HOCHSCHULE MITTWEIDA
University of Applied Sciences

BACHELORARBEIT

Frau
Steffi Voigt

Risikomodellierung im Bereich der Cybersicherheit am Beispiel von Medizintechnik

Mittweida, Oktober 2024

Fakultät **Angewandte Computer- und Biowissenschaften**

BACHELORARBEIT

Risikomodellierung im Bereich der Cybersicherheit am Beispiel von Medizintechnik

Autorin:
Steffi Voigt

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
FO20w2-B

Erstprüfer:
Prof. Dr. rer. pol. Ronny Bodach

Zweitprüfer:
Dirk Eisentraut, M.A.

Einreichung:
Mittweida, 24.10.2024

Verteidigung/Bewertung:
Mittweida, 2024

Faculty of **Applied Computer Sciences and Biosciences**

BACHELOR THESIS

Risk modelling in the field of cyber security using the example of medical technology

Author:
Steffi Voigt

Course of Study:
General and Digital Forensics

Seminar Group:
FO20w2-B

First Examiner:
Prof. Dr. rer. pol. Ronny Bodach

Second Examiner:
Dirk Eisentraut, M.A.

Submission:
Mittweida, 24.10.2024

Defense/Evaluation:
Mittweida, 2024

Bibliografische Beschreibung

Voigt, Steffi:
Risikomodellierung im Bereich der Cybersicherheit am Beispiel von Medizintechnik. – 2024. – 45 S.
Mittweida, Hochschule Mittweida – University of Applied Sciences, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2024.

Referat

Diese Arbeit beschäftigt sich mit der Risikomodellierung im Bereich der Cybersicherheit am Beispiel der Medizintechnik. Es werden Modelle für die Einschätzung des Risikos vorgestellt und diese Anhand eines fiktiven Beispiels angewendet. Des Weiteren wird das Risikomanagement beschrieben und mögliche Schadensklassen nach den Schutzzielen sortiert vorgestellt.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BKA ..... Bundeskriminalamt

BSI ..... Bundesamt für Sicherheit in der Informationstechnik

CVE ..... Common Vulnerabilities and Exposures System

CVSS ..... Common Vulnerability Scoring System

CWSS ..... Common Weakness Scoring System

DoS ..... Denial of Service

DREAD ..... Damage, Reproducibility, Exploitability, Affected Users, and Discoverability

EN ..... Europäische Norm

EU ..... Europäische Union

IEC ..... International Electrotechnical Commission

ISO ..... Internationale Organisation für Normen

IT ..... Informationstechnik

MDR ..... Medical Device Regulation

MPAMIV ..... Medizinprodukte-Anwendermelde- und Informationsverordnung

OP ..... Operation

OWASP ..... Open Worldwide Application Security Project

STRIDE ..... Spoo ng Identity, Tampering with Data, Repudiation, Information Disclosure, Denial of Service, Elevation of Privileges

1 Einleitung

Die Digitalisierung in Deutschland schreitet immer weiter voran, so auch im Gesundheitswesen. Sie bietet viele Möglichkeiten, wie eine schnelle Kommunikation, ef ziente Verwaltungsabläufe, die übergreifende Bereitstellung von Patientendaten und eine schnelle Krankheitserkennung durch systematische Analyse und Auswertung medizinischer Daten.[1] Die Vorteile der Digitalisierung im Gesundheitswesen gehen jedoch auch mit Sicherheitsrisiken einher. So wurden beispielsweise im September des Jahres 2024 die Wertachkliniken im Kreis Augsburg durch einen Ransomwareangriff lahmgelegt. Die Auswirkungen dieses Cybersicherheitsvorfalls gingen so weit, dass geplante Operationen verschoben werden mussten.[2] Der Angriff auf die Wertachkliniken stellt keinen Einzelfall dar. Auch im Jahr 2023 konnten laut Bundeskriminalamt (BKA) mehrere Kliniken durch Ransomwareangriffe nur noch eingeschränkt arbeiten.[3] In einer Umfrage von 1000 Unternehmen gaben 84 Prozent der befragten Unternehmen an, im Jahr 2023 von einem Cyberangriff betroffen gewesen zu sein.[4] Die jährlich entstehenden Kosten durch Cybersicherheitsvorfälle, wie Diebstahl von Informationstechnik (IT)-Ausrüstung, Datendiebstahl, Spionage und Sabotage werden in Deutschland auf rund 203 Milliarden Euro geschätzt.[4] Aufgrund dieser Bedrohungslage kann Digitalisierung ohne Cybersicherheit nicht erfolgreich sein[5]. Dies gilt auch im Bereich der Medizinprodukte. So zeigt eine Statistik aus den USA, dass die Anzahl der registrierten Datenlecks im medizinischen Sektor sogar noch häu ger vorkommt als im Finanzsektor.[6]

Für den Binnenmarkt der Europäischen Union (EU) werden auf gesetzlicher Ebene für Hersteller von Medizinprodukten durch die Medical Device Regulation/EU-Medizinprodukteverordnung Anforderungen gestellt, wenn sie Medizinprodukte in der EU in Verkehr bringen wollen.[7] So müssen Hersteller ihre Produkte auf Risiken analysieren und bewerten, um Maßnahmen zur Beherrschung der Risiken zu ergreifen.[8] Auch durch die Internationale Organisation für Normen (ISO) werden Anforderungen an die Anwendung des Risikomanagements auf Medizinprodukte normiert. Danach hat jeder Hersteller ein Risikomanagementsystem für seine Produkte einzurichten und zu dokumentieren, um gewährleisten zu können, dass Gefahren identi ziert, bewertet und kontrolliert wurden und werden.[9] Problematisch an diesen Anforderungen ist, dass keine verbindliche einheitliche Ausgestaltung des konkreten Risikomanagementsystems speziell für den medizinischen Cybersicherheitsbereich existiert.

1.1 Motivation

Im Bereich der Risikomodellierung existieren verschiedene Modelle wie beispielsweise Spoo ng Identity, Tampering with Data, Repudiation, Information Disclosure, Denial of Service, Elevation of Privileges (STRIDE), Open Worldwide Application Security Project (OWASP) und den IT-Grundschutz des Bundesamt für Sicherheit in der Informationstechnik (BSI). Diese sind allgemein für die Modellierung von Risiken inklusive Bezug zur Cybersicherheit konzipiert. Für den Bereich der Medizintechnik existieren keine genauen Vorgaben, welche Modelle für das Risikomanagement verwendet werden sollen.

1.2 Zielsetzung

Ziel dieser Arbeit ist es daher Bedrohungsmodelle wie STRIDE, OWASP und den BSI IT-Grundschutz auf die Cybersicherheit im medizinischen Bereich an einem ktiven Beispiel anzuwenden, um Wege und Problematiken für die Klassi zierung des Risikos aufzuzeigen.

1.3 Aufbau der Arbeit

Zu Beginn der Arbeit werden grundlegende Begriffe und Modelle im Kapitel 2 vorgestellt. Zunächst werden verschiedene einzelne Bedrohungsmodelle zur Risikoeinschätzung vorgestellt, unter anderem STRIDE, Common Weakness Scoring System (CWSS), Damage, Reproducibility, Exploitability, Affected Users, and Discoverability (DREAD) und das BSI IT-Grundschutzmodell. Nachfolgend wird der generelle Aufbau des Risikomanagements nach der ISO Europäische Norm (EN) 14971 aufgezeigt und mit der International Electrotechnical Commission (IEC) EN 8001-5-1 erweitert. Da in dieser Arbeit die Bedrohungen der Cybersicherheit eingeschätzt werden sollen, werden die für die Medizin relevanten Schutzziele und mögliche Angriffsformen vorgestellt und die Häu gkeit über Statistiken aus den Jahren 2021 und 2022 eingeschätzt. Da die Risikoeinschätzung grundlegend aus den Bereichen Wahrscheinlichkeit eines Angriffs und des potenziellen Schadens besteht, wird hier darauf eingegangen, wie man die potenziellen Cybersicherheitsschäden im medizinischen Bereich einschätzen kann.

Kapitel 3 bildet den praktischen Teil der Arbeit ab. Einige der vorgestellten Modelle werden am Beispiel eines Patientenmonitors berechnet. Das Gerät weist eine Sicherheitslücke in der Überprüfung übertragener Zerti kate auf. Dieser Bedrohungsfall wird analysiert und in den unterschiedlichen Modellen eingeordnet.

Abschließend wird in Kapitel 4 zusammengefasst, welche Modelle geeignet sind, welche Schwierigkeiten und Herausforderungen bestehen und was in Zukunft getan werden muss, um die Herausforderungen ef zienter zu bewältigen.

2 Grundlagenteil

Dieses Kapitel gibt Aufschluss über die relevanten Informationen, welche zum Verständnis der Thematik benötigt werden. Insbesondere wird dabei auf die verschiedenen Bedrohungsmodelle sowie auf das Risikomanagement der Medizintechnik und die Cybersicherheit eingegangen.

2.1 De nitionen

Bei den De nitionen handelt es sich um einen Auszug der für die Arbeit relevanten Begriffe aus der ISO/EN Norm 14971.

- Schaden
  Verletzung oder Schädigung der Gesundheit von Menschen oder Schädigung von Gütern oder der Umwelt.[9]

- Gefährdung
  potentielle Schadensquelle.[9]

- Schweregrad
  Maß der möglichen Auswirkungen einer Gefährdung.[9]

- Lebenszyklus
  Abfolge aller Phasen im Leben eines Medizinprodukts von der anfänglichen Konzeption bis zur endgültigen Außerbetriebnahme und Entsorgung.[9]

- Verfahren
  festgelegte Art und Weise, eine Tätigkeit oder einen Prozess auszuführen.[9]

- Prozess
  Satz zusammenhängender oder sich gegenseitig beein ussender Tätigkeiten, der Eingaben zum Erzielen eines vorgesehenen Ergebnisses verwendet.[9]

- Risiko
  Kombination der Wahrscheinlichkeit des Auftretens eines Schadens und des Schweregrades dieses Schadens.[9]

- Restrisiko Risiko, das nach der Umsetzung von Maßnahmen zur Risikobeherrschung verbleibt.[9]

- Sicherheit
  Freiheit von unvertretbaren Risiken.[9]

2.2 Bedrohungsmodelle

In einem Modell wird versucht, komplexe Zusammenhänge aus der Wirklichkeit in einem kleinen Maßstab nachzuvollziehen, um die Realität besser verstehen zu können und somit beispielsweise mögliche Gefahren besser abschätzen zu können [10]. Bei der Bedrohungsmodellierung, auch Threat Modeling genannt, handelt es sich um eine konzeptionelle Analysetechnik, um mögliche Gefahren und Risiken zu identi zieren und einzuteilen.[11] Grundsätzlich besteht ein Risiko aus der Kombination der Wahrscheinlichkeit des Auftretens eines Schadens und dem Schweregrad des Schadens[9]. Hierfür gibt es verschiedene Modelle, welche im Folgenden genauer vorgestellt werden.

