hier an, ob diese Mechanismen, im Rahmen der Zweckbestimmung, möglich und ob sie optional sind.
MPII-3.1	Ist es möglich auf dem Produkt personenbezogene Daten anzuzeigen (z. B. über einen Bildschirm)?			
MPII-3.2	Erstellt das Produkt physische Berichte oder Bilder, die			Hierbei sind dauerhafte Abzüge der digitalen Information gemeint (hard copy).
MPII-3.3	Kann das Produkt personenbezogene Daten von einem Wechseldatenträger auslesen oder darauf schreiben (z. B. externe Festplatte, USB-Speicherstick oder andere USB-Speichermedien,			Bitte geben Sie hier an, ob es technisch möglich ist personenbezogene Daten von Wechseldatenträgern auszulesen oder darauf zu schreiben und ob dies für die Zweckbestimmung notwendig ist.

MPII-3.4	Kann das Produkt personenbezogene Daten über eine feste Kabelverbindung (z. B. RS-232, RS- 423, USB, FireWire, etc.) empfangen oder versenden?			Bitte geben Sie hier an, ob es technisch möglich ist personenbezogene Daten über eine feste Kabelverbindung zu empfangen oder zu versenden und ob dies deaktivierbar/physikalisch geschützt ist.
MPII-3.5	Kann das Produkt personenbezogene Daten über eine (drahtgebundene)			Hier wird empfohlen, dass wenn die Antwort „yes“ lautet, auf das Kapitel TXCF verwiesen wird.
MPII-3.6	Kann das Produkt personenbezogene Daten über eine drahtlose Netzwerkverbindung empfangen oder versenden (z. B. WiFi, Bluetooth, NFC, Infrarot, Mobiltelefon, etc.)?			Hier wird empfohlen, dass wenn die Antwort „yes“ lautet, auf das Kapitel TXCF verwiesen wird.
MPII-3.7	Kann das Produkt personenbezogene Daten über externe Netzwerke (z. B. Internet) empfangen oder versenden?			
MPII.3.8	Kann das Produkt personenbezogene Daten über Mechanismen zum Scannen importieren?			
MPII-3.9	Kann das Produkt personenbezogene Daten über ein proprietäres Protokoll übertragen oder versenden?			
MPII-3.10	Nutzt das Produkt andere Mechanismen, um personenbezogene Daten zu übertragen, zu importieren oder zu exportieren? Listen Sie diese bitte in einem Freitextfeld auf.			Hier sollten als Funktionen auch funkbasiertes (RFID) und das Lesen eines Fingerabdrucks oder anderer biometrischer Informationen, aufgeführt werden.

Fragenkatalog nach Leitfaden „Sicherheit von Medizinprodukten“ der Allianz für Cyber-Sicherheit

9.6 3 Fragenkatalog ALOF: Automatisches Abmelden

FragenID	Frage	“yes”, “no” oder “n/a”	Antwort	Hinweise
ALOF-1	Kann das Produkt so konfiguriert werden, dass es, nach einer gewissen Zeit der Inaktivität, den (angemeldeten) Nutzer dazu auffordert sich erneut zu autorisieren (z. B. durch eine automatische Abmeldung, Sitzungssperrung oder einen passwortgeschützter Bildschirmschoner).			Bitte geben Sie hier an, ob diese Mechanismen (erneute Anmeldung und passwortgeschützter Bildschirmschoner nach einer bestimmten Zeit der Inaktivität des Nutzers) voreingestellt sind oder ob sie konfigurierbar sind. Dies kann helfen zu verstehen, wie ein solcher Mechanismus ausgeschaltet werden kann (z. B. pro Session oder global durch entsprechende Warnungen an den Nutzer).
ALOF-2	Ist das Zeitintervall, bevor es zu einer automatischen Abmeldung / Bildschirmsperre, bedingt durch Inaktivität kommt, durch Nutzer oder Administratoren konfigurierbar? Bitte geben Sie im Freitextfeld die Zeit, feste Vorgabe oder ein einstellbares Zeitintervall an.			Geben Sie bitte an, ob der Nutzer oder der Administrator das Zeitintervall für eine automatische Abmeldung/Bildschirmsperre selbständig konfigurieren kann. Präzisieren Sie bitte, ob das Produkt auf eine durch den Nutzer bestimmte Zeit oder durch eine zugewiesene Rolle (z. B. Administrator, Nutzer) konfiguriert werden kann.

Fragenkatalog nach Leitfaden „Sicherheit von Medizinprodukten“ der Allianz für Cyber-Sicherheit

9.7 4 Fragenkatalog AUDT: Revisionskontrolle

FragenID	Frage	“yes”, “no” oder “n/a”	Antwort	Hinweise
AUDT-1	Kann das Produkt zusätzlich zu Protokollen des Betriebssystems			Falls Sie hier mit „no“ antworten, geben Sie bitte bei den Antworten AUDT-1.1 bis AUDT-8 „n/a“ an.
AUDT-1.1	Wird die Nutzer-ID in den Audit-Protokollen mit aufgezeichnet?			Wenn dem so ist, geben Sie bitte an, ob das Datensubjekt (z. B. der Patient) für jede personenbezogene Information im Audit-Protokoll identifiziert werden kann. Geben Sie bitte zudem an, ob im Audit-Pfad zwischen dem Erstellen, Anzeigen, Exportieren, etc. von personenbezogenen Daten und anderen Daten unterschieden werden kann.
AUDT-1.2	Existieren andere personenbezogene Daten im Audit-Protokoll? Wenn ja, beschreiben Sie dies bitte in einem Freitextfeld.			Wenn dem so ist, geben Sie bitte an, ob das Datensubjekt (z. B. der Patient) für jede personenbezogene Information im Audit-Protokoll identifiziert werden kann. Geben Sie bitte zudem an, ob im Audit-Pfad zwischen dem Erstellen, Anzeigen, Exportieren, etc. von personenbezogenen Daten und anderen Daten unterschieden werden kann.
AUDT-2	Werden bestimmte Ereignisse durch das Audit-Protokoll aufgezeichnet?			Wenn Sie hier mit „yes“ antworten, spezifizieren Sie bitte die Ereignisse in den Freitextfeldern der folgenden Fragen.
AUDT-2.1	Erfolgreiche Anmelde- und Abmeldeversuche?			

