Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Cyber-Sicherheitsbetrachtung vernetzter Medizinprodukte

BSI-Projekt 392: Manipulation von Medizinprodukten (ManiMed)

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
1.0	11. 12. 2020	Dr. Dina Truxius, BSI Emanuel Müller, BSI Dr. Nikolai Krupp, BSI Julian Suleder, ERNW Dr. Oliver Matula, ERNW Dennis Kniel, ERNW	Erstversion

Tabelle 1: Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: referat-di24@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

Abbildungsverzeichnis

Abkürzungsverzeichnis

Abkürzung	Definition
ACS	Allianz für Cybersicherheit
AD	Active Directory
ADT	Admit Discharge Transfer
AG	Aktiengesellschaft
API	Application Programming Interface
ARM	Avanced RISC Machines
ASLR	Address Space Layout Randomization
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
BLE	Bluetooth Low Energy
BIOS	Basic Input/Output System
BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Inneren, Bau und Heimat
BSI	Bundesministerium für Sicherheit in der Informationstechnik
BTS	Base Transceiver Station
CA	Certificate Authority
CERT	Computer Emergency Response Team
CISA	Cybersecurity and Infrastructure Security Agency
COVID	Coronavirus Disease
CS	Cyber-Sicherheitsanforderungen
CSII	Continuous Subcutaneous Insulin Infusion
CSR	Certificate Signing Request
CT	Computer Tomography
CVD	Coordinated Vulnerability Disclosure
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DDG	Deutsche Diabetes Gesellschaft
DEP	Data Execution Prevention
DICOM	Digital Imaging and Communications in Medicine
DIMDI	Deutsches Institut für Medizinische Dokumentation und Information
DMEA	Digital Medical Expertise & Applications
DNB	Deutsche Nationalbibliothek
DoS	Denial of Service

Abkürzung	Definition
DSP	Digital Signal Processing
EC	European Counsil
ECG	Electrocardiogram
EEC	European Economic Community
EEG	Electroencephalography
EG	Europäische Gemeinschaft
EMR	Electronic Medical Record
EU	European Union
EUDAMED	European Databank on Medical Devices
EWG	Europäische Wirtschaftsgemeinschaft
FDA	Food and Drug Administration
FHIR	Fast Healthcare Interoperability Resources
FIRST	Forum of Incident Response and Security Teams
FSCA	Field Safety Corrective Action
FSN	Field Safety Notice
GATT	Generic Attribute Profile
GmbH	Gesellschaft mit beschränkter Haftung
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
HDMI	High Definition Multimedia Interface
HL7	Health Level 7
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICD	Implantable Cardioverter Defibrillator
ICS	Industrial Control Systems
ICSMA	Industrial Control Systems Medical Advisories
IEC	International Electrotechnical Commission
IP	Internet Protocol
IQTIG	Institut für Qualitätssicherung und Transparenz im Gesundheitswesen
ISBN	International Standard Book Number
ISO	International Organization for Standardization
IT	Information Technology
JTAG	Joint Test Action Group

Abkürzung	Definition
KG	Kommanditgesellschaft
kHZ	Kilohertz
LDAP	Lightweight Directory Access Protocol
LFRX/LFTX	Low Frequency Receiver/Transceiver
LTS	Long-term Support
MAC	Media Access Control
MDCG	Medical Device Coordination Group
MDD	Medical Device Directive
MDR	Medical Device Regulation
MDS2	Manufacturer Disclosure Statement for Medical Device Security
MHz	Megahertz
MICS	Medical Implant Communication Service
MIPS	Millions Instructions per Second
MitM	Man in the Middle
MPG	Medizinproduktegesetz
MR	Magnetic Resonance
MRT	Magnetic Resonance Tomography
NCBI	National Center for Biotechnology Information
NEMA	National Electrical Manufacturers Association
NFC	Near Field Communication
NIH	National Institute of Health
NLM	National Library of Medicine
OS	Operating System
PAS	Patient Administration System
PCB	Printed Circuit Board
PDMS	Patient Data Management System
PGP	Pretty Good Privacy
PIN	Personal Identification Number
RDP	Remote Desktop Protocol
RFID	Radio-frequency Identification
SaMD	Software as a Medical Device
SCEP	Simple Certificate Enrollment Protocol
SD	Secure Digital
SDL	Software Development Lifecycle