2.2.1 STRIDE

Das von Microsoft erstellte Modell Spoo ng Identity, Tampering with Data, Repudiation, Information Disclosure, Denial of Service, Elevation of Privileges besteht aus einer Strukturanalyse und der Einordnung der Bedrohungen in Kategorien. Für die Analyse emp ehlt es sich, ein Daten ussdiagramm zu erstellen, in welchem die Prozesse, Entitäten, Datenspeicher, Daten üsse und Vertrauensgrenzen dargestellt werden. [12, S. 751]

Abbildung 2.1: Daten ussdiagramm Beispiel einer Bibliothek in Anlehnung an [11]

Abbildung 2.1 zeigt ein Daten ussdiagramm am Beispiel einer Bibliothek. In dieser Darstellung werden Entitäten als Rechtecke, doppelte Kreise als Anwendungen, Pfeile als Datenströme, parallele Linien als Datenbanken und gestrichelte Linien als Vertrauensgrenzen dargestellt.[11] Durch diese Darstellung kann ein Überblick über das zu analysierende System geschaffen werden. Somit können

die möglichen Bedrohungen besser erkannt und analysiert werden.[12] Anschließend werden die erkannten Bedrohungen im STRIDE Modell in die Kategorien, welche in Tabelle 2.1 eingeteilt werden, eingeordnet.[11]

Tabelle 2.1: STRIDE Kategorien in Anlehnung an [11]

Typ	mögliche Beschreibung	Schutzziel
Spoo ng	Verschleierung z.B. der eigenen Identität	Authenti zierung
Tampering / Manipulation	Verfälschen von Informationen	Integrität
Reputiation	Bösartiges Handeln in einem System, ohne dass dies erkannt werden kann	Non Repudiation
Veröffentlichung von Informationen	Informationen lesen für diese man keine Berechtigung besitzt	Con dentiality / Geheimhaltung
Denail-of-Service	Überlastung eines Systems damit dieses nicht mehr zur Verfügung steht	Verfügbarkeit
Erhöhung von Rechten	Zugriffsrechte erweitern um Zugang zu Informationen zu bekommen	Authorization

2.2.2 DREAD

DREAD bewertet über die Nutzung von fünf Metriken die Bedrohung von Schwachstellen aller Art. DREAD steht als Akronym für die Begriffe Damage (Schadenspotential), Reproducibility (Reproduzierbarkeit), Exploitability (Ausnutzbarkeit), Affected Users (Nutzerbetroffenheit) und Discoverability (Auf ndbarkeit). Diese bilden gleichzeitig die Kategorien zur Bewertung der Schwachstellen. Für die Berechnung werden Werte von 1 (gering) bis 3 (hoch) für diese Kategorien vergeben. Im Anschluss wird die Summe der Werte berechnet und bildet von 5 ein niedriges bis 15 das höchste Risiko ab. Der Wert stellt das Risiko einer zu bewertenden Schwachstelle dar. In Tabelle 2.2 sind die einzelnen Kategorien sowie deren verbale Einschätzungen aufgeführt.[13]

Die in 2.2 beschriebenen Metriken Schadenspotential und betroffene Benutzer bilden den technischen Schaden ab. Die Metriken Reproduzierbarkeit, Ausnutzbarkeit und Auf ndbarkeit bilden die Eintrittswahrscheinlichkeit ab. DREAD hat die Schwachstelle, dass keine Wichtung der Parameter existiert. Dies kann über manuelle Wichtung der Parameter vorgenommen werden. Ein weiteres Problem ist, dass die Parameter durch unterschiedliche Personen verschieden bewertet werden und somit die Reproduzierbarkeit des Modells nur eingeschränkt gegeben ist. [13, S. 365–366]

Tabelle 2.2: DREAD Kategorien inklusive verbaler Ausführung in Anlehnung an [13, S. 365]

	Hoch (3)	Mittel(2)	Niedrig (1)
D- Damage Potential (Schadenspotential)	Angreifer können Kunden- oder Unternehmensdaten auslesen	Angreifer können sensible Daten auslesen	Angreifer können interne Daten auslesen
R- Reproducibility (Reproduzierbarkeit)	Angriff ist jederzeit ausführbar	Angriff ist nur innerhalb eines bestimmten Zeitfensters ausführbar	Angriff ist nur sehr schwer reproduzierbar
E- Exploitability (Ausnutzbarkeit)	Von Scriptkiddie durchführbar	Fortgeschrittenes Wissen erforderlich	Sehr hohes Wissen erforderlich
A- Affected Users (betroffene Benutzer)	Die meisten Benutzer sind betroffen	Einige Benutzer sind betroffen	Einige wenige (bzw. gar keine) Benutzer sind betroffen
D- Discoverability (Auf ndbarkeit)	Schwachstelle lässt sich von einem Angreifer einfach identi zieren	Schwachstelle schwer aber grundsätzlich von extern identi zierbar	Identi zierung erfordert Insiderwissen oder Quellcode

2.2.3 OWASP

Das Open World wide Application Security Project, kurz OWASP, beschäftigt sich mit der Risikoeinschätzung von Bedrohungen. In diesem Modell werden vier Faktoren aus den Kategorien Bedrohungsfaktor, Vulnerabilitätsfaktor, Technischer Ein ussfaktor und Geschäftlicher Ein ussfaktor berechnet. Die Werte werden entsprechend der Tabellen 2.3 bis 2.6 eingeordnet. Im Anschluss wird aus den Gruppen Bedrohungsfaktor und Vulnerabilitätsfaktor der Durchschnitt berechnet. Der Durchschnitt der technischen und geschäftlichen Auswirkungen wird getrennt voneinander berechnet. Bei der Berechnung entstehen Werte zwischen 1 und 9. Der Durchschnitt kann im Anschluss in die Kategorien Niedrig (0 bis <3), Medium (3 bis <6) und Hoch (6 bis 9) eingeordnet werden.[14]

In Tabelle 2.3 wird die Einordnung des Bedrohungsfaktors dargestellt. Dieser wird dafür verwendet, den Bedrohungsagenten einzuordnen und somit einen Teil der Wahrscheinlichkeit eines erfolgreichen Angriffs abzuschätzen.[14]

Tabelle 2.3: OWASP Bedrohungsfaktor in Anlehnung an [14]

	Beschreibung (Bewertung)
Fähigkeitsniveau - Wie technisch versiert ist diese Gruppe von Bedrohungsagenten?	• Keine technischen Fähigkeiten (1) • Einige technische Fähigkeiten (3) • Fortgeschrittener Computerbenutzer (5) • Netzwerk- und Programmierkenntnisse (6) • Fähigkeiten zum Eindringen in Sicherheitssysteme (9)
Motiv - Wie motiviert ist diese Gruppe von Bedrohungsagenten, diese Schwachstelle zu nden und auszunutzen?	• Geringe oder keine Belohnung (1), • Mögliche Belohnung (4), • Hohe Belohnung (9)
Gelegenheit - Welche Ressourcen und Gelegenheiten sind erforderlich, damit diese Gruppe von Bedrohungsagenten diese Schwachstelle nden und ausnutzen kann?	• Vollzugriff oder teure Ressourcen erforderlich (0), • Spezieller Zugriff oder spezielle Ressourcen erforderlich (4), • Gewisser Zugriff oder gewisse Ressourcen erforderlich (7), • Kein Zugriff oder keine Ressourcen erforderlich (9)
Größe - Wie groß ist diese Gruppe von Bedrohungsagenten?	• Entwickler (2), • Systemadministratoren (2), • Intranetbenutzer (4), • Partner (5), • Authenti zierte Benutzer (6), • Anonyme Internetbenutzer (9)

In Tabelle 2.4 wird die Einordnung der Kategorien für den Vulnerabilitätsfaktor dargestellt. Ziel dieses Faktors ist es, die Schwachstelle nach ihrer Ausnutzbarkeit und der Wahrscheinlichkeit, dass sie entdeckt wird, einzuschätzen. Dies ist ein weiterer Teil zur Einschätzung der Eintrittswahrscheinlichkeit.

Tabelle 2.4: OWASP Vulnerabilitätsfaktor in Anlehnung an [14]

	Beschreibung (Bewertung)
Entdeckung - Wie einfach ist es für diese Gruppe von Bedrohungsagenten, diese Schwachstelle zu entdecken?	• Praktisch unmöglich (1), • Schwierig (3), • Einfach (7), • Automatisierte Tools verfügbar (9)
Ausnutzung - Wie einfach ist es für diese Gruppe von Bedrohungsagenten, diese Schwachstelle tatsächlich auszunutzen?	• Theoretisch (1), • Schwierig (3), • Einfach (5), • Automatisierte Tools verfügbar (9)
Bewusstsein - Wie bekannt ist diese Schwachstelle bei dieser Gruppe von Bedrohungsagenten?	• Unbekannt (1), • Versteckt (4), • Offensichtlich (6), • Öffentlich bekannt (9)
Intrusion Detection - Wie wahrscheinlich ist es, dass ein Exploit erkannt wird?	• Aktive Erkennung in der Anwendung (1), • Protokolliert und überprüft (3), • Protokolliert ohne Überprüfung (8), • Nicht protokolliert (9)

In der Tabelle 2.5 wird der Schweregrad einer Gefährdung eingeschätzt. In den Kategorien werden die möglichen betroffenen Schutzziele wie Vertraulichkeit, Integrität und Verfügbarkeit aufgegriffen.

Tabelle 2.5: OWASP Technische Ein ussfaktoren in Anlehnung an [14]

	Beschreibung (Bewertung)
Verlust der Vertraulichkeit - Wie viele Daten könnten offengelegt werden und wie sensibel sind sie?	• Offenlegung minimaler nicht sensibler Daten (2), • Offenlegung minimaler kritischer Daten (6), • Offenlegung umfangreicher nicht sensibler Daten (6), • Offenlegung umfangreicher kritischer Daten (7), • Offenlegung aller Daten (9)
Integritätsverlust - Wie viele Daten könnten beschädigt sein und wie stark sind sie beschädigt?	• Minimal leicht beschädigte Daten (1), • Minimal stark beschädigte Daten (3), • Umfangreiche leicht beschädigte Daten (5), • Umfangreiche stark beschädigte Daten (7), • Alle Daten völlig beschädigt (9)
Verlust der Verfügbarkeit - Wie viele Dienste könnten verloren gehen und wie wichtig sind sie?	• Dienste unterbrochen (1), • Minimale primäre Dienste unterbrochen (5), • Umfangreiche sekundäre Dienste unterbrochen (5), • Umfangreiche primäre Dienste unterbrochen (7), • Alle Dienste vollständig verloren (9)
Verlust der Verantwortlichkeit - Sind die Aktionen der Angreifer auf eine Einzelperson zurückzuführen?	• Vollständig rückverfolgbar (1), • Möglicherweise rückverfolgbar (7), • Völlig anonym (9)

In der Tabelle 2.6 wird der Ein uss des potenziellen Schadens auf das Geschäft wie z.B. den Jahresgewinn und den Verlust von Kunden eingeschätzt.

Tabelle 2.6: OWASP Geschäftliche Ein ussfaktoren in Anlehnung an [14]

	Beschreibung (Bewertung)
Finanzieller Schaden - Wie hoch ist der nanzielle Schaden, der durch einen Exploit entsteht?	• Geringer als die Kosten zur Behebung der Schwachstelle (1), • Geringe Auswirkung auf den Jahresgewinn (3), • Erhebliche Auswirkung auf den Jahresgewinn (7), • Insolvenz (9)
Reputationsschaden - Führt ein Exploit zu einem Reputationsschaden, der dem Unternehmen schaden würde?	• Minimaler Schaden (1), • Verlust wichtiger Kunden (4), • Verlust von Goodwill (5), • Markenschaden (9)
Nichteinhaltung - Wie viel Aufsehen erregt die Nichteinhaltung?	• Geringfügiger Verstoß (2), • Klarer Verstoß (5), • Schwerwiegender Verstoß (7)
Datenschutzverletzung - Wie viele personenbezogene Daten könnten offengelegt werden?	• Eine Einzelperson (3), • Hunderte von Personen (5), • Tausende von Personen (7), • Millionen von Personen (9)

Die Einordnung der Faktoren kann in der Risikomatrix des Gesamtrisikoschweregrades in Abbildung 2.2 eingeordnet werden. Eine Risikomatrix besteht grundlegend aus den Achsen Eintrittswahrscheinlichkeit und Gefahrenpotential, hier benannt als Wahrscheinlichkeit und Auswirkungen.

Abbildung 2.2: Risikomatrix für das OWASP Modell in Anlehnung an [14]

Sofern ausreichend Informationen zu den geschäftlichen Auswirkungen vorliegen, ist normalerweise der Geschäftliche Ein ussfaktor für die Auswirkung in die Risikomatrix einzuordnen. Liegen nicht genügend Informationen vor, wird normalerweise der Faktor der technischen Auswirkungen verwendet.

Da es sich um Medizinprodukte handelt, ist nach der Medical Device Regulation (MDR) die Einordnung der Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit relevant. Somit sollte für das notwendige Risikomanagement, um Medizinprodukte in Verkehr bringen zu können, der Technische Ein ussfaktor als Auswirkung verwendet werden. Für die Wahrscheinlichkeit wird der Durchschnitt des Bedrohungsfaktors und des Vulnerabilitätsfaktors eingetragen. Somit lässt sich einschätzen, ob das Risiko vertretbar ist. Die Grenze des Vertretbaren muss vorher vom Hersteller festgelegt werden.[14]

2.2.4 Common Weakness Scoring System und Common Vulnerability Scoring System

Das Common Weakness Scoring System (CWSS) wird verwendet, um Softwareschwachstellen im Allgemeinen zu bewerten, um somit eine Priorisierung der Sicherheitslücken vornehmen zu können. Die Bewertung über Common Vulnerability Scoring System (CVSS) und CWSS ähneln sich stark mit dem Unterschied, dass CWSS erlaubt Parameter mit „unbekannt “ zu beziffern, dies sieht CVSS nicht vor. In dem CVSS werden bekannte Standardsicherheitslücken bewertet. [13] Das CVSS lässt sich nur auf Sicherheitslücken, die zuvor in einem Common Vulnerabilities and Exposures System (CVE) identi ziert und mit Parametern versehen wurden, anwenden. [15] Für das CWSS werden 16 Werte benötigt, die allerdings auch unbekannt sein können. Die Werte/ Metriken werden in drei Gruppen eingeteilt: die Basis ndung (in Tabelle 2.7 dargestellt), die Angriffs äche (in Tabelle 2.8 dargestellt) und die Umgebungsbedingungen (in Tabelle 2.9 dargestellt).