AUDT-2.2	Nicht erfolgreiche Anmelde- und Abmeldeversuche?			
AUDT-2.3	Veränderung der Nutzerrechte?			
AUDT-2.4	Erstellen, Ändern oder Löschen von Nutzerkonten?			Hier ist gemeint, dass beispielsweise eine E-Mail-Adresse eines Nutzers geändert werden kann, nicht jedoch die Nutzerrechte, wie in AUDT-2.3.
AUDT-2.5	Anzeige (z. B. Bildschirm, Ausdruck) von klinischen oder personenbezogenen Daten?			
AUDT-2.6	Erzeugung, Veränderung oder Löschung von Daten?			Wenn Sie hier mit „yes“ antworten, geben Sie bitte an, welche Form der Datenmanipulation (Erzeugung und/oder Veränderung und/oder Löschung) mit aufgezeichnet wird.
AUDT-2.7	Import/Export von Daten über Wechseldatenträger (z. B. USB-Speicherstick, externe Festplatte, DVD)?			Wenn Sie hier mit „yes“ antworten, geben Sie bitte an, in welcher Detailtiefe die Daten erfasst werden (z. B. nur die Patienten-ID, eine Liste der Dokumenten-IDs).
AUDT-2.8	Empfangen/Versenden von Daten und Kommandos über ein Netzwerk oder über direkte Punk-zu-Punkt-Verbindungen?			Wenn Sie hier mit „yes“ antworten, geben Sie bitte an, in welcher Detailtiefe die Daten erfasst werden (z. B. nur die Patienten-ID, eine Liste der Dokumenten-IDs).
AUDT-2.8.1	Fernwartung oder Vor-Ort-Wartung?			Wenn Sie hier mit „yes“ antworten, geben Sie bitte an, welche Arten der Service-Aktivitäten aufgezeichnet werden.
AUDT-2.8.2	Programmierschnittstellen (API) und ähnliche Aktivitäten?			Wenn Sie hier mit „yes“ antworten, geben Sie bitte die proprietären und die standardmäßigen Netzwerk APIs, wie z. B. FHIR bei HL7, an, die das Produkt unterstützt und deren Erfassung für die Audit-Protokolle. Weisen Sie bitte zusätzlich darauf hin, ob

AUDT-2.9	Notfall-Zugriff?			Wenn Sie hier mit „yes“ antworten, spezifizieren Sie bitte, welche Daten bei einem Notfall-Zugriff abgefragt werden und wie der Notfall-Zugriff dokumentiert wird.
AUDT-2.10	Andere Vorkommnisse, z. B. Software-Updates? Wenn ja, beschreiben Sie dies bitte im Freitextfeld.			
AUDT-2.11	Werden die Audit-Fähigkeiten detaillierter beschrieben? Wenn ja, beschreiben Sie dies bitte im Freitextfeld.			
AUDT-3	Kann der Betreiber/Bediener selbständig auswählen oder festlegen, welche Vorkommnisse im Audit-Protokoll protokolliert werden? Wenn ja, beschreiben Sie dies bitte im Freitextfeld.			
AUDT-4	Existiert eine Liste der Attribute der Daten, die im Audit-Protokoll für ein Ereignis erfasst werden? Wenn ja, beschreiben Sie dies bitte in einem Freitextfeld.			Bitte geben Sie hier die Datenattribute an, die im Audit-Protokoll erfasst werden oder verweisen Sie auf die Produktdokumentation.
AUDT-4.1	Erfasst das Audit-Protokoll Datum und Zeit?			
AUDT-4.1.1	Können das Datum und die Zeit über das Netzwerk Zeit Protokoll (NTP) oder eine gleichwertige Zeitquelle synchronisiert werden?			Geben Sie hier bitte an, wie die Zeit gesetzt werden kann, wenn nicht NTP genutzt wird.
AUDT-5	Können Audit-Log Inhalte exportiert werden?			
AUDT-5.1	Über physische Medien?			

AUDT-5.2	Über IHE Audit Trail und Node Authentication (ATNA) Profile nach SIEM?			
AUDT-5.3	Über andere Kommunikations-verfahren (z. B. externe Service-geräte, mobile Anwendungen)? Wenn ja, beschreiben Sie dies bitte im Freitextfeld.			
AUDT-5.4	Werden die Audit-Protokolle wäh-rend des Transports oder auf den Speichermedien verschlüsselt? Wenn ja, beschreiben Sie dies bitte im Freitextfeld.			
AUDT-6	Können Audit-Protokolle durch den Kunden überwacht/geprüft werden? Wenn nein, beschreiben Sie bitte den Audit-Prozess im Freitextfeld.			
AUDT-7	Werden die Audit-Protokolle vor Veränderung/Löschung geschützt? Wenn ja, beschreiben Sie dies bitte im Freitextfeld.			
AUDT-7.1	Werden die Audit-Protokolle vor dem Zugriff geschützt? Wenn ja, beschreiben Sie dies bitte im Freitextfeld.			
AUDT-8	Können Audit-Protokolle durch das Produkt selbst analysiert werden? Wenn ja, beschreiben Sie dies bitte im Freitextfeld.			

Fragenkatalog nach Leitfaden „Sicherheit von Medizinprodukten“ der Allianz für Cyber-Sicherheit

9.8 5 Fragenkatalog AUTH: Berechtigungen

FragenID	Frage	“yes”, “no” oder “n/a”	Antwort	Hinweise
AUTH-1	Verhindert das Produkt einen unautorisierten Zugriff durch eine Nutzeranmeldung oder andere Mechanismen?			Falls dem so ist, geben Sie bitte an, welche physischen oder technischen Sicherheitsmaßnahmen (Passwort, biometrische Merkmale, Chipkarten, Schlüsselkarten, etc.) durch das Produkt genutzt werden, um
AUTH-1.1	Kann das Produkt so konfiguriert werden, dass es zentrale Verwaltungssysteme für die Benutzeranmeldung (z. B. LDAP, OAuth) zur Autorisierung der Nutzer verwendet? Wenn ja, beschreiben Sie dies bitte im Freitextfeld.			
AUTH-1.2	Können Kunden Gruppenrichtlinien (Policies) auf das Produkt übertragen (z. B. Active Directory)?			
AUTH-1.3	Werden spezielle Benutzergruppen, organisatorische Einheiten oder Gruppenrichtlinien (Policies) benötigt? Wenn ja, beschreiben Sie diese bitte im Freitextfeld.			

AUTH-2	Können Nutzer abgestufte Rechte zugeteilt bekommen, die auf dem Rollenprinzip basieren (z. B. Gast, regulärer Nutzer, Administrator)?			
AUTH-3	Kann der Kunde des Produkts unbeschränkte administrative Rechte erlangen (z. B. auf das Betriebssystem oder lokale Applikationen über lokale Root-Rechte, bzw. den Administrator-Account)?			Bei einer Antwort mit „yes“, geben Sie bitte an, ob das Produkt mehrere privilegierte Benutzerkonten (z. B. Administrator, Root-Rechte) unterstützt und ob es Einschränkungen für Nutzer gibt, den Administrator-Account zu benutzen. Es sollte zudem deutlich zwischen Betreiber, einschließlich Installation, Wartung und Außerbetriebnahme, und Bediener, hier ist der Benutzer im medizinischen Normalbetrieb gemeint, unterschieden werden.
AUTH-4	Werden alle Zugriffe zu Netzwerk-Schnittstellen (API) über eine Zugriffsautorisierung gesteuert? Falls nicht, erläutern Sie dies bitte im Freitextfeld.			Bitte stellen Sie hier die detaillierte Zugriffsautorisierung dar.
AUTH-5	Läuft das Produkt standardmäßig in einem eingeschränkten Zugriffsmodus oder im Kiosk Modus (Auto-Login)? Wenn ja, beschreiben Sie dies bitte im Freitextfeld.			