Abkürzung	Definition
SDR	Software Defined Radio
SIM	Subscriber Identity Module
SMS	Short Message Service
SPI	Serial Peripheral Interface
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
SZ	Süddeutsche Zeitung
TLS	Transport Layer Security
TPM	Trusted Platform Module
UART	Universal Asynchronous Receiver Transmitter
UEFI	Unified Extensible Firmware Interface
UI	User Interface
UMDNS	Universal Medical Device Nomenclature System
URL	Uniform Resource Locator
US	United States
USA	United States of America
USB	Universal Serial Bus
USRP	Universal Software Radio Peripheral
VGA	Video Graphics Array
WHO	World Health Organization
WLAN	Wireless Local Network Area
XML	Extensible Markup Language
XSS	Cross-Site-Scripting

Tabelle 1: Abkürzungsverzeichnis

1 Einleitung

Durch die fortschreitende Digitalisierung und Vernetzung tauchen zunehmend Schwachstellen in IT-Systemen auf, die selbst vor medizinischen Geräten keinen Halt machen. IT-Sicherheitslücken, die in vernetzten medizinischen Geräten entdeckt werden, geben in der Regel Anlass zu großer Besorgnis, da ihre Ausnutzung Auswirkungen auf die Patientensicherheit oder auf ihre Umgebung, z. B. das Krankenhausnetzwerk, haben könnte. Dieses Dokument stellt die Ergebnisse des *BSI-Projekts 392: Manipulation von Medizinprodukten (ManiMed)* vor, das die IT-Sicherheit der getesteten Geräte beleuchtet. Ein Ziel dieses Projekts ist es, den aktuellen Stand der IT-Sicherheitslage für vernetzte Medizinprodukte, die kürzlich für den deutschen Markt zugelassen wurden sowie die IT-sicherheitsrelevanten Prozesse zu bewerten.

Da der Markt für vernetzte Medizinprodukte in den letzten Jahren deutlich gewachsen ist (BSI, 2018), konnten nicht alle in Deutschland vorhandenen Geräte im Rahmen dieses Projekts bewertet werden. Daher wurde eine Marktanalyse durchgeführt, um relevante Medizinprodukte für die stichprobenartige Prüfung zu identifizieren. Die Ergebnisse der Marktanalyse wurden genutzt, um insgesamt zehn Geräte aus fünf verschiedenen Kategorien (zwei Geräte pro Kategorie) auszuwählen. Die fünf Kategorien, die im Rahmen dieses Projekts untersucht wurden, sind:

- Implantierbare Herzschrittmacher und Defibrillatoren sowie deren Equipment
- Insulinpumpen
- Beatmungsgeräte
- Infusionspumpen
- Patientenmonitore.

Die ausgewählten Geräte, einschließlich der für ihren Betrieb erforderlichen Infrastrukturkomponenten, wurden anhand einer IT-Security-Untersuchung bewertet.

Die Schwachstellen, die im Rahmen der Tests identifiziert wurden, konnten koordiniert veröffentlicht werden. Das Projektteam arbeitete stets eng mit den Herstellern zusammen, um eine rechtzeitige Behebung der Schwachstellen zu gewährleisten. Als Ergebnis dieser Prüfungen wurden über alle Produkte hinweg insgesamt über 150 Schwachstellen im Rahmen des Projekts ManiMed identifiziert. Neben dem aktuellen IT-Sicherheitsstatus ausgewählter medizinischer Geräte zeigt das Projekt ManiMed Strategien auf, wie nachfolgende Behebungs- und Veröffentlichungsprozesse gehandhabt und koordiniert werden können. Die Ergebnisse dienen darüber hinaus dazu, eine kritische Überprüfung der internen Prozesse, des Reifegrades der IT-Sicherheit und zukünftiger Entscheidungen ermöglichen. Das übergeordnete Ziel des Projekts ist es, die IT-Sicherheit bei medizinischen Geräten auf einem hohen Niveau zu halten und zur ständigen Verbesserung zu ermutigen.