Tabelle 2.7: CWSS Basis ndung in Anlehnung an [16] aus dem Englischen übersetzt

Gruppe Basis ndung	Zusammenfassung
Technische Auswirkungen (TI)	Das mögliche Ergebnis, das durch die Schwachstelle hervorgerufen werden kann, sofern die Schwachstelle erfolgreich erreicht und ausgenutzt werden kann.
Erworbene Privilegien (AP)	Die Art der Berechtigungen, die ein Angreifer erlangt, wenn er die Schwachstelle erfolgreich ausnutzen kann.
Erworbene Berechtigungsschicht (AL)	Die Betriebsebene, für die der Angreifer durch erfolgreiches Ausnutzen der Schwachstelle Privilegien erlangt.
Wirksamkeit der internen Kontrolle (IC)	die Fähigkeit der Kontrolle, die Schwachstelle für einen Angreifer unausnutzbar zu machen.
Vertrauen nden (FC)	die Gewissheit, dass es sich bei dem gemeldeten Problem um eine Schwachstelle handelt, die von einem Angreifer ausgenutzt werden kann

Tabelle 2.8: CWSS Angriffs äche in Anlehnung an [16] aus dem Englischen übersetzt

Gruppe Angriffs äche	Zusammenfassung
Erforderliche Berechtigung (RP)	Die Art der Berechtigungen, über die ein Angreifer bereits verfügen muss, um an den Code/die Funktionalität zu gelangen, die die Schwachstelle enthält.
Erforderliche Berechtigungsebene (RL)	Die Betriebsebene, für die der Angreifer Berechtigungen haben muss, um zu versuchen, die Schwachstelle anzugreifen.
Zugriffsvektor (AV)	Der Kanal, über den ein Angreifer kommunizieren muss, um an den Code oder die Funktionalität zu gelangen, die die Schwachstelle enthält.
Authenti zierungsstärke (AS)	Die Stärke der Authenti zierungsroutine, die den Code/die Funktionalität schützt, die die Schwachstelle enthält.
Ebene der Interaktion (IN)	die Aktionen, die vom menschlichen Opfer bzw. den menschlichen Opfern erforderlich sind, um einen erfolgreichen Angriff zu ermöglichen.
Bereitstellungsumfang (SC)	Ob die Schwachstelle in allen einsetzbaren Instanzen der Software vorhanden ist oder auf eine Teilmenge von Plattformen und/oder Kon gurationen beschränkt ist.

Tabelle 2.9: CWSS Umgebungsbedingungen in Anlehnung an [16] aus dem Englischen übersetzt

Gruppe Umgebungsbedingungen	Zusammenfassung
Auswirkungen auf das Geschäft (BI)	Die potenziellen Auswirkungen auf das Geschäft oder die Mission, wenn die Schwachstelle erfolgreich ausgenutzt werden kann.
Wahrscheinlichkeit der Entdeckung (DI)	Die Wahrscheinlichkeit, dass ein Angreifer die Schwachstelle entdeckt
Wahrscheinlichkeit eines Exploits (EX)	die Wahrscheinlichkeit, dass ein Angreifer mit den erforderlichen Berechtigungen/Authenti zierung/Zugriffen die Schwachstelle erfolgreich ausnutzen kann, wenn sie entdeckt wird.
Wirksamkeit externer Kontrollen (EC)	die Möglichkeit von Kontrollen oder Abhilfemaßnahmen außerhalb der Software, die es einem Angreifer möglicherweise erschwert, die Schwachstelle zu erreichen und/oder auszulösen.
Prävalenz (P)	Wie häu g diese Art von Schwachstelle in Software auftritt.

Die einzutragenden Werte sind vorde niert und können über eine Tabelle eingeordnet werden. Die genauen Kriterien und Werte sind in der Quelle [16] zu nden. Sie werden im praktischen Teil für die Modellierung verwendet. Die Werte innerhalb einer Gruppe werden über die folgenden Formeln miteinander verrechnet. Die Formeln innerhalb der einzelnen Gruppen:
Basis ndungsscore Formel
Der Basisscore kann einen Wert zwischen 0 und 100 einnehmen. BasisSubscore = [(10 TI + 5 (AP + AL) + 5 FC) f(TI) IC] 4:0

Der Angriffs ächensubscore und der Umweltsubscore erhalten durch die Berechnung einen Wert zwischen 0 und 1.
Angriffs äche Formel
AngriffsflaecheSubscore = [20 (RP + RL + AV) + 20 SC + 15 IN + 5 AS]=100:0

Umwelt Formel
UmweltSubscore= [(10 BI + 3 DI + 4 EX + 3 P) f(BI) EC]=20:0
Anschließend werden die Ergebnisse der einzelnen Gruppen miteinander multipliziert. Durch die Berechnung entsteht ein Wert zwischen 1 und 100. Je höher der Wert, desto größer ist das Risiko der einzuschätzenden Bedrohung.[16]

2.2.5 BSI IT-Grundschutz 200-3

Im BSI IT-Grundschutz wird zunächst eine Skizze des Systems erstellt (Daten ussdiagramm), in welchem die einzelnen Komponenten des Systems aufgezeigt werden. Im Anschluss wird für jedes im System be ndliche Gerät eine Liste mit möglichen Schwachstellen erstellt, welche nach ihrer Eintrittswahrscheinlichkeit (in Tabelle 2.10 dargestellt) und ihres Schadenspotentials (in Tabelle 2.11 dargestellt) eingeschätzt werden.[17]

Tabelle 2.10: BSI IT-Grundschutz 200-3 Häu gkeitseinordnung in Anlehnung an [17]

Häu gkeit	Beschreibung
Selten	Ereignis könnte nach heutigem Kenntnisstand höchstens Jahre eintreten.
mittel	Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.
häu g	Ereignis tritt einmal im Jahr bis einmal pro Monat ein.
sehr häu g	Ereignis tritt mehrmals im Monat ein

Tabelle 2.11: BSI IT-Grundschutz 200-3 Schadenspotentialeinteilung in Anlehnung an [17]

Schadenskategorie	Beschreibung
Vernachlässigbar	Die Schadensauswirkungen sind gering und können vernachlässigt werden.
Begrenzt	Die Schadensauswirkungen sind begrenzt und überschaubar.
Beträchtlich	Die Schadensauswirkungen können beträchtlich sein.
existenzbedrohend	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Anschließend wird die Eintrittswahrscheinlichkeit und das Schadenspotential in der Risikomatrix, welche in Tabelle 2.3 dargestellt ist, übertragen und das Risiko abgelesen. Als Ergebnis lässt sich das Risiko direkt in vertretbar oder nicht vertretbar einordnen.[17]

Abbildung 2.3: Risikomatrix nach dem BSI IT-Grundschutz 200-3 in Anlehnung an [17]

2.2.6 Zusammenfassung und Besonderheiten der Modelle

In Tabelle 2.12 werden die vorgestellten Modelle mit ihren Vorteilen und Nachteilen aufgezeigt.

Tabelle 2.12: Zusammenfassung der aufgezeigten Modelle

Modell	Besonderheit	Vorteil	Nachteil
DREAD	5 Metriken in Leicht, Mittel, Schwer einzuordnen	einfache Werte und Berechnung	Subjektiv, keine Wichtung der Werte
OWASP	16 Werte einzuordnen	einfache Berechnung	Umfangreiches Wissen über Produkt und Szenario erforderlich
CWSS	16 Werte einzuordnen	genauere Einschätzung, Wichtung der Werte, Bewertungsmöglich-keit „Unbekannt“	umfangreiches Wissen über Produkt und Szenario erforderlich
BSI IT-Grundschutz	2 Werte einzuordnen	einfache Werte und Einordnung in Bedrohungsmatrix	Subjektiv, keine Wichtung der Werte, Beschreibung nicht medizintechnikspezi- sch
STRIDE	Daten ussdiagramm, Einschätzung der Angriffe in deren Kategorien	Daten ussdiagramm erschafft Überblick über Produkt und mögliche Sicherheitslücken	keine genaue Einschätzung der Bedrohung in Bedrohungsmatrix

2.3 Risikomanagement

Risikomanagement beschreibt den systematischen und professionellen Umgang mit Risiken. Ziel ist es, präventiv vor Schäden zu schützen und diese bereits bevor sie eintreten zu erkennen, um entsprechende Maßnahmen ergreifen zu können. Allerdings kann auch nach dem Eintreten eines Schadens dieser systematisch über das Risikomanagement analysiert werden, um mögliche Ursachen und Folgen zu erkennen und den Umgang mit diesen für die Zukunft anzupassen. Ein konstruktives Risikomanagement behandelt mögliche Gefahren, bevor sie zu einem größeren Schaden führen.[18] Der Hersteller muss zunächst einen Risikomanagementplan erstellen, in welchem die Rahmenbedingungen für das Risikomanagement festgelegt werden. Dieser muss für jedes Medizinprodukt erstellt werden. Der Risikomanagementprozess besteht aus drei Elementen, welche sich in Risikoanalyse, Risikobewertung und Risikobeherrschung unterteilen. Sie sind im gesamten Produktlebenszyklus relevant und sind als parallel laufende Prozesse zu betrachten [9], welche sich wie in einem Kreislauf wiederholen.[18] Jedoch muss der gesamte Risikomanagementprozess vorher geplant werden. Dies ndet im Risikomanagementplan statt, dieser muss für jedes Medizinprodukt erstellt werden. Des weiteren muss der Hersteller eine Risikomanagementakte anlegen, in welcher alle Informationen zu den festgestellten Gefahren erfasst werden. Anhand der Informationen müssen Rückschlüsse auf die Risikoanalyse, Risikobewertung, die Implementierung und Veri zierung der Maßnahmen zur Risikobeherrschung und die Ergebnisse der Bewertung der Restrisiken nachvollzogen werden können.[9]

2.3.1 Risikomanagementplan

Im Risikomanagementplan wird das Risikomanagement geplant und muss nach der ISO/EN 14971 folgendes enthalten (Ausschnitt aus [9]): „

- „den Aufgabenbereich der geplanten Tätigkeiten des Risikomanagements, wobei das Medizinprodukt und die Phasen seines Lebenszyklus, für die jedes Element des Plans gilt, festzulegen und zu beschreiben
- die Zuordnung von Verantwortlichkeiten und Befugnissen
- Anforderungen an die Überprüfung der Tätigkeiten des Risikomanagements
- Kriterien für die Akzeptanz von Risiken auf der Grundlage der Politik des Herstellers zur Bestimmung akzeptabler Risiken, einschließlich der Kriterien für die Akzeptanz von Risiken, wenn die Wahrscheinlichkeit des Auftretens eines Schadens nicht eingeschätzt werden kann sind
- eine Methode zur Bewertung des Gesamt-Restrisikos und Kriterien für die Akzeptanz des Gesamt Restrisikos auf Grundlage der Politik des Herstellers zur Bestimmung des akzeptablen Risikos
- Tätigkeiten zur Veri zierung der Implementierung und Wirksamkeit der Maßnahmen der Risikobeherrschung
- Tätigkeiten im Zusammenhang mit der Erfassung und Überprüfung relevanter Informationen aus der Herstellung und der Herstellung nachgelagerten Phasen “ [9]

2.3.2 Risikoanalyse

In der Norm ISO/EN14971 werden die Ziele der Risikoanalyse de niert und in Abschnitte unterteilt. Sie bestehen aus:

1. „Zweckbestimmung und vorhersehbare Fehlanwendungen dokumentieren
2. Identi zierung sicherheitsbezogener Merkmale
3. Identi zierung von Gefahren und Gefährdungssituationen
4. Risikoeinschätzung“ [9]

Um die Risiken de nieren, analysieren und einschätzen zu können, ist eine Bedrohungsmodellierung wie im Abschnitt 2.2 beschrieben zu empfehlen. Der Hersteller ist zum derzeitigen Zeitpunkt frei in der Wahl seiner Methodik zur Umsetzung der de nierten Ziele.[9] Zunächst muss de niert werden, um welches Medizinprodukt es sich handelt und welche Aufgaben es erfüllen soll. Es müssen die Personen, welche für das Risikomanagement verantwortlich sind und die Rahmenbedingungen für die Risikoanalyse festgelegt werden.[9] Von der International Electrotechnical Commission (IEC) dem Normierungsgremium für Elektrotechnik, wurde die Norm EN IEC 81001-5-1 „Gesundheitssoftware und Gesundheits-IT-Systeme Sicherheit, Effektivität und Security Teil 5-1: Security - Aktivitäten im Produktlebenszyklus“ erstellt. In dieser wird beschrieben, dass zunächst das Sicherheitsumfeld des Produktes de niert werden muss. Dies könnte bestehen aus: [19]

- Standort im Netzwerk
- physische Sicherheit oder IT-Sicherheit durch die Umgebung, in der das Produkt bereitgestellt wird
- Trennung (aus einer Netzwerkperspektive)
- falls bekannt, mögliche Auswirkungen auf die Sicherheit (Gefährdungsfreiheit) durch Beeinträchtigung der IT-Sicherheit
- IT-Sicherheitsmaßnahmen, die in spezieller Hardware implementiert sind, mit der die Gesundheitssoftware verwendet werden soll

Dies würde in die Beschreibung der ISO 14971 Abschnitt 2 Identi zierung sicherheitsbezogener Merkmale passen. Für die Identi zierung von Schwachstellen und Bedrohungen müssen nach der IEC EN 81001-5-1 folgende Bereiche beachtet werden und bezüglich derer ein Bedrohungsmodell angewandt werden, sofern diese im Produkt vorkommen.[19]

- „korrekter Fluss klassi zierter Informationen durch das gesamte System
- Vertrauensgrenzen
- Prozesse
- Datenspeicher
- Wechselwirkung mit externen Einheiten
- Implementierung interner und externer Kommunikationsprotokolle in dem Produkt
- von außen zugängliche physische Anschlüsse, einschließlich Debuganschlüsse
- Leiterplattenanschlüsse wie JTAG-Verbindungen oder Debug-Header, die zum Angriff auf die Hardware genutzt werden könnten
- potentielle Angriffsvektoren, einschließlich Angriffen auf die (vorgesehene) Hardware
- mögliche Bedrohungen
- identi zierte Probleme bezüglich der IT-Sicherheit
- externe Abhängigkeiten in Form von Treibern oder Drittanbieter-Anwendungen (nicht vom Lieferanten entwickelter Code), die in die Anwendung eingebunden sind.“[19]

Das BSI IT-Grundschutzkompendium hat eine Liste von möglichen Komponenten eines medizinischen Produktes erstellt, welche für die Cybersicherheit des Medizinproduktes relevant sein könnten. Die entsprechende Liste wird in der Quelle angefügt.