Fragenkatalog nach Leitfaden „Sicherheit von Medizinprodukten“ der Allianz für Cyber-Sicherheit

9.9 6 Fragenkatalog CSUP: Sicherheitsupgrades für das Produkt

FragenID	Frage	“yes”, “no” oder “n/a”	Antwort	Hinweise
CSUP-1	Läuft auf dem Produkt irgendwelche Software oder Firmware (damit ist sowohl vom Hersteller selbst als auch durch Drittanbieter hergestellte Software gemeint), die Sicherheits- Updates während ihrer geplanten Verwendungszeit benötigt. Wenn nicht, dann überspringen Sie dieses Kapitel.			Geben Sie bitte an, welche Randbedingungen es beim Aufspielen von Sicherheits-Updates gibt und verweisen Sie auf die Produktdokumentation, die diese Randbedingungen näher bezeichnet.
CSUP-2	Beinhaltet das Produkt ein Betriebssystem? Wenn ja, füllen Sie bitte die nachfolgenden Fragen, bis einschließlich 2.4 aus.			Geben Sie bitte an, welche Randbedingungen es beim Aufspielen von Sicherheits-Updates gibt und verweisen Sie auf die Produktdokumentation, die diese Randbedingungen näher bezeichnet. Wenn Sie „no“ angeben und ein Betriebssystem erforderlich ist (SaMD), beantworten Sie bitte auch die Fragen bis einschließlich 2.4.
CSUP-2.1	Liefert die Produktdokumentation Anleitungen für den Bediener oder Betreiber, wie Software-Patches oder Updates des Betriebssystems durchgeführt werden?			

CSUP-2.2	Benötigt das Produkt den Hersteller oder herstellereigenen Service, um Software-Patches oder Updates für das Betriebssystem durchzuführen?			
CSUP-2.3	Ist es möglich Software-Patches und Updates für das Betriebssystem auf dem Produkt per Fernwartung zu installieren?			
CSUP-2.4	Ist es erlaubt, dass Sicherheits- Updates für das Betriebssystem durch Dritt-Komponenten-Anbieter (z. B. Microsoft) ohne vorherige Freigabe des Herstellers installiert werden?			Geben Sie bitte auch dann „no“ an, wenn es eine generische, vom Hersteller vorgegebene Freigabeprozedur gibt und erklären Sie diese.
CSUP-3	Beinhaltet das Produkt Treiber und Firmware? Wenn ja, füllen Sie bitte die nachfolgenden Fragen, bis einschließlich 3.4 aus.			Geben Sie bitte an, welche Randbedingungen es beim Aufspielen von Sicherheits-Updates gibt und verweisen Sie auf die Produktdokumentation, die diese Randbedingungen näher bezeichnet.
CSUP-3.1	Liefert die Produktdokumentation Anleitungen für den Bediener oder Betreiber, wie Software-Patches oder Updates für das Produkt selbst durchgeführt werden?			
CSUP-3.2	Benötigt das Produkt den Hersteller oder herstellereigenen Service, um Software-Patches oder Updates für das Produkt selbst durchzuführen?			

CSUP-3.3	Ist es möglich Software-Patches und Updates für das Produkt selbst auf dem Produkt per Fernwartung zu installieren?			
CSUP-3.4	Ist es erlaubt, dass Sicherheits-Updates für das Produkt selbst durch Dritt-Komponenten-Anbieter (z. B. Microsoft) ohne vorherige Freigabe des Herstellers installiert werden?			Diese Frage zielt auf den Fall, dass das Produkt Komponenten von Dritt-Anbietern enthält.
CSUP-4	Benutzt das Produkt Anti-Schadsoftware? Wenn ja, füllen Sie bitte die nachfolgenden Fragen, bis einschließlich 4.4 aus.			Geben Sie bitte an, welche Randbedingungen es beim Aufspielen von Updates dieser Anti-Schadsoftware gibt und verweisen Sie auf die Produktdokumentation, die diese Randbedingungen näher bezeichnet.
CSUP-4.1	Liefert die Produktdokumentation Anleitungen für den Bediener oder Betreiber, wie Software-Patches oder Updates der Anti-Schadsoftware durchgeführt werden?			
CSUP-4.2	Benötigt das Produkt den Hersteller oder herstellereigenen Service, um Software-Patches oder Updates der Anti-Schadsoftware durchzuführen?			
CSUP-4.3	Ist es möglich Software-Patches und Updates der Anti-Schadsoftware auf dem Produkt per Fernwartung zu installieren?			
CSUP-4.4	Ist es erlaubt, dass Sicherheits- Updates der Anti-Schadsoftware durch Dritt-Komponenten-Anbieter (z. B. Microsoft) ohne vorherige Freigabe des Herstellers installiert werden?			

CSUP-5	Beinhaltet das Produkt weitere handelsübliche (Software-) Komponenten (COTS), die nicht zum Betriebssystem gehören? Wenn ja, füllen Sie bitte die nachfolgenden Fragen, bis einschließlich 5.4 aus.			Geben Sie bitte an, welche Randbedingungen es beim Aufspielen von Sicherheits-Updates gibt und verweisen Sie auf die Produktdokumentation, die diese Randbedingungen näher bezeichnet.
CSUP-5.1	Liefert die Produktdokumentation Anleitungen für den Bediener oder Betreiber, wie Software-Patches oder Updates dieser handelsüblichen Komponenten durchgeführt werden?			
CSUP-5.2	Benötigt das Produkt den Hersteller oder herstellereigenen Service, um Software-Patches oder Updates dieser handelsüblichen Komponenten durchzuführen?			
CSUP-5.3	Ist es möglich Software-Patches und Updates dieser handelsüblichen Komponenten auf dem Produkt per Fernwartung zu installieren?			
CSUP-5.4	Ist es erlaubt, dass Sicherheits- Updates dieser handelsüblichen Komponenten durch Dritt- Komponenten-Anbieter (z. B. Microsoft) ohne vorherige Freigabe des Herstellers installiert werden?			