1.1 Motivation

Die digitale Vernetzung ist bereits heute in vielen Lebensbereichen nicht mehr wegzudenken. Im Gesundheitswesen ist ein deutlicher Trend in Richtung vernetzter Medizintechnik zu beobachten, sodass die Zahl der angeschlossenen Hightech-Geräte, z. B. in Krankenhäusern, Arztpraxen und medizinischen Versorgungszentren, stetig zunimmt (BSI, 2018). Dazu gehören Infusionspumpen, Implantate und medizinische Großgeräte, wie Computertomographie- und Magnetresonanztomographiesysteme. Abgesehen vom üblichen Ausfall-Risiko der Geräte, aufgrund der extensiven Nutzung über eine längere Lebensdauer hinweg, birgt ihre Interkonnektivität neue Risiken, die bisher nicht vorhanden waren. Wenn die Soft- oder Hardware eines Geräts oder die dazugehörige Infrastruktur Mängel aufweist, könnten böswillige Akteure diese Schwachstellen ausnutzen und dadurch die Sicherheit des Patienten gefährden.

Selbst wenn eine Schwachstelle die Sicherheit eines Patienten nicht direkt betrifft, kann es trotzdem möglich sein, dass sensible Patientendaten abgegriffen werden können.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) strebt als zentrale IT-Sicherheitsbehörde in Deutschland an, Hersteller und die Öffentlichkeit für IT-Sicherheitsrisiken vernetzter medizinischer Geräte sensibilisieren. Als Reaktion auf die bisherigen Sicherheitsmeldungen von vernetzten Medizinprodukten (BSI, 2018), (BSI, 2019), (Suleder, Dewald, & Grunow) hat das BSI das Projekt *Manipulation von Medizinprodukten (ManiMed*) initiiert. In diesem Projekt wird eine IT-Sicherheitsanalyse ausgewählter Produkte durch Sicherheitsprüfungen durchgeführt, um Einblicke in die IT-Sicherheitslage vernetzter Medizinprodukte auf dem deutschen Markt zu gewinnen. Die Veröffentlichungsprozesse wurden mit elf Herstellern koordiniert, um das Bewusstsein für die Bedeutung von Prozessen zur Verbesserung der allgemeinen IT-Sicherheit in medizinischen Geräten zu schärfen.

1.1.1 Die Lage der IT-Sicherheit in Deutschland

In den letzten drei Fassungen des vom Bundesamt für Sicherheit in der Informationstechnik veröffentlichten Dokuments *Der Stand der IT-Sicherheit in Deutschland* (BSI, 2020; BSI, 2019; BSI, 2018) wird festgestellt, dass es einen klaren Trend gibt, Ärzten, medizinischem Personal oder Patienten selbst den Zugriff auf Daten medizinischer Geräte über mobile Anwendungen zu ermöglichen. In Einzelfällen kann die mobile Anwendung sogar zur Steuerung des Medizinprodukts genutzt werden.

Die gesammelten Daten könnten an ein Cloud-Backend übertragen werden, wo sie entweder weiterverarbeitet oder Ärzten oder medizinischem Personal zur Verfügung gestellt werden können, die für die Analyse dieser Daten nicht mehr persönlich anwesend sein müssen.

Da jedes Jahr stetig mehr dieser intelligenten medizinischen Geräte in Verkehr gebracht werden, ist es wahrscheinlich, dass auch Angriffe mit Auswirkungen auf die Privatsphäre und Sicherheit zunehmen. Wie im Bericht 2018 festgestellt wird, sind solche Angriffe aufgrund fehlender oder schwacher Authentifizierungsmechanismen und schwacher oder fehlender Verschlüsselung bei der Kommunikation und Speicherung von Daten möglich. Im Lagebericht von 2020 werden detailliertere Informationen über die IT-Sicherheit medizinischer Geräte und aktuelle Angriffsszenarien beleuchtet.

1.1.2 BfArM – Vigilanz und Vorkommnismeldungen

Das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) veröffentlicht Informationen über Risiken, die von Medizinprodukten ausgehen. Abbildung 1 zeigt die Anzahl der jährlichen Risikomeldungen im Zeitraum von 2008 bis 2017.