2.3.3 Risikobewertung

In dieser Phase soll eingeschätzt werden, ob ein Risiko nach den im Risikomanagementplan de - nierten Akzeptanzkriterien akzeptabel ist oder nicht. Ist ein Risiko nach den vorher im Risikomanagementplan de nierten Kriterien nicht akzeptabel, müssen in der Risikobeherrschung Maßnahmen durchgeführt werden, um dieses Risiko abzumildern, und das Restrisiko muss erneut eingeschätzt werden. Ist das Risiko akzeptabel, ist es als Restrisiko zu behandeln. [9] In der IEC 81001-5-1 werden für die Risikobewertung Bedrohungsmodelle wie das CVSS erwähnt.[19]

2.3.4 Risikobeherrschung

In diesem Abschnitt müssen Maßnahmen/ Aktivitäten eingeführt werden, um das bestehende Risiko abzumildern. Der Hersteller muss eine oder mehrere der folgenden Optionen zur Beherrschung des Risikos durchführen, um das Risiko auf ein akzeptables Maß zu mindern.[9]

1. „Inhärent sicheres Design und sichere Herstellung
2. Schutzmaßnahmen im Medizinprodukt selbst oder im Herstellungsprozess
3. Informationen für die Sicherheit und, soweit zutreffend, die Schulung von Anwendern“[9]

2.3.5 Dokumentation des Risikomanagements

Es wird zum Risikomanagement eine Risikomanagementakte angelegt, in welcher der Risikomanagementplan und der Bericht über das Risikomanagement eingefügt werden. In die Dokumentation gehört zusammenfassend:

- Risikomanagementplan
  - Festlegung des betreffendes Medizinprodukt
  - Nennung verantwortliche Personen
  - Aufgabenstellung und Datum der Risikoanalyse
  - Zweckbestimmung des Produkts
- Risikomanagementbericht
  - Sicherheitsbezogene Merkmale, Aufbau, eventuell Daten ussdiagramm
  - Mögliche Bedrohungen
  - Risikoeinschätzung der festgestellten möglichen Bedrohungen
  - Bewertung der Risiken akzeptabel, nicht akzeptabel
  - Vorkehrungen/ Maßnahmen zur Risikobeherrschung
  - Restrisikobewertung und Nutzenanalyse falls nötig

2.4 Cybersicherheit

Cybersicherheit beschäftigt sich mit dem digitalen Schutz vor böswilligen Angriffen auf Computer, Server, Mobilgeräte, elektronische Systeme, Netzwerke und Daten [20]. Dies sind Themen, welche vor allem auch im medizinischen Bereich relevant sind. Im Laufe des Kapitels werden zunächst die Schutzziele, welche für die Medizintechnik relevant sind, vorgestellt. Anschließend werden mögliche Angriffsarten beschrieben. Da ein Risiko über die Wahrscheinlichkeit und das Schadenspotenzial eingeschätzt werden kann, müssen diese im Risikomanagementplan klassi ziert werden. Wie diese für die beschriebenen Schutzziele eingeordnet werden könnten, wird nachfolgend beschrieben.

2.4.1 Schutzziele

Die drei wesentlichen Schutzziele der Cybersicherheit gelten ebenfalls für die Medizintechnik und werden im Folgenden de niert und erklärt.

Integrität
bezeichnet die „Eigenschaft der Genauigkeit und Vollständigkeit“ in der ISO/IEC 27001. Es soll sichergestellt werden, dass die Informationen nicht durch andere Personen oder Angreifer manipuliert, verfälscht oder gelöscht werden können.[21]

Verfügbarkeit
Wird als „Eigenschaft, auf Anforderung durch eine autorisierte Stelle zugänglich und nutzbar zu sein “ in der ISO/IEC 27001 de niert. Die Verfügbarkeit in der Medizin ist von essenzieller Bedeutung, da es erhebliche Folgen für den Patienten haben kann, sollte ein Gerät im laufenden Betrieb ausfallen [21].

Vertraulichkeit
Wird in der ISO/IEC 27001 als „Eigenschaft, dass Informationen nicht unbefugten Personen, Organisationen oder Prozessen zur Verfügung gestellt oder offengelegt werden“ de niert. Dieses Schutzziel ist betroffen, wenn auf vertrauliche Informationen (Daten) von Angreifern unautorisiert zugegriffen wird [21].

2.4.2 Angriffsarten und deren Wahrscheinlichkeiten

In einer Umfrage aus den USA wurde analysiert, welche Arten von Sicherheitsvorfällen 2021 im Gesundheitswesen stattfanden. Die Ergebnisse sind in 2.4 dargestellt.

Abbildung 2.4: Umfrage zur Art der Sicherheitsvorfälle im Gesundheitswesen in den USA im Jahre 2021 in Anlehnung an [22]

Daraus ist zu entnehmen, dass die meisten Sicherheitsvorfälle im Cybersicherheitsbereich durch Phishing, Ransomware und Datenlecks entstehen. Fahrlässiges internes Verhalten und Social Engineering sind vom Menschen verursachte Sicherheitslücken.[22] Es gibt weitere Statistiken, die die allgemeine Angriffshäu gkeit auf Unternehmen analysieren. So z.B. die Bitcom Umfrage, welche in dem Diagramm 2.5 dargestellt wird. Hier ist zu sehen, dass die Häu gkeiten innerhalb eines Jahres sehr schwanken.

Ransomware
Ziel eines Ransomware Angriffs ist es, mit der Verschlüsselung und somit der Einschränkung der Verfügbarkeit wichtiger Daten Lösegeld zu erpressen. Dieser Angriff kann gerade im medizinischen Bereich schwerwiegende Folgen haben.[24]

Denail of Service
Bei einem Denial of Service (DoS) Angriff wird das Zielsystem mit Anfragen überlastet, um somit die Verfügbarkeit des Systems einzuschränken und so gezielt Schaden zu verursachen [25].

Man in the Middle
Bei einem Man in the Middle Angriff schaltet sich der Angreifer zwischen zwei Kommunikationspartner und erlangt somit Zugriff über den Datenverkehr, zwischen den Kommunikationspartnern.[26]

Phishing
Bei einem Phishingangriff wird versucht, eine Person zum Handeln, beispielsweise dem Klicken auf einen Link oder das Herausgeben von Benutzerinformationen, zu bewegen. Dies wird beispielswei-

Abbildung 2.5: Angriffshäu gkeiten in Prozent in Anlehnung an [23]

se über gefälschte Emails erreicht, welche vortäuschen, von einer of ziellen, vertrauenswürdigen Stelle verschickt worden zu sein und somit den Nutzer dazu bewegen, auf einen Link zu klicken. Ein weiteres Beispiel für einen Phishing Angriff ist das Fälschen von Webseiten, welche wie eine of zielle Webseite aussehen und somit den Nutzer dazu bewegen, Nutzerdaten wie Nutzername und Passwort einzugeben.[27]

Brute Force Bei einem Brute Force Angriff werden Anmeldeinformationen wie z.B. Passwörter durch Ausprobieren erraten, um somit wichtige Informationen oder Zugriff auf ein System zu erhalten.[28]

2.4.3 Bewertung des Schadenspotentials

Eine Risikobewertung besteht grundsätzlich aus der Kombination aus dem Schweregrad des Schadens und der Wahrscheinlichkeit, dass es zu diesem Schaden kommt.[9] Eine Möglichkeit, um ein Risiko berechnen zu können, ist es, den potenziellen Schaden und die Wahrscheinlichkeit in Kategorien einzuteilen. Die ISO/EN 14971 gibt keine Klassi zierungen des Schweregrads vor. Die Klassi zierung und die Beschreibung der Schadensklassen ist vom Produkt abhängig und wird vom Hersteller erstellt. [9] Es gibt verschiedene Modelle wie den BSI IT-Grundschutz 200-3 in welchem die potentiellen Schäden, wie in Tabelle 2.11 dargestellt, in die Kategorien „existenzbedrohend, beträchtlich, begrenzt, vernachlässigbar“ eingeordnet werden. Es ist zu sehen, dass diese Einschätzung sehr allgemein ist und somit für den medizinischen Bereich angepasst werden müsste. Im medizinischen Bereich können Schäden am Patienten bis hin zum Tod entstehen, es können aber auch nanzielle Einbußen für die medizinische Einrichtung oder Datenschutzschäden der Patientendaten eintreten.[18] Wie genau diese eingeschätzt werden, konnte man schon in Ansätzen in der Risikomodellierung nachlesen, Genaueres wird nachfolgend erläutert.

Gesundheitlicher Schaden
Da die ISO/EN 14971 keine Schadensklassen de niert, müssen sie vom Hersteller selbst erstellt und de niert werden. Das Johner Institut hat einen neuen Ansatz für die Einordnung des Schweregrades gesundheitlicher Schäden erstellt, so werden die Klassi zierungsmerkmale von Schäden wie folgt beschrieben:[29]

- „Tod (j/n)
- Hospitalisierungsdauer > n Tage (j/n)
- Grad der Behinderung > x % (j/n)
- Intensivmedizinische Behandlung (eines Nicht-Intensivpatienten) notwendig (j/n)
- Ärztliche Intervention notwendig (j/n)
- Reversibel (j/n)
- Verkürzung der Lebenserwartung > n Monate (j/n)
- Verkürzung der Lebenserwartung > x % verglichen mit der Lebenserwartung bei „richtiger Behandlung“ (j/n)
- Schmerz-Level > X (j/n)
- Lebensqualität, psychische Belastung gemäß „Quality of Life“-Kriterien.“ [29]

Im Anschluss müssen die Schadensgrade de niert werden. Dies ist zu erreichen, indem die Klassi zierungsmerkmale für jeden Schadensgrad de niert werden, damit die Schäden später in die richtigen Schadensgrade eingeordnet werden können.[29]

In anderen allgemeinen Schadenseinteilungen des gesundheitlichen Schadens wie z.B. in der Herzchirurgie werden die Bedrohungen wie in Tabelle 2.13 beschrieben[18]. Diese Einordnung ist beispielhaft, lässt sich aber auf mögliche allgemeine gesundheitliche Schäden eines Patienten anwenden. Sie könnten somit auch in der Bedrohungseinschätzung im Cybersicherheitsbereich für die Einordnung gesundheitlicher Schäden verwendet werden. Im § 2 der Medizinprodukte-Anwendermelde- und Informationsverordnung (MPAMIV) werden die Begriffe der schwerwiegenden Vorkommnisse de niert. Diese sind als schwerwiegend zu betrachten, wenn sie eine der anschließenden potenziellen Folgen haben:

- „den Tod eines Patienten Anwenders oder einer anderen Person
- die vorübergehende oder dauerhafte schwerwiegende Verschlechterung des Gesundheitszustands eines Patienten, Anwenders oder einer anderen Person
- oder eine schwerwiegende Gefahr für die öffentliche Gesundheit.“[30]

Tabelle 2.13: Allgemeine Gesundheitliche Risikoeinschätzung in Anlehnung an [18]

Schadenskategorie	Beschreibung
Extrem	• Tod eines Patienten, der nicht in unmittelbarem Zusammenhang mit der Erkrankung steht und nicht dem erwarteten Behandlungsergebnis entspricht
Groß	• Schwerwiegende anhaltende Funktionsstörung, die nicht in unmittelbarem Zusammenhang mit der Erkrankung steht und nicht dem erwarteten Behandlungsergebnis entspricht • Jegliche Form der Entstellung • Dringender chirurgischer Handlungsbedarf
Moderat	• Anhaltende Funktionsstörung, die nicht in unmittelbarem Zusammenhang mit der Erkrankung steht und nicht dem erwarteten Behandlungsergebnis entspricht • Jeder Fall mit verlängertem stationären Aufenthalt • Erfordernis einer zusätzlichen Operation
Geringfügig	• Erhöhter P egebedarf
Sehr geringfügig	• Zwischenfall, der jedoch keinerlei weitere p egerische oder chirurgische Maßnahmen nach sich zieht

Finanzieller Schaden

Im bereits vorgestellten OWASP Modell wird der nanzielle Schaden eingeschätzt. Beispielhaft kann die Klassi zierung des nanziellen Schadens wie nachfolgend aussehen (Anordnung von hohem zu niedrigem Schaden):

- Insolvenz
- erhebliche Auswirkung auf den Jahresgewinn
- geringe Auswirkung auf den Jahresgewinn
- Geringer als die Kosten zur Behebung der Schwachstelle

Datenschutz

Ebenso wird der Datenschutz im OWASP-Modell eingeordnet. Hierbei richtet sich die Einordnung danach, welche bzw. wie viele Daten offengelegt werden konnten und der Anzahl der Personen die betroffen sind. Die Darstellung erfolgt wieder von extrem zu sehr geringfügig und ist als Beispiel für eine Klassi zierung der Schäden des Datenschutzes zu betrachten.