CSUP-6	Gibt es auf dem Produkt weitere Software-Komponenten (z. B. Assetmanagement-Software oder Lizenzverwaltungsprogramme)? Wenn ja, füllen Sie bitte die nachfolgenden Fragen, bis einschließlich 6.4 aus.			Geben Sie bitte an, welche Randbedingungen es beim Aufspielen von Sicherheits-Updates gibt und verweisen Sie auf die Produktdokumentation, die diese Randbedingungen näher bezeichnet.
CSUP-6.1	Liefert die Produktdokumentation Anleitungen für den Bediener oder Betreiber, wie Software-Patches oder Updates der weiteren Software-Komponenten durchgeführt werden?			
CSUP-6.2	Benötigt das Produkt den Hersteller oder herstellereigenen Service, um Software-Patches oder Updates der weiteren Software-Komponenten durchzuführen?			
CSUP-6.3	Ist es möglich Software-Patches und Updates der weiteren Software-Komponenten auf dem Produkt per Fernwartung zu installieren?			
CSUP-6.4	Ist es erlaubt, dass Sicherheits- Updates der weiteren Software- Komponenten durch Dritt- Komponenten-Anbieter (z. B. Microsoft) ohne vorherige Freigabe des Herstellers installiert werden?			
CSUP-7	Informiert der Hersteller den Kunden, wenn Updates zur Installation freigegeben worden sind? Wenn ja, beschreiben Sie dies bitte genauer im Freitextfeld.			Bitte geben Sie hier an, über welchen Kommunikationskanal Sie diese Informationen zur Verfügung stellen und ob es sich um das Betriebssystem, die Hauptapplikations-Software, Anti- Schadsoftware, kommerzielle Software oder um weitere Komponenten handelt.

CSUP-8	Kann das Produkt automatisch Software-Updates installieren?			Bitte geben Sie hier an, ob es sich um das Betriebssystem, die Hauptapplikations-Software, Anti- Schadsoftware, kommerzielle Software oder um weitere Komponenten handelt.
CSUP-9	Hat der Hersteller eine Liste von geprüfter Dritt-Anbieter-Software, die auf dem Produkt installiert werden kann? Wenn ja, referenzieren Sie dies bitte in einem Freitextfeld.			Geben Sie bitte die Liste der geprüften Dritt-Anbieter- Software an oder verweisen Sie auf diese. Zudem beschreiben Sie bitte den Genehmigungsprozess bei Anfragen von weiterer Dritt-Anbieter-Software.
CSUP-10	Kann der Betreiber/Bediener vom Hersteller freigegebene Software von Dritt-Anbietern auf dem Produkt installieren?			Hier sollten Sie bitte zwischen den unterschiedlichen Rollen unterscheiden und ob es beispielsweise möglich ist, dass auch Anwender Installationsrechte erhalten.
CSUP-10.1	Verfügt das Produkt über einen Mechanismus, um der Installation von nicht geprüfter Software vorzubeugen?			Bitte geben Sie hier auch Whitelisting-Software an.
CSUP-11	Verfügt der Hersteller über einen Prozess, um Schwachstellen und Updates zu bewerten?			Hier ist es auch möglich den Prozess verallgemeinert darzustellen und eine entsprechende Fallunterscheidung
CSUP-11.1	Verfügt der Hersteller über einen Prozess, der den Kunden regelmäßig über Updates, mit einem Bewertungs- und Genehmigungsstatus, informiert?			(Betriebssystem, Hauptapplikations-Software, Anti-Schadsoftware, kommerzielle Software oder weitere Komponenten) vorzunehmen.
CSUP-11.2	Gibt es einen regelmäßigen Update- Zyklus? Wenn ja, beschreiben Sie diesen bitte im Freitextfeld.			

Fragenkatalog nach Leitfaden „Sicherheit von Medizinprodukten“ der Allianz für Cyber-Sicherheit

9.10 7 Fragenkatalog DIDT: De-Identifikation von Gesundheitsdaten

FragenID	Frage	“yes”, “no” oder “n/a”	Antwort	Hinweise
DIDT-1	Verfügt das Produkt über einen eingebauten Mechanismus, um personenbezogene Daten zu de- identifizieren?			Bitte geben Sie hier an, ob sich der Anonymisierungs- oder Pseudonymisierungs-Prozess nach einem Standard oder einer Hilfestellung richtet und ob der Mechanismus verschieden konfiguriert werden kann.
DIDT-1.1	Unterstützt das Produkt eine Anonymisierung von Profilen nach dem DICOM-Standard? Wenn ja, beschreiben Sie dies bitte im Freitextfeld.			DICOM-Standards werden bei medizinischen, bildgebenden Verfahren verwendet.

Anlagen, Teil 2: Weitere Informationen BSI

Weitere Informationen aus BSI IT-Grundschutz-Kompendium zu ausgewählten Komponenten:

Audits und Revisionen DER.3.1

„Audits und Revisionen sind grundlegend für jedes erfolgreiche Managementsystem für Informationssicherheit (ISMS). Nur wenn etablierte Sicherheitsmaßnahmen und -prozesse regelmäßig daraufhin überprüft werden, ob sie noch wirksam, vollständig, angemessen und aktuell sind, lässt sich der Gesamtzustand der Informationssicherheit beurteilen. Audits und Revisionen sind somit ein Werkzeug, um ein angemessenes Sicherheitsniveau festzustellen, zu erreichen und aufrechtzuerhalten. Durch Audits und Revisionen ist es möglich, Sicherheitsmängel und Fehlentwicklungen zu erkennen und entsprechende Gegenmaßnahmen zu ergreifen."

Allgemeiner Verzeichnisdienst APP.2.1

„Ein Verzeichnisdienst stellt in einem Datennetz Informationen über beliebige Objekte in einer definierten Art zur Verfügung. In einem Objekt können zugehörige Attribute gespeichert werden, zum Beispiel können zu einer Kennung der Name und Vorname des oder der Benutzenden, die Personalnummer und der Name des IT-Systems abgelegt werden. Diese Daten können dann gleichermaßen von verschiedenen Applikationen verwendet werden. Der Verzeichnisdienst und seine Daten werden in der Regel von zentraler Stelle aus verwaltet.

Einige typische Anwendungsgebiete von Verzeichnisdiensten sind:

- Verwaltung von Adressbüchern, z. B. für Telefonnummern, E-Mail-Adressen und Zertifikate für elektronische Signaturen
- Benutzendenverwaltung, z. B. zur Verwaltung von Konten und Berechtigungen
- Bereitstellung eines Backend-Dienstes für Authentifizierungsfunktionen, z. B. zur Anmeldung an Betriebssystemen oder Anwendungen

Verzeichnisdienste sind auf Lesezugriffe hin optimiert, da Daten aus dem Verzeichnisdienst typischerweise vorwiegend abgerufen werden. Schreibzugriffe, bei denen Einträge erstellt, geändert oder gelöscht werden, sind seltener notwendig.

Wenn ein Verzeichnisdienst eingesetzt wird, können manche Verwaltungsaufgaben innerhalb des Netzes, wie z. B. Kontenerstellung, Passwortänderungen und Zuweisungen von Rollen und Gruppen, an zentraler Stelle durchgeführt werden."