Wie in Abbildung 1 ersichtlich, hat die Zahl der Risikomeldungen von 2008 bis 2017 deutlich zugenommen. Die überwiegende Zahl an Meldungen macht auf mechanische Fehler, elektrische Fehler und andere Arten von Fehlern oder Fehlfunktionen (BfArM, 2017) aufmerksam. IT-Sicherheitsvorfälle werden in keiner eigenen Kategorie geführt. Sie werden daher nur dann in die Statistik aufgenommen, wenn sie potenzielle Auswirkungen auf die Patientensicherheit (engl.: Safety) haben.

Das Bundesinstitut für Arzneimittel und Medizinprodukte veröffentlicht auf seiner Website (BfArM) eine Liste von Vorkommnismeldungen mit Bezug zur IT-Sicherheit. Zum Zeitpunkt der Erstellung dieses Berichts waren 21 solcher Vorkommnismeldungen auf dieser Website veröffentlicht. Verglichen mit der Zahl der Risikomeldungen insgesamt, ist diese Zahl relativ gering.

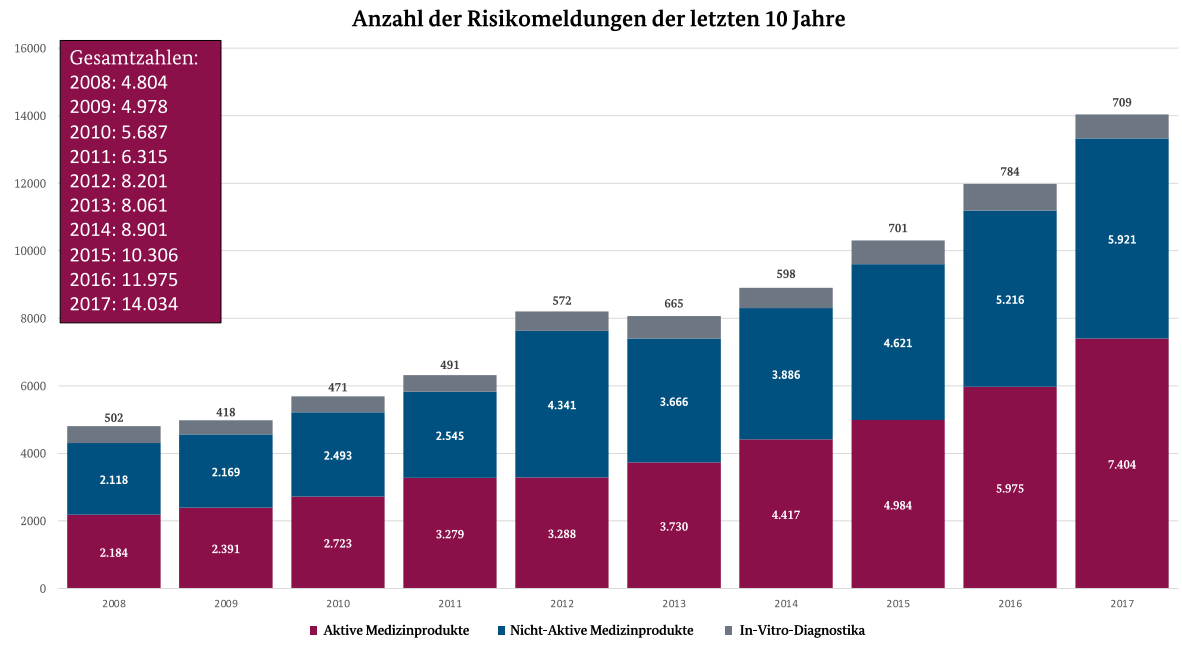

Abbildung 1: Anzahl der Vorkommnismeldungen pro Jahr entnommen aus (BfArM, 2018)

Die gegenwärtige Arbeit soll das Bewusstsein, dass IT-Sicherheitsfragen bei der Erörterung potenzieller Risiken, die von medizinischen Geräten ausgehen, berücksichtigt werden müssen, schärfen. Daher wird in diesem Bericht versucht zu beurteilen, ob Fragen der IT-Sicherheit bei der Beschreibung potenzieller Risiken, die von Medizinprodukten ausgehen, gesondert untersucht werden sollten.