Art und Umfang der Daten:

- Offenlegung aller Daten
- Offenlegung umfangreicher kritischer Daten
- Offenlegung minimaler kritischer Daten und Offenlegung umfangreicher nicht sensibler Daten
- Offenlegung minimaler nicht sensibler Daten

Anzahl der betroffenen Personen:

- Millionen von Personen
- Tausende von Personen
- Hunderte von Personen
- Eine Einzelperson

In der BSI Studie eCARE werden sowohl die gesundheitlichen als auch die Datenschutzschäden in einer Tabelle aufgegriffen. Es ist zu sehen, dass jeder gesundheitliche Schaden an einer Person höher bewertet wurde, als der Schaden im Bereich des Datenschutzes.[31] Dies könnte in möglichen Modellen zur Cybersicherheit im medizinischen Bereich aufgegriffen werden. Die Einteilung der Schadensklassen und der jeweiligen Beschreibungen kann auch vom Hersteller selbst erstellt und de niert werden, ebenso wie die Risikoakzeptanzkriterien. Ein Risiko ist erst dann akzeptabel, wenn es so gering wie möglich ist und der Nutzen des Medizinprodukts den Risiken überwiegt.[32]

2.4.4 Klassi zierung der Wahrscheinlichkeit

In einigen Modellen wird die Eintrittswahrscheinlichkeit über die Beschreibung und Einordnung der Randbedingungen, in welchen das Produkt eingesetzt wird, und der Beschreibung des potenziellen Angreifers eingeordnet. So z.B. in den Modellen CWSS, OWASP und DREAD.[13, 14, 16] Die Klassi zierung der Wahrscheinlichkeit kann auch vom Hersteller selbst übernommen werden. Das Johner Institut nennt ein Beispiel zur Einordnung der Wahrscheinlichkeit über die Häu gkeit des Vorkommens eines Vorfalls. Dieses Beispiel ist in Tabelle 2.14 zu sehen:[32]

Tabelle 2.14: Beispiel der Wahrscheinlichkeitsklassen in Anlehnung an [32]

Begriff	Beschreibung	Häu gkeit (pro Behandlung)
Häu g	Ein- oder mehrmals pro Behandlung	x 10^0(1)
Wahrscheinlich	Kann bei bestimmungsgemäßem Gebrauch vorkommen	10^{2} x < 10^0
Gelegentlich	Tritt in unregelmäßigen Abständen mehrfach pro Monat/Jahr auf	10^{4} x < 10^{2}
Entfernt vorstellbar	Ein bis mehrmals pro Lebensdauer des Medizinprodukts	10^{6} x < 10^{4}
Unwahrscheinlich	Nicht während Lebensdauer des Medizinprodukts	10^{8} x < 10^{6}
Unvorstellbar	Nicht während der Lebensdauer aller Produkte	x < 10^{8}

2.5 Das Medizinprodukt und seine Vernetzung

Die De nition nach ISO 14971 für ein Medizinprodukt lautet:

„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 spezi schen 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

- Desinfektionsmitte
- Hilfen für Menschen mit Behinderungen
- Produkte, die tierische und/oder menschliche Gewebe enthalten
- Produkte für die In-vitro-Fertilisation oder Technologie für die künstliche Befruchtung.“[9]

Somit können Medizinprodukte sehr vielfältig sein und besitzen Schnittstellen, über welche sie in der Telematikinfrastruktur vernetzt werden können. In der Telematikinfrastruktur wird die Vernetzung verschiedener medizinischer Geräte realisiert. Des Weiteren werden über die Telematikinfrastruktur beispielsweise Arztpraxen, Krankenhäuser, Apotheken, Medizintechnik und Patientendaten miteinander verknüpft, um die Arbeitswege und den Aufwand gering zu halten. Somit können z.B. auf der Gesundheitskarte Notfalldaten gespeichert werden, die es jedem Arzt ermöglichen, in Notsituationen schnell und ef zient handeln zu können. Durch die elektronische Patientenakte können Ärzte durchgeführte Behandlungen, Befunde und Dokumente der Patientenakte einsehen. Des Weiteren können medizinische Rezepte seit diesem Jahr in allen Apotheken ohne ein Papierrezept mit der Gesundheitskarte über das E-Rezept eingelöst werden. [33] Ein schematisches Beispiel für die Telematikinfrastruktur ist in Abbildung 2.6 dargestellt.

Abbildung 2.6: Telematikinfrastruktur Beispiel in Anlehnung an [34]

Das BSI hat eine Studie zur Cybersicherheit von Arztpraxen vorgenommen, in welcher sie 16 Arztpraxen aus verschiedenen Bereichen (sechs Haus- und Allgemeinarztpraxen, fünf Zahnarzt-, drei psychotherapeutische und zwei radiologische Praxen) zum Thema Cybersicherheit befragt wurden. In 2.7 werden die Häu gkeiten der Schwachstellen aus den Arztpraxen in Prozent dargestellt.

Auch wenn diese Statistik nicht als repräsentativ für andere Praxen zu betrachten ist, ist dennoch aus der Statistik in der Abbildung 2.7 zu entnehmen, dass es in den befragten Praxen Sicherheitslücken gibt und hier Handlungsbedarf besteht.[35]

Abbildung 2.7: Häu gkeit der Schwachstellen in Prozent in Anlehnung [35]

3 Bedrohungsmodellierung

Die Risikomodellierung wird hier an einem Patientenmonitor mit bekannten und behobenen Sicherheitslücken, welche in der BSI-Studie ManiMed aufgefallen sind durchgeführt. Betrachtet wird eine der Sicherheitslücken. Aus rechtlichen Gründen sind die Angaben zum Patientenmonitor beispielhaft und stehen nicht für ein real existierendes Produkt, sondern sind anhand von Informationen zu einzelnen Patientenmonitoren zusammengestellt.

3.1 Aufgaben und Funktionsweise eines Patientenmonitors

Die Aufgabe der Patientenmonitore ist es, die Vitalwerte des Patienten zuverlässig in Echtzeit anzuzeigen, je nach Modell die Werte über das Netzwerk an die Patientenakte zu senden und die Patientenakte aufzurufen. Sie kommen in Krankenhäusern, auf Intensivstationen, im Operation (OP) und zur generellen Patientenüberwachung sowohl stationär als auch tragbar zum Einsatz.[21]

Betrachtet wird ein Patientenmonitor mit den oben genannten Aufgaben, welcher vorwiegend während einer Operation (OP) zum Einsatz kommt. In der Analysephase muss zunächst festgelegt werden, wie die Cybersicherheitsziele für das Gerät aussehen. In folgendem wird die Sicherheit des Patientenmonitors so betrachtet, dass keine von außen gestellten Sicherheitsvorkehrungen berücksichtigt werden, sondern nur das Produkt an sich. Sicherheitsvorkehrungen in der Telematikinfrastruktur werden nicht betrachtet und somit kann auch von keiner Sicherheit von außen ausgegangen werden.

Beschreibung der entdeckten Sicherheitslücke
In der Kommunikation zwischen dem Patientenmonitor und dem Server überprüft der Patientenmonitor die ankommenden Zerti kate zu wenig, so dass sich hier ein Angreifer die Position des Man in The Middle einnehmen kann, sofern er sich vorher Zugriff auf ein vertrauenswürdiges Zerti kat verschafft hat. Dies kann er durch einen Brut Force Angriff erlangen. In Folge des Man in the Middle Angriffs kann der Patientenmonitor zum Abstürzen gebracht oder sogar übertragene Daten abgefangen und modi ziert werden.[21] Somit würde es die Schutzziele der Verfügbarkeit, Vertraulichkeit und der Integrität betreffen.

3.2 Risikoanalyse

Im Folgenden wird diese Schwachstelle des Patientenmonitors im Rahmen der Arbeit in den Modellen DREAD, OWASP, CWSS, STRIDE und dem IT-Grundschutz modelliert und die dabei entstehenden Problematiken aufgezeigt.

3.2.1 Analyse nach STRIDE

STRIDE wird dazu verwendet, mögliche Risiken identi zieren zu können und diese in Angriffsarten zu unterteilen, um sie anschließend besser analysieren zu können. Es wird zunächst ein Daten uss-diagramm erstellt, welches das zu betrachtende System darstellt.

Abbildung 3.1: Daten ussdiagramm zwischen Patientenmonitor Server

In der Abbildung 3.1 wird der Patientenmonitor dargestellt, welcher die Vitaldaten vom Patienten erhält, diese verarbeitet, zum Server überträgt und mit diesem kommuniziert. Für den Aufbau der Kommunikation werden Zerti kate verwendet. In dem zu betrachtenden Szenario bzw. der Sicherheitslücke werden die Zerti kate, die der Patientenmonitor empfängt, an diesem nicht genügend überprüft, so dass sich ein Angreifer als der Server ausgeben und sich somit zwischen die Kommunikation schalten kann, dies ist in Abbildung 3.2 dargestellt.

Abbildung 3.2: Daten ussdiagramm eines Man in the Middle Angriffs

Anschließend wird die Bedrohung in eine der in Kapitel 2.2.1 beschriebenen Angriffskategorien unterteilt. Da dieser Angriff die Verfügbarkeit des Patientenmonitors einschränkt, wäre dieser Angriff hier als ein Denail of Service Angriff einzuschätzen. Da der Angreifer auch die übertragenen Daten mitlesen oder manipulieren könnte, kann dieser Angriff auch in Veröffentlichung von Informationen oder Tampering/ Manipulation eingeordnet werden. In den folgenden Modellen wird die Einschränkung der Verfügbarkeit betrachtet und eingeordnet.