OpenLDAP APP.2.3

„OpenLDAP ist ein frei verfügbarer Verzeichnisdienst, der in einem Datennetz Informationen über beliebige Objekte, beispielsweise Konten, IT-Systeme oder Konfigurationen, in einer standardisierten und definierten Art zur Verfügung stellt. Die Informationen können einfache Attribute wie die Namen oder Nummern von Objekten oder auch komplexe Formate wie Fotos oder Zertifikate für elektronische Signaturen umfassen. Typische Einsatzgebiete sind zum Beispiel Adressbücher oder Kontenverwaltungen, aber auch Konfigurationen.

OpenLDAP stellt eine Referenz-Implementierung für einen Server-Dienst im Rahmen des Lightweight Directory Access Protocols (LDAP) dar. Als Open-Source-Software kann OpenLDAP auf einer Vielzahl von Betriebssystemen installiert werden und gilt als einer der am meisten verbreiteten Verzeichnisdienste. Zur Besonderheit von OpenLDAP gehören die *Overlays*. Overlays erweitern den Funktionsumfang von OpenLDAP um zahlreiche Funktionen und werden auch für grundlegende Funktionen wie Protokollierung, Replikation und die Wahrung der Integrität verwendet.“

Unified Communications und Collaboration (UCC) APP.5.4

„Unified Communications bezeichnet einen Dienst, der verschiedene Kommunikationsdienste in einer Anwendung und in der Regel auch einem Softclient vereint. Damit wird der Anteil der traditionellen Telefonie in der persönlichen digitalen Kommunikation reduziert. Die möglichen Kommunikationswege werden um zusätzliche Dienste wie Video, diverse Formen von Chats und Erreichbarkeitsanzeigen erweitert.

Eine Kommunikationsbeziehung zwischen zwei oder mehr Teilnehmenden wird unabhängig vom benutzten Dienst als Konversation bezeichnet.“

IBM Z SYS.1.7

„Systeme vom Typ „IBM Z“ gehören zu den Server-Systemen, die allgemein als Großrechner („Mainframes“) bezeichnet werden. Großrechner haben sich von klassischen Einzelsystemen mit Stapelverarbeitung hin zu modernen Client-Server-Systemen entwickelt. Die Z-Architektur ist der Nachfolger der 1964 eingeführten S/360-Architektur und wird bei heutigen Großrechner-Installationen häufig eingesetzt.“

Terminalserver SYS.1.9

„Ein Terminalserver ist ein Server, auf dem Client-Anwendungen (kurz Anwendungen) direkt ausgeführt werden und der nur deren grafische Oberfläche (Bedienoberfläche) an die Clients weiterleitet. Hierfür wird eine Terminalserver- Software verwendet. Der Terminalserver ist dann das zugrundeliegende IT-System, auf dem diese Software ausgeführt wird. Die Eingaben am Client, z. B. über Tastatur und Maus, werden an die

Terminalserver-Software übertragen, die diese Eingaben dann dem Terminalserver übergibt. In der bereitgestellten Anwendung auf dem Terminalserver werden daraufhin die Aktionen ausgeführt, die gegebenenfalls durch die Eingaben ausgelöst werden und der Terminalserver ermittelt die neue (möglicherweise geänderte) Bedienoberfläche. Diese Bedienoberfläche wird dann von der Terminalserver-Software an den Client übertragen."

Virtual Desktop Infrastructure SYS.2.6

„Eine Virtual Desktop Infrastructure (VDI) steuert und verwaltet standardisierte virtuelle Clients. Hierdurch können zentralisiert einzelne Anwendungen (z. B. Office-Programme) oder ganze Desktops zur Verfügung gestellt werden. Virtuelle Clients sind dabei virtualisierte IT-Systeme, auf die über Terminalserver-Protokolle zugegriffen werden kann. Die virtuellen Clients werden auf Virtualisierungsservern ausgeführt, die mit einem Managementsystem zu einer Virtualisierungsinfrastruktur zusammengefasst werden (siehe Bausteine SYS.1.5 *Virtualisierung* und SYS.2.5 *Client-Virtualisierung*)."

Prozessleit- und Automatisierungstechnik IND.1

„Prozessleit- und Automatisierungstechnik (Operational Technology, OT) ist Hard- und Software, die physische Geräte, Prozesse und Ereignisse in der Institution überwacht und steuert.

In der Industrie, zu der unter anderem auch die Kritischen Infrastrukturen gehören, zählen dazu insbesondere industrielle Steuerungssysteme (Industrial Control Systems, ICS) und Automationslösungen, die dort Steuerungs- und Regelfunktionen aller Art übernehmen. Weitere Beispiele sind Laborgeräte, z. B. automatisierte Mikroskope oder Analysewerkzeuge, Logistiksysteme, wie Barcodescanner mit Kleinrechner, oder Gebäudeleittechnik."

Allgemeine ICS-Komponente IND.2.1

„Eine ICS-Komponente ist eine elektronische Komponente, die eine Maschine oder Anlage steuert oder regelt. Sie ist damit Bestandteil eines industriellen Steuerungssystems (englisch Industrial Control System, ICS) oder allgemeiner einer Betriebstechnik (englisch Operational Technology, OT). Diese Komponenten können Speicherprogrammierbare Steuerungen (SPS) (englisch Programmable Logic Controller, PLC), Sensoren, Aktoren, eine Maschine oder andere Teile eines ICS sein."

Maschine IND.2.4

„Eine Maschine ist eine technische Vorrichtung, die automatisierte Aufgaben durchführt. Ein typisches Beispiel dafür ist eine Werkzeugmaschine, die Werkstücke auf eine vorgegebene Art bearbeitet. Dabei wird sie von einem IT-System gesteuert, das die

entsprechenden Arbeitsanweisungen und -schritte vorgibt. Solche Maschinen werden auch als Automaten bezeichnet.“

Verkabelung NF.12

„Die ordnungsgemäße und normgerechte Ausführung der Verkabelung ist Grundlage für einen sicheren IT-Betrieb. Dabei muss grundsätzlich zwischen der elektrotechnischen Verkabelung und der IT-Verkabelung unterschieden werden.“

Anlagen, Teil 3: BSI-CS 132 mit Beispiel

BSI-Empfehlungen für netzwerkfähige Medizinprodukte, BSI-CS 132, Version 1, mit Beispiel

Für jede Position wurde eine Kategorie (Kat.) festgelegt, die den Schwierigkeitsgrad bei Umsetzung und Prüfung wiederspiegelt. Hierbei steht:

1 für umsetzbar mit guten IT-Kenntnissen,
2 für umsetzbar durch IT-Experten,
3 für umsetzbar durch IT-Sicherheitsexperten.