1.2 Verwandte Arbeiten

In der Vergangenheit gab es bereits mehrere Veröffentlichungen zur IT-Sicherheit medizinischer Geräte. So wurde beispielsweise im Vortrag *Understanding and Exploiting Implanted Medical Devices* (Black Hat USA, 2018) über kritische Schwachstellen in implantierbaren medizinischen Geräten berichtet (Rios & Butts, 2018).

Das ERNW White Paper 66 fasst den Stand der IT-Sicherheit medizinischer Geräte, auf der Grundlage öffentlich zugänglicher Informationen, zusammen (Suleder, Dewald, & Grunow). Darüber hinaus zeigte die von ERNW durchgeführte Forschung an Patientenmonitoren, Spritzenpumpen, Elektroenzephalographiesystemen, Heimüberwachungsgeräten und einem Magnetresonanztomographiesystem, dass die analysierten Geräte von mehreren Schwachstellen betroffen waren (SZ, 2015) (Grunow, 2015).

Wie bereits erwähnt, veröffentlicht das Bundesinstitut für Arzneimittel und Medizinprodukte in Deutschland (BfArM) eine Liste von Meldungen zu Fragen der IT-Sicherheit. Auf internationaler Ebene wird eine Liste von Cybersecurity Safety Communications von der U.S. Food & Drug Administration zur Verfügung gestellt (FDA, 2020). Die Cybersecurity and Infrastructure Security Agency (CISA, USA) veröffentlicht regelmäßig ICSMA (ICS Medical Advisories) zur Kommunikation von Schwachstellen in Medizinprodukten.

Zurzeit gibt es keine systematische Studie zur Bewertung des Ausmaßes, in dem Schwachstellen in medizinischen Geräten auftreten. Daher sind nur wenige Daten über die Wirksamkeit von Regulierungsmaßnahmen zur Verhinderung solcher Schwachstellen verfügbar.

ManiMed ist das erste Projekt, das den allgemeinen IT-Sicherheitszustand vernetzter medizinischer Geräte betrachtet. Die IT-Sicherheitslage wird auf Grundlage von IT-Sicherheitsprüfungen ausgewählter

vernetzter Medizinprodukte bewertet. Die Ergebnisse des öffentlich geförderten Projekts ManiMed sollen als Informationsgrundlage für die Öffentlichkeit und für zukünftige regulatorische Vorgaben dienen.

1.3 Zielgruppe dieses Dokuments

Zum einen soll das Dokument die Öffentlichkeit mit den Projektergebnissen vertraut machen. Um das Verständnis zu erleichtern haben die Autoren in Abschnitt 2 die diesem Dokument zugrundeliegende Terminologie angegeben. Um ein besseres Verständnis für die bei den IT-Sicherheitsprüfungen verwendeten Methodik zu ermöglichen, enthält Abschnitt 7 eine genauere Beschreibung der Vorgehensweisen.

Zum anderen soll das Dokument Betreibern medizinischer Einrichtungen (einschließlich des medizinischen Personals) Informationen zur Verfügung stellen, um einen Überblick über die IT-Sicherheitslage vernetzter Medizinprodukte auf dem deutschen Markt zu erhalten. Es soll die Betreiber dabei unterstützen, zu verstehen, welche zusätzlichen Risiken durch die Integration vernetzter medizinischer Geräte in ihre Infrastruktur entstehen können. Es ist jedoch zu beachten, dass dies nicht bedeutet, dass die vernetzten Produkte im Allgemeinen das Gesamtrisiko hinsichtlich der Patientensicherheit erhöhen. Im Vergleich zu nicht vernetzten Geräten gibt es oft mehrere Vorteile, wie z. B. eine schnellere Reaktion im Notfall (wenn medizinische Daten eines Patienten zur Überwachung solcher Ereignisse verwendet werden). Dennoch können vernetzte Medizinprodukte zusätzliche Risiken mit sich bringen, derer sich die Betreiber medizinischer Einrichtungen bewusst sein sollten.

Des Weiteren soll das Dokument Hersteller von Medizinprodukten adressieren, um sie a) auf Arten von Schwachstellen aufmerksam zu machen, die in vernetzten Medizinprodukten auftreten können, und b) sie bei der Verringerung oder Beseitigung von Schwachstellen in ihren Geräten zu unterstützen, indem technische und prozessbezogene Maßnahmen aufgezeigt werden.