3.2.2 Analyse nach DREAD

Zusammenfassend müssen in diesem Modell Werte für die Parameter Schadenspotential, Reproduzierbarkeit, Ausnutzbarkeit, betroffene Benutzer und Auf ndbarkeit vergeben werden. Der Patientenmonitor hat die Funktion, die Vitalparameter zuverlässig zu überwachen, in diesem Beispiel vorwiegend im OP. Somit sind Ausfälle wie Abstürze, in denen die Verfügbarkeit betroffen ist, eine Gefährdung, welche nach ihrem Schweregrad eingeordnet werden muss. Hierbei ist zu beachten, dass die Vitalwertüberwachung des Patienten bei einem Absturz unterbrochen wird und die optimale Versorgung des Patienten nicht mehr garantiert werden kann. Stehen keine Alternativen zur Verfügung, kann es im schlimmsten Fall zum Tod des Patienten führen. Wenn man sich nun an der Einschätzung in der eCare Studie des BSIs orientiert, ist der mögliche Tod eines Patienten als größter einzutretender Schaden einzuordnen. Somit muss für die Kategorie „Schadenspotential “ der Wert 3 vergeben werden. Des Weiteren entstehen bei einem Man in the Middle Angriff daten- und integritätsbezogene Sicherheitslücken. Die übertragenen Daten können abgefangen und manipuliert werden. Hier muss überprüft werden, welche Daten genau verschickt werden, ob diese einem Patienten zugeordnet werden können und ob der Angreifer die Vitaldaten verändern kann. In der Kategorie „Reproduzierbarkeit“ stellt sich die Frage, wie leicht sich der Angriff wiederholen lässt. Da sich die Sicherheitslücke serienmäßig an diesem Monitortyp be ndet, ist davon auszugehen, dass sich der Angriff an allen Monitoren dieses Typs reproduzierbar lässt, bis die Sicherheitslücke geschlossen wurde. Somit muss der Wert 3 festgelegt werden. Unter der „Ausnutzbarkeit“ ist der Erfahrungsschatz der Angreifer zu verstehen. Wie viel muss man für die Ausnutzung dieser Sicherheitslücke wissen? Hierbei steht 1 für sehr viel Wissen erforderlich und 3 für wenig Wissen erforderlich. Der Angreifer muss in diesem Beispiel zwei Angriffe (den Brutforce Angriff auf das vertrauenswürdige Zerti kat und den Man in the Middle Angriff) durchführen. Somit ist von einem fortgeschrittenen Wissensstand auszugehen und wird mit 2 „fortgeschrittenes Wissen“ bewertet. In der Kategorie „betroffene Benutzer“ ist die zur Einkategorisierung erforderliche Anzahl der betroffenen Benutzer nicht zahlenmäßig bestimmt. Die Begriffe „die meisten Benutzer“, „einige Benutzer“ und „einige wenige Benutzer“ sind unbestimmt. Stellt sich die Frage, ab welcher Anzahl von Benutzern diese Kategorie als „viele“ oder „wenig“ zu klassi zieren ist. In dem OWASP-System wurden erforderliche Anzahl an Benutzern bei Datenschutzverletzungen aufgegriffen. Da hier allerdings von einem Benutzer auszugehen ist, solange es kein zentral geführter Angriff auf alle diese Patientenmonitore gleichzeitig ist, kann dieser Wert mit 1 bewertet werden. Da dies dem unteren Maß der möglichen betroffenen Benutzer entspricht. Der Wert der „Auf ndbarkeit “ wird im Beispiel mit 1 bewertet, da er versteckt ist und aktives Suchen nach Eintrittsmöglichkeiten in das System erfordert.[36] In der Tabelle 3.1 sind die eingetragenen Werte zusammengefasst.

Tabelle 3.1: Beispielmodellierung Patientenmonitor Wertezusammenfassung für DREAD

Kategorie	Wert
Schadenspotential	3
Reprodukzierbarkeit	3
Ausnutzbarkeit	2
betroffene Benutzer	1
Auf ndbarkeit	1

Daraus ergibt sich die Formel:
$Score = (3 + 3 + 2 + 1 + 1) \quad = 5$
$Score = 2$

Der Durchschnitt der eingetragenen Werte ist 2. Somit lässt sich das Risiko, welches mit dieser Sicherheitslücke einhergeht, als Mittel einordnen. Dieses Modell ist leicht anzuwenden, da die Einschätzung sehr grob ist und nur 5 Werte eingeschätzt werden müssen. Allerdings sind die Nachteile, wie im Abschnitt 2.2.2 erläutert, dass es eine subjektive Einschätzung ist und keine Wichtung der Faktoren existiert.

3.2.3 Analyse nach OWASP

Auch im OWASP System müssen Werte eingeschätzt werden. Bei der Bewertung der einzelnen Kategorien ist auffällig, dass über umfangreiche Kenntnisse zum Produkt und deren Sicherheitslücken verfügt werden muss. Dies macht es für außenstehende Personen herausfordernd, Sicherheitslücken in diesem Modell einzuschätzen.

Bedrohungsfaktor
Laut der Beschreibung, der zu vergebenden Werte im Bereich Fähigkeiten, sind für einen Man in The Middle Angriff Netzwerk- und Programmierkenntnisse gefordert, wenn nicht gar gezielte Fähigkeiten zum Eindringen in ein Sicherheitssystem. Im Bereich des Motivs ist es schwierig abzuschätzen, was sich genau als lohnenswert darstellt. Dies hängt vom einzelnen Angreifer ab, sind es persönliche Ziele, jemandem Schaden zuzufügen oder sich selbst zu bereichern im Sinne von Geld oder Macht.. Welche Gelegenheiten bieten sich, um diesen Angriff durchzuführen? Hier ist wieder einzuschätzen, welche Ressourcen für diesen Angriff erforderlich sind und mit welchem Aufwand sie verfügbar sind. In diesem Beispiel wird ein vertrauenswürdiges Zerti kat über die Verbindung zwischen Server und Patientenmonitor gefordert, welches man wie oben beschrieben durch einen Brut Force Angriff erlangen kann. Somit ist der Zugriff auf eine spezielle Ressource erforderlich, welche erst durch einen anderen Angriff herausgefunden werden muss. Somit ist es als Wert spezieller Zugriff oder spezielle Ressource einzuschätzen und erfordert Wert 4. In der Kategorie Größe muss eingeordnet werden, von welchen Personen der Angriff durchgeführt werden kann. Dieser Angriff kann von einem anonymen, beliebigen Internetbenutzer ausgeführt werden, sofern er sich vorher Zugriff auf ein Zerti kat verschafft hat. Somit ist der Wert 9 zu wählen. Die beschriebenen Werte sind in Tabelle 3.2 zusammengefasst.

Tabelle 3.2: OWASP Bedrohungsfaktor Beispielmodellierung Patientenmonitor

Kategorie	Beschreibung
Fähigkeitsniveau - Wie technisch versiert ist diese Gruppe von Bedrohungsagenten?	• 6 Netzwerk- und Programmierkenntnisse (6) • 9 Fähigkeiten zum Eindringen in Sicherheitssysteme (9)
Motiv - Wie motiviert ist diese Gruppe von Bedrohungsagenten, diese Schwachstelle zu nden und auszunutzen?	• Geringe oder keine Belohnung (1), • mögliche Belohnung (4), • hohe Belohnung (9)
Gelegenheit - Welche Ressourcen und Gelegenheiten sind erforderlich, damit diese Gruppe von Bedrohungsagenten diese Schwachstelle nden und ausnutzen kann?	• spezieller Zugriff oder spezielle Ressourcen erforderlich (4),
Größe - Wie groß ist diese Gruppe von Bedrohungsagenten?	• anonyme Internetbenutzer (9)

Vulnerabilitätsfaktor

Unter Vulnerabilität versteht man die Verwundbar- oder auch Verletzbarkeit, diese wird in folgendem beginnend mit der Entdeckung eingeordnet. Wie bereits im Modell DREAD beschrieben ist die Angriffsstelle versteckt, da sie nicht direkt gefunden werden kann, es sei denn, es wird danach gesucht. Somit ist der Wert mit 3 „schwierig “ einzuordnen. Die Ausnutzung wird in diesem Fall als schwierig bewertet, da die Voraussetzung für die Ausnutzung dieser Schwachstelle ein vertrauliches Zerti kat ist. In der Kategorie des Bewusstseins ist diese Schwachstelle normalerweise versteckt und nicht leicht erkennbar, allerdings wurde diese Schwachstelle bereits in einer Studie herausgefunden und veröffentlicht, somit wäre sie jetzt als öffentlich bekannt einzustufen. Da es sich allerdings um eine Beispielmodellierung handelt, wird zunächst davon ausgegangen, dass diese Sicherheitslücke noch nicht bekannt ist und wird somit als versteckt (Wert 4) eingestuft. Wie gut ein Exploit erkannt wird, ist davon abhängig, ob der Angreifer das Gerät zum Absturz bringt oder die Daten nur unbemerkt erfasst. Wenn der Angreifer nur Daten erfasst, ist es wie die AVG schon geschrieben hat, schwer zu erkennen, dass ein Man in the Middle Angriff statt ndet [36]. Die AVG ist ein Sicherheitssoftwarehersteller, welcher sich mit der digitalen Sicherheit beschäftigt. Da in der Bedrohungseinordnung das Szenario des Ausfallens im OP angesprochen wurde, wird hier auch von einem möglichen Ausfall ausgegangen und somit ist von einer aktiven Erkennung des Angriffs auszugehen (Wert 1) sofern der Patientenmonitor abstürzt. Die beschriebenen Werte sind in Tabelle 3.3 zusammengefasst.

Tabelle 3.3: OWASP Vulnerabilitätsfaktor Beispielmodellierung Patientenmonitor

	Beschreibung und Wertezuordnung
Entdeckung - Wie einfach ist es für diese Gruppe von Bedrohungsagenten, diese Schwachstelle zu entdecken?	• schwierig (3),
Ausnutzung - Wie einfach ist es für diese Gruppe von Bedrohungsagenten, diese Schwachstelle tatsächlich auszunutzen?	• schwierig (3),
Bewusstsein - Wie bekannt ist diese Schwachstelle bei dieser Gruppe von Bedrohungsagenten?	• versteckt (4),
Intrusion Detection - Wie wahrscheinlich ist es, dass ein Exploit erkannt wird?	• Aktive Erkennung in der Anwendung (1),

Technische Ein ussfaktoren
Dieser Faktor ist in der Berechnung des Risikos, für das Inverkehrbringen eines Medizinproduktes zu verwenden, da hier die Schutzziele der MDR verwendet werden. Im Bereich der Technischen Ein ussfaktoren entstehen die Werte über folgende Überlegungen:

In diesem Fall können Daten wie die Patientennummer und die Vitaldaten abgegriffen werden, sofern diese nicht bei der Übertragung verschlüsselt wurden. Da es sich um personenbezogene Gesundheitsdaten / Vitalwerte handelt, welche sich allerdings nur auf die eine Person beziehen, die gerade überwacht wird, ist ohne eine Verschlüsselung davon auszugehen, dass es sich um die Kategorie Offenlegung minimaler kritischer Daten handelt. In diesem Fall schwierig zu bewerten ist, was mit allen Daten gemeint ist. In diesem Fall ist nicht klar, was mit „allen Daten“ gemeint ist. Sind alle Daten die übertragen werden, alle Daten über den Patienten, oder alle Daten aus einer möglichen Datenbank, gemeint.

Im Bereich des Integritätsverlustes muss abgeschätzt werden, inwieweit die Daten durch den Man in the Middle Angriff verändert werden können. Da in diesem Angriff die übertragenen Daten auch manipuliert werden können, muss somit von starken Beschädigungen der Daten ausgegangen werden.

Wenn der Monitor durch einen Man in the Middle Angriff abstürzt, wird dieser nach 20 sek. wieder neu gestartet. Hierbei ist allerdings die Frage, ob er auch wieder funktionieren würde, wenn nach den 20 Sekunden der Angriff immer noch statt ndet. Somit könnten hier nach der kategorischen Beschreibung alle Werte angegeben werden, von Diensten unterbrochen bis alle Dienste vollständig verloren.

Verlust der Verantwortlichkeit - hierbei bleibt abzuschätzen, ob man den Angreifer erkennen und zurückverfolgen könnte. Dies hängt jedoch auch stark vom Angreifer selbst ab, wie gut er sich selbst verschleiert. Die beschriebenen Werte sind in Tabelle 3.4 zusammengefasst.

Tabelle 3.4: OWASP Technische Ein ussfaktoren Beispielmodellierung Patientenmonitor

	Beschreibung und Wertezuordnung
Verlust der Vertraulichkeit - Wie viele Daten könnten offengelegt werden und wie sensibel sind sie?	• Offenlegung minimaler kritischer Daten (6),
Integritätsverlust - Wie viele Daten könnten beschädigt sein und wie stark sind sie beschädigt?	• Minimal leicht beschädigte Daten (1), • minimal stark beschädigte Daten (3), • umfangreiche leicht beschädigte Daten (5), • umfangreiche stark beschädigte Daten (7), • alle Daten völlig beschädigt (9)
Verlust der Verfügbarkeit - Wie viele Dienste könnten verloren gehen und wie wichtig sind sie?	• Dienste unterbrochen (1), • minimale primäre Dienste unterbrochen (5), • umfangreiche sekundäre Dienste unterbrochen (5), • umfangreiche primäre Dienste unterbrochen (7), • alle Dienste vollständig verloren (9)
Verlust der Verantwortlichkeit - Sind die Aktionen der Angreifer auf eine Einzelperson zurückzuführen?	• möglicherweise rückverfolgbar (7), • völlig anonym (9)

Geschäftliche Ein ussfaktoren

Im Bereich der geschäftlichen Ein ussfaktoren werden Schäden in den Kategorien nanzielle Schäden, Reputationsschäden, Aufsehens und Datenschutzschäden bewertet. Normalerweise ist dieser Faktor bevorzugt zu behandeln, sofern genügend Informationen vorliegen [14]. Da dies keine Schutzziele der MDR im für das Inverkehrbringen der Medizinprodukte sind und somit für die Zulassung des Produkts nicht relevant sind, muss hier der technische Ein ussfaktor verwendet werden.

Finanzieller Schaden ist als geringe Auswirkung auf den Jahresgewinn des Herstellers aber auch der Gesundheitseinrichtung zu bewerten. Bei dem Hersteller könnte durch den Verlust wichtiger Kunden, durch die Behebung der Schwachstelle und eventuelle Schadenszahlungen bei einer möglichen Klage ein Ein uss auf den Jahresgewinn entstehen. In diesem Fall gehen wir davon aus, dass diese Schäden in geringem Umfang entstehen könnten. Also wird der Wert hier mit 3 „Geringe Auswirkung auf den Jahresgewinn“ angegeben.