Gute IT-Kenntnisse besitzt jemand, der sicher im Umgang mit der IT als Arbeitsmittel ist, selbständig Programme / Applikationen sowohl installieren als auch deinstallieren kann, Sich mit den allgemeinen Anforderungen an die IT-Sicherheit insofern auskennt, dass er durch betriebsinterne Schulungen die häufig auftretenden Gefährdungen kennt und bewältigt, wie beispielsweise Erkennung von Emails mit unzulässigen Anhängen, Sicherheit von Webseiten (http vs. shttp) und deren Seriosität grundsätzlich einschätzen kann.

IT-Experten sind Personen, welche sich auf dem Niveau eines Systemadministrators bewegen, damit beispielsweise über Ports, Protokolle und Rechtevergaben grundlegend Bescheid wissen, Logfiles erkennen und auslesen können und das grundlegende Zusammenspiel der Komponenten eines Netzwerkes verstehen.

IT-Sicherheitsexperten sind Personen, deren Kenntnisse über das allgemeine Niveau eines IT-Experten hinaus gehen, mittels Schulungen zum Thema IT-Sicherheit auf dem technisch aktuellen Stand bezüglich auftretender Gefahren und deren Gegenmaßnahmen sind, oder Spezialkenntnisse bezüglich einzelner sicherheitsrelevanter Bausteine haben, wie beispielsweise zu verschiedenen kryptographische Verfahren oder Softwareverknüpfungen auf Betriebssystemebene besitzen.

Entsprechend kann es für das Prüfinstitut notwendig werden, dass für Medizinprodukte, welche notwendige Dokumentationen bezüglich Kategorie 3 aufweisen oder aufweisen sollten, IT-Sicherheitsexperten mit der Beurteilung der Dokumentation und ggf. des Prüfobjekts hinzugezogen werden sollten. Letztlich wird dieses von den tatsächlichen IT-Fähigkeiten der mit der Prüfung beauftragten Personen abhängen.

9.11 Für alle Betriebsarten

	Fragestellung	Kommentar	Beispiel Insulinpumpe	Kat.
1	**Identifizierung**			
1.1	Dokumentation aller Schnittstellen	Grundlage für das systematische Abarbeiten von potentiellen Risiken Schnittstellen sollten mit Bezeichnung, zugehörigen Protokollen und zugehörigen Daten mit Bestimmungsort erfasst werden.	Sensor: Bluetooth Pumpe: Bluetooth Steuergerät: Bluetooth, WLAN, USB	2
1.2	Bestimmung des maximal möglichen Schadens, der durch Angriffe auf diese Schnittstelle entstehen kann	Grundlage für die Bestimmung der Schweregrade der Risiken	zu hoher Insulinspiegel: Ernst zu niedriger Insulinspiegel: Katastrophal unberechtigter Zugriff auf personenbezogene Daten: Ernst	2

	Fragestellung	Kommentar	Beispiel Insulinpumpe	Kat.
2	**Klärung der Fragen**			
2.1	Welche Schnittstellen gibt es und was passiert, wenn unerwartete Signale auf diese gegeben werden	Siehe Punkt a) Identifizierung	Geeignet: Tabellarische Darstellung Komponente, Schnittstelle, Schadenspotential	2
2.2	Welche anderen Komponenten sind anschließbar und was kann dadurch passieren	Auflistung der möglichen Anschlüsse und welche Folgen sich daraus ergeben können. Wie sind die Anschlüsse dagegen abgesichert?	USB-Anschluss des Steuergerätes; Zugriff auf Daten nur über zugehörige Herstellersoftware und Authentifizierung, andere Hardware kann physisch angeschlossen werden, jedoch nicht auf die Daten oder das Programm zugreifen.	2
2.3	Wie werden die Komponenten angeschlossen (physischer Verbindungstyp) und welches Risiko geht von dieser Technologie aus	Auflistung	USB-Schnittstelle des Steuergerätes, USB-Schnittstelle des Smartphones	1

2.4	In welche Richtung geht der Signalfluss / Datenfluss und kann dieser auch in eine andere Richtung gehen	Verbindungen auflisten mit zugehöriger Datenflussrichtung. Bei einseitigem Datenfluss angeben, wodurch der Datenfluss in die andere Richtung verhindert wird	Datenfluss von und zum Steuergerät (bidirektional) zum Auslesen von Daten, Logs etc. und zur Konfiguration.	1
2.5	Welche Daten / Signale fließen, können sie geändert, gelöscht oder zugefügt werden, wie sind sie vor Zugriff Unberechtigter geschützt	Auf welche Daten ist ein Zugriff möglich, wie ist die Rechtezuweisung und wie sind diese vor Manipulation geschützt. Datenarten sollten hier aufgelistet werden, mit Informationen zu Rechten und Zugriffsschutz als Basis zur Einschätzung des Risikos durch Manipulation	Konfigurationsdaten können gelesen und durch authentifizierten Zugriff überschrieben werden. Messdaten und Insulinabgabe gespeichert in Datenbank können über die Schnittstelle nur gelesen werden, Datenbank arbeitet nach dem First-in-First- out-Prinzip. Logfiles können nur gelesen werden, alle Zugriffsversuche, Fehlermeldungen, abgesetzte Alarme werden automatisch geloggt. Bei Überschreiten einer festgelegten Dateigröße der Logfiles (z.B. durch Anzahl an Fehlversuchen des potentiell unberechtigten Einloggens) erscheint eine Meldung zum Aufsuchen des Herstellerservices, um Manipulationsversuche oder Fehlfunktion auszuschließen. (Internes Kontrollprogramm)	2
2.6	Welche Risiken können daraus für die Beteiligten erwachsen, sind diese im akzeptablen Bereich oder braucht es risikomindernde Maßnahmen	Angaben zur durchgeführten Risikobewertung und Risikoakzeptanz	Die Gefahr eines zu hohen oder zu niedrigen Insulinspiegels kann durch absichtliche oder unabsichtliche Manipulation an Daten entstehen, Risikominimierungsmaßnahmen wurden getroffen und das Risiko wurde in einen akzeptablen Bereich geführt.	1

	Fragestellung	Kommentar	Beispiel Insulinpumpe	Kat.
3	**Cybersicherheitsspezifische Produkteigenschaften zur Minderung der zuvor identifizierten Gefahren**			
3.1	Ist eine Systemhärtung des Betriebssystems und aller Anwendungen erfolgt? Sind für den Betrieb nicht benötigte Anwendungen abgeschaltet oder wird der Anwender auf eine Abschaltung hingewiesen? Werden sichere Protokollalternativen verwendet (z.B. https statt http)?	Kann z.B: durch Anwendung des IT- Grundschutzprotokolls des BSI nachgewiesen werden.	Betriebssysteme: - Sensor: NuttX (Microcontroler) - Pumpe: NuttX (Microcontroler) - Steuergerät: MicroC (zertifiziert nach ISO62304) - Smartphone: iOS, Android mit Sandboxing	2
3.2	Werden nach Stand der Technik nur absicherbare Technologien verwendet?	Konnten die Empfehlungen des BSI zum Grundschutz erfolgreich angewendet werden?		2
3.3	Wurde die Implementierung der grundlegenden Kommunikationsprotokolle einer Testung auf Toleranz und Robustheit unterzogen?	z. B. Blackbox / Whitebox-Tests		3
3.4	Standardimplementierung oder Eigenentwicklung von Diensten und Protokollen	Angaben zu verwendeten Diensten und Protokollen, möglichst mit zugehörigen Sicherheits- oder Zertifizierungsangaben. Für Eigenentwicklungen kann eine Bewertung der Sicherheit der Dienste und Protokolle durch IT- Spezialisten notwendig werden, da es hier um das Erkennen von Schwachstellen geht, welche noch unbekannt sind.	Für das Steuergerät wurde das kostenpflichtige Betriebssystem MicroC gewählt, welches nach ISO 62304 für Medizingeräte zertifiziert ist.	3
3.5	Sensible Daten geschützt gespeichert und übertragen?			