Viertens wendet sich das Dokument auch an Entscheidungsträger, die entsprechende Vorschriften oder sogar Regularien für Medizinprodukte beschließen. Die Ergebnisse dieses Dokuments sollen Impulse geben und ihnen ermöglichen, die IT-Sicherheit in Zukunft im Zusammenhang mit Vorschriften für Medizinprodukte zu bewerten. Es ist zu beachten, dass sich die Regulierungslandschaft in der Europäischen Union und damit auch in Deutschland mit der Verbindlichkeit der Medizinprodukteverordnung (siehe Abschnitt 2.2) deutlich verändern wird. Die Ergebnisse dieser Arbeit wurden jedoch im Rahmen der derzeitigen regulatorischen Situation für Medizinprodukte in Deutschland erzielt und gleichzeitig können diese Ergebnisse keinen Hinweis auf die IT-Sicherheitslage von Medizinprodukten geben, die nach der Medizinprodukteverordnung Zugang zum deutschen Markt erhalten.

1.4 Danksagung

Die Autoren möchten diesen Absatz nutzen, um allen Herstellern und beteiligten Parteien, die an diesem Projekt mitgewirkt haben, ihren Dank auszusprechen. Alle Teilnehmer zeigten großes Interesse an einer unabhängigen Prüfung, welche die Absicht hat die Sicherheit ihrer Produkte zu verbessern.

Durch ihre Teilnahme an diesem Projekt zeigten die Hersteller, dass ihnen die Sicherheit ihrer Produkte ein großes Anliegen ist und dass sie sich bemühen, ihre Produkte auf transparente Weise zu verbessern.

Darüber hinaus möchten sich die Autoren auch bei den medizinischen Einrichtungen bedanken, die sich die Zeit genommen haben, die Anfragen zu beantworten und Informationen über ihre Ausstattung zur Verfügung zu stellen. Die Informationen waren hilfreich, um Geräte zu identifizieren, die im Rahmen dieses Projekts analysiert werden sollten, da sie bereits eingesetzt werden.

Die Autoren möchten allen beteiligten nationalen und internationalen Behörden danken, insbesondere dem BfArM und der CISA.

Abschließend möchten die Autoren auch allen anderen beteiligten Parteien danken, die hier nicht explizit aufgeführt wurden.

1.5 Projektpartner

Dieser Abschnitt stellt die an der Durchführung des Projekts beteiligten Parteien vor: die ERNW Research GmbH, die ERNW Enno Rey Netzwerke GmbH und das Bundesamt für Sicherheit in der Informationstechnik.

1.5.1 ERNW Research GmbH & ERNW Enno Rey Netzwerke GmbH

ERNW Research GmbH ist ein unabhängiger IT-Sicherheits-Dienstleister mit Sitz in Heidelberg, Deutschland. Seit ihrer Gründung im Jahr 2015 liegt der Schwerpunkt der ERNW Research GmbH auf der Durchführung von Forschungsprojekten in allen Bereichen der IT-Sicherheit - öffentlich geförderte Projekte in Kooperation mit Hochschulen, Kundenprojekte und interne Forschungsprojekte.

Die ERNW Enno Rey Netzwerke GmbH ist ein herstellerunabhängiger Beratungs- und Sicherheitsprüfungsdienstleister mit dem Schwerpunkt Netzwerk- und Anwendungssicherheit. Das Unternehmen wurde 2001 gegründet. Viele der Mitarbeiter verfügen über mehr als zehn Jahre Erfahrung in Design, Implementierung, Betrieb und Sicherung umfangreicher Unternehmensnetzwerke.

Die Mitarbeiter beider Unternehmen, der ERNW Research GmbH und der ERNW Enno Rey Netzwerke GmbH, tauschen ihr Wissen regelmäßig auf internationalen Sicherheitskonferenzen aus (z. B. seit 2006 regelmäßig auf der Black Hat) und haben eine Vielzahl von Büchern, Fachartikeln und White Papers veröffentlicht. In enger Zusammenarbeit mit verschiedenen Universitäten entstehen jedes Jahr zahlreiche Abschlussarbeiten zu aktuellen Themen der Informationssicherheit.