In der Kategorie Reputationsschäden ist zu betrachten, bei wem dieser Schaden ausgelöst wird. Der Patientenmonitor kommt in medizinischen Einrichtungen zum Einsatz, in welchen auch der gesundheitliche Schaden im Schadensfall an Patienten entstehen würde. Der Imageschaden bezieht sich zunächst auf das Krankenhaus, weitergehend allerdings auf den Hersteller des Patientenmonitors bzw. generell auf den Hersteller des fehlerhaften Produkts. Wenn eine Gesundheitseinrichtung beispielsweise wiederkehrende Probleme mit der Verfügbarkeit eines Patientenmonitors durch Man in the Middle Angriffe hat, ist es möglich, dass dieses Krankenhaus sich davon distanziert, weitere Geräte bei diesem Hersteller zu kaufen. Der Verlust wichtiger Kunden ist somit für den Hersteller denkbar.

In der Kategorie Nichteinhaltung soll abgeschätzt werden, wie viel Aufsehen ein Verstoß gegen die Richtlinien hervorruft. Die Datenschutzverletzung betrifft in diesem Szenario die Person, die zum Zeitpunkt des Angriffs von dem Patientenmonitor überwacht wird. Somit ist die Kategorie mit einer Einzelperson Wert 3 zu bewerten. Die beschriebenen Werte sind in Tabelle 3.5 zusammengefasst.

Tabelle 3.5: OWASP Geschäftliche Ein ussfaktoren Beispielmodellierung Patientenmonitor

	Beschreibung und Wertezuordnung
Finanzieller Schaden - Wie hoch ist der nanzielle Schaden, der durch einen Exploit entsteht?	• geringe Auswirkung auf den Jahresgewinn (3),
Reputationsschaden - Führt ein Exploit zu einem Reputationsschaden, der dem Unternehmen schaden würde?	• Verlust wichtiger Kunden (4),
Nichteinhaltung - Wie viel Aufsehen erregt die Nichteinhaltung?	• Geringfügiger Verstoß (2), • klarer Verstoß (5), • schwerwiegender Verstoß (7)
Datenschutzverletzung - Wie viele personenbezogene Daten könnten offengelegt werden?	• Eine Einzelperson (3),

Minimalwert:

$$\text{Bedrohungsfaktor} = (6 + 1 + 4 + 9) \quad =4 = 5$$
$$\text{V ulnerabilit ätsfaktor} = (3 + 3 + 4 + 1) \quad =4 = 2\,;75$$
$$\text{Gesamtwahrscheinlichkeit} = (5 + 2\,;75) =2 = 3\,;875$$

Maximalwert:

$$\text{Bedrohungsfaktor} = (9 + 9 + 4 + 9) \quad =4 = 7\,;75$$
$$\text{V ulnerabilit ätsfaktor} = (3 + 3 + 4 + 1) \quad =4 = 2\,;75$$
$$\text{Gesamtwahrscheinlichkeit} = (7\,;75 + 2;75) =2 = 5\,;25$$

Technischer Ein ussfaktor:
Minimalwert $TechnischerEinflussfaktor = (6 + 1 + 1 + 7) \quad 4 = 3;75$
Maximalwert $TechnischerEinflussfaktor = (6 + 9 + 9 + 9) \quad 4 = 8;25$
Minimalwert: hier Medium
Maximalwert: Hoch

Geschäftlicher Ein ussfaktor:
Minimalwert $GeschäftlicherEinflussfaktor = (3 + 4 + 2 + 3) \quad 4 = 3$
Maximalwert $GeschäftlicherEinflussfaktor = (3 + 4 + 7 + 3) \quad 4 = 4;25$
Minimalwert: Medium
Maximalwert: Medium

In der Einordnung des OWASP Systems ist abschließend zu bemerken, dass es sehr komplex ist, diese Werte einzuordnen und keine klaren Regeln zur Einordnung existieren. Ebenso ist auffällig, dass die Einordnung von dem entstehenden Szenario abhängig ist und somit die Einschätzung je nach Szenario unterschiedlich bewertet werden kann. Da das Produkt und deren Sicherheitslücken allgemein bewertet werden sollen, ist dieses Modell nur eingeschränkt geeignet, um das allgemeine Risiko der Sicherheitslücke einzuordnen. Des Weiteren sind die einzutragenden Werte sehr subjektiv, da es keine messbaren Vorgaben gibt, nach denen die Kategorien eingeordnet werden können. Es fehlen Echtwerte zu einem Beispielprodukt. Im Modell müssten die Werte genauer beschrieben werden, wenn das Ergebnis des Modells auch durch unterschiedliche Anwender reproduziert sein soll.

3.2.4 Analyse nach CWSS

Für die CWSS Modellierung gibt es eine Website, in welcher man die Werte der unterschiedlichen Kategorien auswählen kann und die Berechnung online statt ndet. Zur Modellierung selbst wurde allerdings im Rahmen der Arbeit eine Exceltabelle erstellt, welche das Ergebnis der Modellierung berechnet. In Abbildung 3.3 ist die Tabelle und deren Ergebnisse zu sehen. In diesem Beispiel wurde wieder der Patientenmonitor mit der Schwachstelle der Zerti katsüberprüfung, in welchem ein Man in the Middle Angriff statt nden kann, gewählt.

Abschließend ist festzuhalten, dass dieses Modell zahlreiche Werte mit einbezieht, was umfangreiches Wissen über das Produkt und das Szenario, in welchem es Verwendung nden, benötigt. Vermeintlich erleichtert wird es dadurch, dass bei verschiedenen Werten auch „unbekannt “ oder der „Median “ angegeben werden kann. Dies sollte nicht überstrapaziert werden, da das Modell sonst nicht mehr aussagekräftig ist.

Abbildung 3.3: Ergebnisse der CWSS Modellierung

3.2.5 Analyse nach IT-Grundschutz

Im IT-Grundschutz werden zunächst die möglichen Gefahren eingeordnet. In diesem Fall wird der Man in the Middle Angriff als Verhindern von Diensten eingeordnet, da er zum Absturz des Monitors führen kann und somit die Vitalwertüberwachung nicht mehr verfügbar ist. Da es ebenso möglich ist, die Werte zu verändern und zu sabotieren, wurden diese Gefahren ebenso eingeordnet.

Abbildung 3.4: Bedrohungsliste am Patientenmonitor bezogen auf die beschriebene Schwachstelle

Nachdem eine Liste der möglichen Bedrohungen erstellt wurde, müssen die Gefahren eingeschätzt werden.

Abbildung 3.5: BSI Risikomodellierung Einordnung und Beschreibung

Nach dieser Modellierung und Einordnung in eine Risikomatrix wäre das Risiko in diesem Beispiel ein vertretbares Risiko.

3.2.6 Zusammenfassung der Modellierungen

Durch die Analyse der Bedrohung im STRIDE Modell wurde die Einschränkung der Verfügbarkeit in die Kategorie Denail of Service eingeordnet. In diesem Modell ndet keine weitere Einschätzung der Risiken statt, diese wurde in den nachfolgenden Modellen vorgenommen. Durch die DREAD Modellierung wurde die betrachtete Sicherheitslücke des Patientenmonitors in ein mittleres Risiko eingeschätzt. Im OWASP Modell wurden mehrere Werte berechnet, da die im OWASP Modell vorgegebenen Kriterien nicht immer passend waren und von dem Szenario, in welchem sich der Patientenmonitor be ndet, abhängig sind. Somit wurde ein Minimalwert und ein Maximalwert berechnet. In der Bewertung wurde der technische Ein ussfaktor zur Einordnung des Risikos verwendet, da nur dieser für die Zulassung des Medizinproduktes relevant ist. Der geschäftliche Ein ussfaktor wurde als Vergleichswert mitberechnet. Es hat sich herausgestellt, dass die Risikoeinschätzung mit den technischen Ein ussfaktoren höher eingeordnet wurde, als die Einordnung mit dem geschäftlichen Ein ussfaktor. Die CWSS Modellierung hat den Wert 15,01 als Ergebnis. Dieser müsste noch entsprechend interpretiert werden, was von der vorherigen Einordnung der Risikoakzeptanzkriterien des Herstellers abhängig ist. Das CWSS Modell ist sehr umfangreich. Dadurch wird es komplex in der Anwendung und erfordert viel Wissen über das Produkt und das Szenario, in welchem sich das Produkt be ndet. Da verschiedene Einsatzmöglichkeiten des Patientenmonitors existieren, müsste hier auf verschiedene Szenarien eingegangen werden, was die allgemeine Risikoeinschätzung eines Produktes erschwert.

Im BSI IT-Grundschutz 200-3 werden die Gefahren anhand zweier Metriken (der Wahrscheinlichkeit und dem Schadenspotential) eingeordnet und anschließend in einer Risikomatrix bewertet. In der Modellierung wurden die vom BSI beschriebenen Schadenskategorien verwendet. Somit wurde das Schadenspotential durch den Man in The Middle Angriff als katastrophal (Tod eines Patienten) und die Wahrscheinlichkeit des Eintritts als unwahrscheinlich eingeordnet. Nach der BSI Risikomatrix wäre dies als ein vertretbares Risiko einzuordnen.

Tabelle 3.6: Zusammenfassung der Ergebnisse aus den verschiedenen Modellen zum Patientenmonitor

Modell	Mögliche Einordnung	Risiko Patientenmonitor	Bemerkung
DREAD	1 niedrig bis 3 hoch	2 mittleres Risiko	
OWASP	1 bis 9	Minimalwert: 3,75 (Medium) Maximalwert 8,25(Hoch)	hier wurden zwei Werte berechnet da die Kategorien nicht klar de niert waren und somit verschiedene Werte eingeordnet wurden
CWSS	1 bis 100	15,01	als niedriges bis mittleres Risiko Klassi zierbar je nach de nierter Risikoakzeptanz
BSI IT-Grundschutz 200-3		vertretbares Risiko	

Bei der Modellierung ist auffällig, dass in den Modellen OWASP, CWSS, und DREAD die Wahrscheinlichkeit eines Angriffes über die Situation, in welcher sich das Medizinprodukt be ndet, modelliert werden. Somit sind diese Modelle abhängig von dem Szenario, in welchem sich das Gerät be ndet, und werden je nach Szenario unterschiedlich ausfallen. Alle Modelle hatten ihre Schwierigkeiten in der Einordnung der Schadens- und Wahrscheinlichkeitsklassen. Diese müssen laut der ISO/EN 14971 vom Hersteller festgelegt werden. Die Klassi zierung, die in den Modellen selbst steht, müssen auf den medizinischen Bereich angepasst werden.

4 Zusammenfassung und Ausblick

Ziel dieser Arbeit war es, Bedrohungsmodelle wie STRIDE, OWASP und dem BSI IT-Grundschutz auf die Cybersicherheit im medizinischen Bereich an einem ktiven Beispiel anzuwenden, um Wege und Problematiken für die Klassi zierung des Risikos aufzuzeigen.

4.1 Zusammenfassung

Zusammenfassend wurden in der Arbeit die Modelle DREAD, OWASP, CWSS, STRIDE und der IT-Grundschutz vorgestellt. Des Weiteren wurde das Risikomanagement vorgestellt. Es wurde aufgezeigt, dass zunächst ein Risikomanagementplan erstellt werden muss, welcher die Randbedingungen des Risikomangements festlegt. Es wurden die drei Phasen des Risikomanagements (Analyse, Bewertung und Beherrschung) vorgestellt, welche während des gesamten Lebenszyklus des Medizinproduktes parallel statt nden. Nachfolgend wurden im Bereich Cybersicherheit die Schutzziele für die Medizintechnik de niert und erklärt. Anschließend wurden die statistisch häu gsten Angriffsformen aufgezeigt und Möglichkeiten zur Einordnung der Wahrscheinlichkeitsklassen und der Schadenspotentialklassen dargestellt. In der beispielhaften praktischen Modellierung wurde der Patientenmonitor als Medizinprodukt gewählt. Der Patientenmonitor hat die Aufgabe, die Vitalparameter des Patienten zuverlässig zu überwachen. In dieser beispielhaften Risikomodellierung wurde angenommen, dass der Patientenmonitor im OP eingesetzt wird und während der Überwachung der Vitalparameter ausfallen könnte. In diesem Szenario könnte dies zum größtmöglichen Schaden führen, dem Tod des Patienten. In Tabelle 3.6 sind die Ergebnisse der verschiedenen Modellierungen zusammengefasst und wurden nachfolgend weiter erläutert. Es hat sich herausgestellt, dass die Modelle DREAD, OWASP und CWSS aufgrund der spezi schen Einordnung der Kategorien die Wahrscheinlichkeit für das jeweilige Szenario eingeschätzt wird. Somit wird kein allgemeingültiges Risiko für diese Schwachstelle erstellt, sondern das Risiko in diesem Szenario bewertet. Für die Modellierung des Risikos nach dem BSI IT-Grundschutz wurde das im BSI IT-Grundschutz beschriebene Schadenspotential und die Wahrscheinlichkeitseinordnung verwendet. Dies ist ohne weitere De nition eine subjektive Bewertung und müsste genauer im Risikomanagementplan beschrieben werden.