3.5.1	Standardimplementierung und anerkannte Algorithmen der Kryptographie oder Eigenentwicklung	Angaben, welche Verschlüsselungsmethoden zum Einsatz kommen. Bei Eigenentwicklung kann es notwendig sein, dass ein IT- Spezialist mit Kenntnissen der Kryptographie zur Überprüfung der Eignung des Verfahrens hinzugezogen werden muss.	Zugriffsdaten aller Komponenten des Systems werden mit SHA512 (kryptographische Hashfunktion) gespeichert.	3
3.5.2	Wird die Vorschrift TR- 02102 des BSI zu Kryptoverfahren eingehalten?	Welche Algorithmen kommen zum Einsatz? Bei Eigenentwicklungen kann es notwendig sein, das Einhalten der Empfehlung durch einen IT- Spezialisten mit Kenntnissen der Kryptographie bei der Überprüfung hinzu zu ziehen.	SHA 512 ist ein standardisierter und empfohlener Algorithmus	3
3.5.3	Sind Integritäts-checks bzgl. sicherheits-relevanter Daten vorhanden?	Abhängig vom Ausmaß des Risikos kann eine Hinzuziehung eines IT- Spezialisten zur Bewertung der Eignung der ausgeführten Integritätschecks erforderlich sein.	Das durch die Insulinpumpe auszuführende Programm wird nach jeder Änderung SHA512 gehasht und in festgelegten Zeitabständenüberprüft.	3
3.5.4	Sind die Schnittstellen mit Eingabevalidierung ausgestattet (Verhinderung Manipulation)?	Sicherung der Schnittstellen vor unberechtigtem Zugriff, beispielsweise durch Authentifizierung	Eingaben nur nach vorheriger Authentifikation möglich	2
3.6	Kann das Netzwerk gehärtet betrieben werden?			
3.6.1	Segmentierung des Netzwerks vorhanden oder Hinweise dazu für den Anwender? Ist eine Trennung der Konfigurationsdaten vom medizinischen Betrieb vorhanden?	Haben Anwender Zugriff auf Konfigurationsdaten? Wie sind die Datenwege und die Rechte ausgelegt? Wurden unnötige Lese- und Schreibzugriffsrechte entfernt? Werden die Daten von Nutzerkonten getrennt abgelegt? Gibt es eine	Der Anwender hat nur eingeschränkte Rechte, Daten zu ändern. Eine Änderung von Konfigurationsdaten durch den Anwender ist nicht möglich. Der Anwender kann lediglich Injektionsmengen in einem festgelegten Toleranzbereich und begrenzt auf ein im Maximum festgelegtes Zeitfenster ändern.	2

		Zugriffsmöglichkeit von Komponenten auf andere Bestandteile der IT-Infrastruktur?		
3.6.2	Abschalten von nicht benötigten Diensten und Technologien möglich, wenn diese vom Anwender nicht benötigt werden?		Die Apps können sich aus dem System ausloggen. Der automatische Datenupload erfolgt durch täglich vorgesehenes einloggen auf den Server und einem unidirektionalen Upload der Daten. Bei Unterbrechung des Zyklus wird dieser wiederholt bis 30 Tage nach letztem Upload. Danach wir der Upload für den Nutzer dauerhaft deaktiviert. Der Konfigurationsmodus wird automatisch spätestens mit physischer Trennung verlassen, die Menüsteuerung des Steuergeräts deaktiviert sich ebenfalls zeitabhängig automatisch. Weitere nicht benötigte Technologien und Dienst gibt es nicht.	2
3.6.3	Wurden Dienste und Technologien nach Stand der Technik bestmöglich gehärtet oder Hinweise zur Umsetzung für den Anwender vorhanden?	Wurden die vom BSI empfohlenen Grundschutz-Maßnahmen zur Härtung des Systems durchgeführt? Wurde diese Härtung auf mit dem Medizingerät verbundene IT-Infrastruktur erweitert? Gibt es in der Dokumentation Hinweise auf notwendige Härtungsmaßnahmen für den Anwender, wenn das Gerät in die eigene IT zu integrieren ist?	BSI-Grundschutz, Zugriffe auf Konfiguration und Daten erfolgt nur nach Authentifizierung.	2
3.7	Client-Server-Betrieb abgesichert			
3.7.1	Werden die Parameter für die Cybersicherheit (wie Cookies) serverseitig berechnet und geprüft?		Sitzungscookies werden serverseitig berechnet und zeitabhängig entwertet	1

3.7.2	Werden alle Eingaben des Clients serverseitig validiert?		Logindaten und Sitzungscookies werden geprüft	1
3.8	feingranulare Zugriffskontrolle (Login/ Authentifizierung) zum Schutz sensibler Daten vorhanden und ist die Benutzerverwaltung hinreichend?			1
3.8.1	Zugangsdaten (z.B. Passwörter) kryptographisch gespeichert?		Mittels SHA512+Salt	1
3.8.2	Bei fehlerhaftem Login eine Fehlermeldung, welche keinen Hinweis auf die Art des Fehlers des Logins ermöglicht (z.B. kein Hinweis, dass Passwort oder Anmeldename falsch)		Einfacher Hinweis “Login fehlerhaft”	1
3.8.3	Kann der Netzwerkzugriff auf bestimmte MAC- Adressen, IP-Adressen oder Adressbereiche beschränkt werden?		App und Steuergerät können nur mit Herstellerserver verbinden (IP-Freigabe), Bluetooth- Verbindungen werden bei Inbetriebnahme vom Fachpersonal gekoppelt.	1
3.8.4	ergänzende Maßnahmen zur Absicherung eines Zugriffs		Zeitabhängiger Logout	1
3.8.5	Welche Software oder Prozesse laufen mit Systemprivilegien und wie sind diese geschützt?	Hier kann die Überprüfung durch einen IT-Spezialisten mit Kenntnissen im Bereich Betriebssysteme zur Beurteilung erforderlich werden	Sandboxing der Smartphone-App	3
3.9	Gibt es für Mehrnutzeranwendung ein abgesichertes Session-Management?			2