Das Leitbild beider Unternehmen lautet: "Make the World a Safer Place!“ Diese mutige, aber einfache Botschaft ist der moralische Kompass, der die Unternehmen leitet. Diese Aussage gilt für die Methodik und die Forschung darüber, wie ERNW seine Mitarbeiter entwickelt, seinen Kunden seine Integrität vermittelt und wie es sich innerhalb der lokalen und globalen Gemeinschaft verhält. Besondere Aufmerksamkeit gilt den Bereichen Incident Response, Forensic Computing, Malware-Analyse und Sicherheit medizinischer Geräte sowie fortgeschrittenen Sicherheitsprüfungen.

Kontakt:

ManiMed Projekt-Team
manimed@ernw.de
ERNW Research GmbH
Carl-Bosch-Str. 4
69115 Heidelberg
Deutschland
https://www.ernw-research.de/

1.5.2 Bundesamt für Sicherheit in der Informationstechnik (BSI)

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde 1991 per Gesetz gegründet und hat seinen Sitz in Bonn. Das BSI steht unter der Aufsicht des Bundesministeriums des Inneren, für Bau und Heimat (BMI) und hat acht Abteilungen, eine zentrale und sieben Fachabteilungen. Jede Abteilung besteht aus ein bis drei Fachbereichen, die wiederum aus mehreren Referaten bestehen. In seiner Rolle als Bundesbehörde für Informationssicherheit gestaltet das BSI die Informationssicherheit in der

Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. Das übergeordnete Ziel ist die Förderung der IT-Sicherheit in Deutschland. Seit seiner Gründung hat das BSI seine Ressourcen und Kompetenzbereiche kontinuierlich ausgebaut.

Je mehr Menschen von der Informationstechnologie abhängig werden, desto relevanter wird das Thema IT-Sicherheit. Die Bedrohung unserer Gesellschaft durch Angriffe auf IT-Systeme, die Computerausfälle, -missbrauch oder -sabotage zur Folge haben können, ist größer denn je. Aufgrund dieser Komplexität ist das Aufgabenspektrum des BSI sehr breit gefächert. Dennoch ist das BSI in erster Linie der zentrale IT-Sicherheitsdienstleister für die Bundesregierung in Deutschland. Es werden jedoch sowohl Dienstleistungen für IT-Hersteller, als auch für private und gewerbliche Nutzer und Anbieter von Informationstechnik angeboten, denn wirksame Sicherheit ist nur möglich, wenn alle Beteiligten ihren Beitrag leisten. Deshalb will das BSI auf dem Gebiet der IT-Sicherheit noch enger mit allen Akteuren der IT- und Internetwirtschaft zusammenarbeiten.

Das BSI untersucht Sicherheitsrisiken von IT-Systemen, definiert den Stand der Technik, veröffentlicht Informationen über Risiken und Bedrohungen (BSI, 2020) und sucht nach geeigneten Lösungen zur Verbesserung der IT-Sicherheitslage in Deutschland. Alle IT-Systeme, auch technisch sichere Informations- und Telekommunikationssysteme, weisen zu jedem Zeitpunkt potenziell ausnutzbare Schwachstellen auf. Folglich müssen alle erdenklichen Risiken und Folgeschäden berücksichtigt werden. Um diese Risiken zu vermindern oder gar zu vermeiden, richten sich die Dienstleistungen des BSI an verschiedene Zielgruppen: Das BSI berät Hersteller, Vertreiber und Anwender von Informationstechnologie und analysiert aktuelle Trends im Bereich der Informationstechnologie.