4.2 Fazit

Man konnte das Cybersicherheitsrisiko eines Man in the Middle Angriffs auf einen Patientenmonitor anhand der verschiedenen Modelle klassi zieren. Hierbei ist jedoch erkennbar, dass die Modelle zu unterschiedlichen Ergebnissen kommen können. Grund hierfür ist eine unterschiedliche Wichtung verschiedener Parameter. Während die Modelle DREAD, OWASP und CWSS eine szenarienbezogene Wahrscheinlichkeit berechnen, wird in dem BSI IT-Grundschutz zuvor die Wahrscheinlichkeit klassi ziert und de niert. Hierbei ist festzuhalten, dass die im BSI IT-Grundschutz be ndliche Klassi zierung nur grob de niert ist und somit für den medizinischen Bereich im Risikomanagementplan genauer auf das zu Bewertende Produkt angepasst werden sollte.

4.3 Ausblick

Die im Fazit benannten Herausforderungen sind vor allem, dass die Medizingeräte in unterschiedlichen Situationen zum Einsatz kommen. In den Modellen DREAD, CWSS und OWASP wird versucht, die Wahrscheinlichkeit eines Angriffs durch das gegebene Szenario zu modellieren und zu berechnen. Da die Szenarien, in denen z.B. der Patientenmonitor eingesetzt wird, sehr unterschiedlich sind, müssten hier alle möglichen Szenarien modelliert werden, um eine generelle Risikoeinschätzung für das Produkt zu erhalten. Da dies mit sehr viel Aufwand und sehr vielen Eventualitäten verbunden ist, wäre ein Modell, welches auf statistischen Werten beruht, in denen die Wahrscheinlichkeiten nicht über die Modellierung unterschiedlicher Situationen eingeschätzt wird, sondern über die Anzahl der eingesetzten Geräte und die Statistik, wie oft ein Angriff in Deutschland oder weltweit vorkommt. Daraus könnte sich die Wahrscheinlichkeit berechnen. Das Schadenspotential müsste nach wie vor eingeschätzt werden und in den Kategorien gesundheitlicher Schaden, nanzieller Schaden und Datenschutzschäden eingeteilt und de niert werden. Für diesen Ansatz könnte das BSI Modell erweitert werden, indem die Kategorien mit Werten hinterlegt werden. So würde ein generell anwendbares Modell entstehen. Für dieses Modell wären Auswertungen der Angriffsstatistiken und die Einordnung in die Kategorien erforderlich.

Literaturverzeichnis

[1] Bundesministerium für Gesundheit. „Digitalisierung im Gesundheitswesen“. (), Adresse: https://www.bundesgesundheitsministerium.de/themen/digitalisierung/digitalisierung-im-gesundheitswesen (besucht am 09. 09. 2024).

[2] Bayerischer Rundfunk. „Cyberangriff auf Wertachkliniken: Dutzende Operationen geschoben“, BR24. (4. Sep. 2024), Adresse: https://www.br.de/nachrichten/bayern/cyberangriff-auf-wertachkliniken-dutzende-operationen-geschoben,UNJhvyb (besucht am 07. 10. 2024).

[3] Bundeskriminalamt. „Lageprodukte aus dem Bereich Cybercrime - Bundeslagebild Cybercrime 2023“. (), Adresse: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2023.html?nn=28110 (besucht am 16. 09. 2024).

[4] Bitkom e.V. „203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen | Presseinformation | Bitkom e. V.“ (31. Aug. 2022), Adresse: https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022 (besucht am 16. 09. 2024).

[5] Bundesamt für Sicherheit in der Informationstechnik, „Cyber-Sicherheit als Wettbewerbsvorteil in der Digitalisierung“, Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Cyber-Sicherheit_als_Wettbewerbsvorteil.pdf?__blob=publicationFile&v=1 (besucht am 24. 10. 2024).

[6] Statista. „Internetsicherheit - Registrierte Datenlecks in den USA nach Sektor bis 2022“, Statista. (), Adresse: https://de.statista.com/statistik/daten/studie/862432/umfrage/anzahl-registrierter-datenlecks-in-den-usa-nach-sektor/ (besucht am 24. 10. 2024).

[7] „VERORDNUNG (EU) 2017/ 745 DES EUROPÄISCHEN PARLAMENTS UND DES RATES - vom 5. April 2017 - über Medizinprodukte, zur Änderung der Richtlinie 2001/ 83/ EG, der Verordnung (EG) Nr. 178/ 2002 und der Verordnung (EG) Nr. 1223/ 2009 und zur Aufhebung der Richtlinien 90/ 385/ EWG und 93/ 42/ EWG des Rates“,

[8] L. Salvatore. „Medical Device Regulation MDR: Alles, was Sie wissen müssen“, Regulatorisches Wissen für Medizinprodukte. (27. Aug. 2024), Adresse: https://www.johner-institut.de/blog/regulatory-affairs/medical-device-regulation-mdr-medizinprodukteverordnung/ (besucht am 20. 10. 2024).

[9] *Medical devices - Application of risk management to medical devices [ISO 14971:2019]*.

[10] F. Kuenzel. „Modellierung in der Wissenschaft“, ACAD WRITE. (24. März 2021), Adresse: https://www.acad-write.com/ratgeber/tipps/modellierung-in-der-wissenschaft/ (besucht am 17. 10. 2024).

[11] OWASP Foundation. „Threat modeling process“. (), Adresse: https://owasp.org/www-community/Threat_Modeling_Process (besucht am 14. 08. 2024).

[12] M. Kus und K. Sohr, „Praktische Erfahrungen und Ansätze für âSecurity by Design‘ auf Basis der STRIDE-Methodik“, *Datenschutz und Datensicherheit - DuD*, Jg. 44, Nr. 11, S. 750–754, 1. Nov. 2020, ISSN: 1862-2607. DOI: 10.1007/s11623-020-1361-6. Adresse: https://doi.org/10.1007/s11623-020-1361-6 (besucht am 03. 09. 2024).

[13] M. Rohr, „Sicherheitsuntersuchungen von Webanwendungen“, in *Sicherheit von Webanwendungen in der Praxis: Wie sich Unternehmen schützen können – Hintergründe, Maßnahmen, Prüfverfahren und Prozesse*, M. Rohr, Hrsg., Wiesbaden: Springer Fachmedien, 2018, S. 345–431, ISBN: 978-3-658-20145-6. DOI: 10.1007/978-3-658-20145-6_4. Adresse: https://doi.org/10.1007/978-3-658-20145-6_4 (besucht am 03. 09. 2024).

[14] OWASP Foundation. „OWASP-Risikobewertungsmethode“. (), Adresse: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology (besucht am 04. 09. 2024).

[15] „Overview | CVE“. (), Adresse: https://www.cve.org/About/Overview (besucht am 03. 09. 2024).

[16] CWE. „emeinsames Schwachstellenbewertungssystem (CWSS)“. (), Adresse: https://cwe.mitre.org/cwss/cwss_v1.0.1.html#2.4 (besucht am 04. 09. 2024).

[17] „BSI-Standard 200-3“, Bundesamt für Sicherheit in der Informationstechnik. (), Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.html?nn=128620 (besucht am 06. 10. 2024).

[18] J. Ennker und T. Walker, „Qualityätssicherung und Risikomanagement in der Herzchirurgie“, in *Herzchirurgie: Die Eingriffe am Herzen und den herznahen Gefäßen*, G. Ziemer und A. Haverich, Hrsg., Berlin, Heidelberg: Springer, 2010, S. 49–62, ISBN: 978-3-540-79713-5. DOI: 10.1007/978-3-540-79713-5_3. Adresse: https://doi.org/10.1007/978-3-540-79713-5_3 (besucht am 06. 08. 2024).

[19] International Electrotechnical Commission, IEC, *Gesundheitssoftware und Gesundheits-IT-Systeme Sicherheit, Effektivität und Security Teil 5-1: Security – Aktivitäten im Produktlebenszyklus*, 1. Aug. 2023.

[20] Kaspersky. „Was ist Cybersicherheit?“, /. Section: Definitionen. (17. Okt. 2020), Adresse: https://www.kaspersky.de/resource-center/definitions/what-is-cyber-security (besucht am 09. 09. 2024).

[21] „Cybersicherheitsbetrachtung vernetzter Medizinprodukte BSI-Projekt 392: Manipulation von Medizinprodukten (ManiMed)“,

[22] Statista. „Cybersicherheit - Sicherheitsvorfälle im US-Gesundheitswesen 2021“, Statista. (), Adresse: https://de.statista.com/statistik/daten/studie/1192964/umfrage/umfrage-zu-cybersicherheitsvorfaellen-im-us-gesundheitswesen/ (besucht am 24. 10. 2024).

[23] G. Schnaack, „Wirtschaftsschutz 2022“,

[24] Bundeskriminalamt. „Cybercrime“. (), Adresse: https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html (besucht am 10. 09. 2024).

[25] „DoS- und DDoS-Attacken“, Bundesamt für Sicherheit in der Informationstechnik. (), Adresse: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/DoS-Denial-of-Service/dos-denial-of-service.html?nn=132356 (besucht am 17. 10. 2024).

[26] *Man-in-the-Middle-Angriff*, in *Wikipedia*, Page Version ID: 245401251, 28. Mai 2024. Adresse: https://de.wikipedia.org/w/index.php?title=Man-in-the-Middle-Angriff&oldid=245401251 (besucht am 07. 10. 2024).

[27] *Phishing*, in *Wikipedia*, Page Version ID: 248907886, 26. Sep. 2024. Adresse: https://de.wikipedia.org/w/index.php?title=Phishing&oldid=248907886 (besucht am 16. 10. 2024).

[28] Kaspersky. „Brute-Force-Angriffe: Passwortschutz“, /. Section: Definitionen. (18. Dez. 2018), Adresse: https://www.kaspersky.de/resource-center/definitions/brute-force-attack (besucht am 24. 10. 2024).

[29] C. Rosenzweig. „Schweregrade von Schäden gemäß ISO 14971“, Regulatorisches Wissen für Medizinprodukte. (1. Okt. 2024), Adresse: https://www.johner-institut.de/blog/iso-14971-risikomanagement/schweregrad-schaden-iso-14971/ (besucht am 23. 10. 2024).

[30] „MPAMIV - Einzelnorm“. (), Adresse: https://www.gesetze-im-internet.de/mpamiv/__2.html (besucht am 22. 10. 2024).

[31] Bundesamt für Sicherheit in der Informationstechnik. „eCare Abschlussbericht“, Bundesamt für Sicherheit in der Informationstechnik. (), Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/DigitaleGesellschaft/eCare_Abschlussbericht.html?nn=132646 (besucht am 24. 09. 2024).

[32] C. Rosenzweig. „Risikoakzeptanzmatrix – Risikobewertungsmatrix“, Regulatorisches Wissen für Medizinprodukte. (18. Apr. 2023), Adresse: https://www.johner-institut.de/blog/iso-14971-risikomanagement/risikoakzeptanzmatrix-risikobewertungsmatrix/ (besucht am 22. 10. 2024).

[33] „Telematikinfrastruktur – sichere Vernetzung medizinischer Versorgung“, Bundesamt für Sicherheit in der Informationstechnik. (), Adresse: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/E-Health/Telematikinfrastruktur/telematikinfrastruktur.html?nn=127024 (besucht am 10. 09. 2024).

[34] M. Leyck Dieken, „Telematikinfrastruktur“, in *Telemedizin: Grundlagen und praktische Anwendung in stationären und ambulanten Einrichtungen*, G. Marx, R. Rossaint und N. Marx, Hrsg., Berlin, Heidelberg: Springer, 2021, S. 361–373, ISBN: 978-3-662-60611-7. DOI: 10.1007/978-3-662-60611-7_32. Adresse: https://doi.org/10.1007/978-3-662-60611-7_32 (besucht am 21. 10. 2024).

[35] „CyberPraxMed Abschlussbericht“, Bundesamt für Sicherheit in der Informationstechnik. (), Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/DigitaleGesellschaft/CyberPraxMed_Abschlussbericht.html?nn=132646 (besucht am 16. 09. 2024).

[36] AVG. „Man-in-the-middle-angriffe: Was sie sind und wie man sie verhindern kann“, Man-in-the-Middle-Angriffe: Was sie sind und wie man sie verhindern kann. (), Adresse: https://www.avg.com/de/signal/man-in-the-middle-attack (besucht am 27. 09. 2024).