3.9.1	Verhinderung der Ausführung kritischer Aktionen ohne die dazu notwendigen Rechte?	Hier kann die Überprüfung durch einen IT-Spezialisten mit Kenntnissen im Bereich Betriebssysteme zur Beurteilung erforderlich werden	Authentifikation für alle Aktionen Notwendig	3
3.9.2	Sessions untereinander geschützt?	Hier kann die Überprüfung durch einen IT-Spezialisten mit Kenntnissen im Bereich Betriebssysteme zur Beurteilung erforderlich werden	keine Mehrfachsessions erlaubt	3
3.9.3	Gibt es ein Timeout (Abbruchzeitpunkt) der Sessions und ist dieser konfigurierbar?		Timeout für Sessions sowohl für Steuergerät, als auch Smartphone-App	1
3.9.4	Kann ein Angriff auf die Verfügbarkeit, welcher durch zu viele offene Verbindungen realisiert werden könnte, mit entsprechenden Vorkehrungen verhindert oder mindestens erschwert werden?	Hier kann die Überprüfung durch einen IT-Spezialisten mit Kenntnissen im Bereich Betriebssysteme zur Beurteilung erforderlich werden	Mehrfachverbindungen nicht möglich	3
4	Sonstige Cybersicherheitsfunktionen			
4.1	Erkennung und Schutz vor Schadprogrammen notwendig und möglich?		Keine Speichermöglichkeit von Schadware für Pumpe, Sensor und Steuergerät	2
4.2	Denial-of-Service: bleibt Funktionalität erhalten und wird der normale Betrieb automatisch wieder		Kontakt der Pumpe zum Sensor und Steuergerät darf unterbrochen werden, es erfolgt in dem Falle zeitabhängig die Ausführung mit letzter Einstellung und Rückstellung zum Grundprogramm.	2
4.3	Update-Mechanismen (Firmware) ausreichend abgesichert? Integritätsprüfung über Prüfsumme, Authentifizierung		Ja, im Rahmen einer Serviceleistung durch zertifizierte Dienstleister auszuführen.	2

	und Absicherung über Signaturen?			
4.4	Standardverfahren oder nutzerfreundliche Mechanismen für Backups und Wiederherstellung vorhanden?		Nicht zutreffend	1
5	Cybersicherheit zur Erkennung von Angriffen			
5.1	Logging			
5.1.1	Logdaten kritischer Aktionen (geänderte Konfiguration, fehlerhafte Logins, Konnektierung und Trennung von Speichern oder USB-Geräten etc.)?		Implementiert	2
5.1.2	Wird ein Zugriff auf geschützte Daten über die Logdaten verhindert?		Ja	2
5.2	Auswertung der Logdaten			
5.2.1	Möglichkeit automatisierter Alarmierung bei kritischen Ereignissen vorhanden?		Ja, Alarm für mehrfach fehlerhafte Logins, Alarm bei Überschreiten von Sollbereichen von Messwerten und Abgabewerten	1
5.2.2	Warnmeldung bei Brute- Force-Angriff auf den Login- Prozess vorhanden?		Ja	1

9.12 Für die Konfiguration

	Fragestellung	Kommentar	Beispiel Insulinpumpe	Kat.
6	**Konfiguration:**			
	Konfiguration nur nach vorheriger Authentifizierung?		Ja	1
	sichere Standardkonfiguration bei Auslieferung?		Ja	2
	Passwörter, Zertifikate für alle Dienste austauschbar?		ja, jedoch für die tiefere Konfiguration, welche durch den Herstellerservice erfolgt, sind Passwörter, Zertifikate etc. nicht vom Anwender austauschbar.	1
	geschützte Konfiguration gegen unautorisierte Manipulation (Prüfsumme, Signatur)		Ja	2
	Bei Standard-IT für Konfiguration:			
	ausreichend abgesichert?	Hier ist zu prüfen, ob z.B. die Empfehlungen des BSI- Grundschutzkompendiums angewendet wurden.	Für das Beispiel wäre eine Dokumentation für den zertifizierten Service notwendig, welche die Anforderungen an den Konfigurationscomputer zur Einhaltung der Empfehlungen zu erfüllen sind. Hier ist zusätzlich in der Dokumentation für die Konformitätsbewertung aufzunehmen, wie die Umsetzung dieser Anforderungen gewährleistet und kontrolliert wird. (z.B. APP.1.2, APP.2.1)	3
	Empfehlungen und technische Richtlinien sauber implementiert?	Prüfung, welche zusätzlichen Empfehlungen, neben dem BSI- Grundschutz und BSI-CS 132 in Frage kommen und ob diese berücksichtigt wurden	Ja	2
	Bei Verwendung einer Weboberfläche ausschließlich		ja, Grundschutz APP.1.2 und APP.2.1	2

	verschlüsselte Verbindung?			
	Einhaltung der technischen Mindestanforderungen des BSI TLS?	Die Anwendung des BSI TLS empfiehlt sich für Medizingeräte, welche über das Internet kommunizieren, oder mittels Schnittstellen und Protokollen, welche gewöhnlich für den Datenverkehr im Internet Verwendung finden (im Falle von Intranet). Die Anwendung dieser Empfehlungen kann sich auf den Ablauf der Risikoanalyse auswirken.	Ja	2
	Webserver nach Cyber- Sicherheitsempfehlungen „Entwicklung sicherer Webanwendungen“, insbesondere Abschnitt „Entwicklungsphase“?	Der „Mindeststandard des BSI zur Verwendung von Transport Layer Security“ und das zugehörige Hilfsdokument geben zum BSI Grundschutz zusätzliche Hinweise zur Umsetzung der Cybersicherheit bei der Kommunikation von Anwendungen mit einem Webserver.	Wurde für die Datenübertragung vom Steuergerät / Smartphone-App zum auf den Server des Herstellers umgesetzt, wie auch für die Anbindung des Konfigurationscomputers des Serviceanbieters.	2
	Logoff-Prozess, der bei vergessener Abmeldung eine Konfiguration durch unberechtigte Personen verhindert?		Ja	1

9.13 Für den Servicebetrieb

	Fragestellung	Kommentar	Beispiel Insulinpumpe	Kat.
	Servicebetrieb			
	Verwendete Schnittstellen gegen unberechtigten Zugriff geschützt		Whitelisting für die IP des Herstellerservers	2
	Fernwartung: die verwendeten Komponenten dürfen den Betrieb nicht beeinträchtigen		keine Fernwartung	2
	Fernwartung (Schreibzugriff) auf Produkt / Komponente nur bei expliziter Aktivierung der Komponente, expliziter Willenserklärung und zeitlich beschränkt		keine Fernwartung	2

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Aschaffenburg, den 26. Juli. 2023

Eva Nagamine-Jones