Kontakt:

ManiMed Projekt-Team
referat-di24@bsi.bund.de
Bundesamt für Sicherheit in der Informationstechnik
Cyber-Sicherheit im Gesundheits- und Finanzwesen
Godesberger Allee 185-189
53175 Bonn
Deutschland
www.bsi.bund.de

1.6 Über dieses Dokument

Das folgende Dokument wurde vom BSI sowie Sicherheitsforschern, auf der Grundlage von Erfahrungen aus IT-Sicherheitsprojekten, z. B. Penetrationstests, Konzept Reviews, Audits von Systemumgebungen und Entwicklung von Sicherheitskonzepten, verfasst. Weder die ERNW Research GmbH, noch die ERNW Enno Rey Netzwerke GmbH, sind Hersteller von digitalen Gesundheitsanwendungen, Medizinprodukten oder Auditoren einer Benannten Stelle oder anderer Zertifizierungsstellen, Anwender oder Betreiber von Medizinprodukten oder haben ähnliche Rollen, die eine andere Sicht auf die Produkte haben könnte. Neben einschlägigem Expertenwissen zur Identifizierung von Sicherheitslücken in medizinischen Geräten, Systemen und Betriebsumgebungen sowie zum ethischen Umgang mit Schwachstellen in koordinierten Veröffentlichungsprozessen, verfügen die Autoren über Grundkenntnisse über die Zulassung von Medizinprodukten und die geltenden gesetzlichen Anforderungen.

2 Terminologie

In diesem Abschnitt werden die in diesem Dokument verwendeten Grundbegriffe vorgestellt. Dazu gehören z. B. allgemeine medizinische Begriffe sowie Fachbegriffe, die zur Beschreibung von IT-Sicherheitsfragestellungen verwendet werden. Darüber hinaus werden die Zuständigkeiten der Stellen erörtert, die an der Veröffentlichung von Informationen über Medizinprodukte, der Zulassung von Medizinprodukten für den deutschen Markt und der Beantwortung von Sicherheitsfragen bei Medizinprodukten beteiligt sind oder diese verantworten.

2.1 Medizinprodukte

Ein Medizinprodukt ist nach Artikel 2 (1) der Medizinprodukteverordnung (MDR) folgendermaßen definiert (European Parliament and the Council of the European Union, 2017):

„Medizinprodukt" bezeichnet ein Instrument, einen Apparat, ein Gerät, eine Software, ein Implantat, ein Reagenz, ein Material oder einen anderen Gegenstand, das dem Hersteller zufolge für Menschen bestimmt ist und allein oder in Kombination einen oder mehrere der folgenden spezifischen medizinischen Zwecke erfüllen soll:

— Diagnose, Verhütung, Überwachung, Vorhersage, Prognose, Behandlung oder Linderung von Krankheiten,

— Diagnose, Überwachung, Behandlung, Linderung von oder Kompensierung von Verletzungen oder Behinderungen,

— Untersuchung, Ersatz oder Veränderung der Anatomie oder eines physiologischen oder pathologischen Vorgangs oder Zustands,

— Gewinnung von Informationen durch die In-vitro-Untersuchung von aus dem menschlichen Körper — auch aus Organ-, Blut- und Gewebespenden — stammenden Proben und dessen bestimmungsgemäße Hauptwirkung im oder am menschlichen Körper weder durch pharmakologische oder immunologische Mittel noch metabolisch erreicht wird, dessen Wirkungsweise aber durch solche Mittel unterstützt werden kann.

Die folgenden Produkte gelten ebenfalls als Medizinprodukte:

— Produkte zur Empfängnisverhütung oder -förderung,

— Produkte, die speziell für die Reinigung, Desinfektion oder Sterilisation der in Artikel 1 Absatz 4 genannten Produkte und der in Absatz 1 dieses Spiegelstrichs genannten Produkte bestimmt sind.

2.2 Gesetzliche Grundlage und Verordnungen und Regelungen für den Marktzugang von Medizinprodukten in Deutschland

Medizinprodukte erhalten in Deutschland nur dann eine Marktzulassung, wenn sie eine CE-Kennzeichnung besitzen. Die CE-Kennzeichnung ist eine Erklärung des Herstellers, dass das Produkt den gesetzlichen Anforderungen entspricht. In einem so genannten Konformitätsbewertungsverfahren wird geprüft und bestätigt, ob die rechtlichen Anforderungen beachtet wurden.

Die Anforderungen sind in Anhang I der Richtlinie 90/385/EWG über aktive implantierbare medizinische Geräte (European Parliament and the Council of the European Union, 1990), der Richtlinie 98/79/EG über In-vitro-Diagnostika (European Parliament and the Council of the European Union, 1998) und der Richtlinie 93/42/EWG über andere medizinische Geräte (European Parliament and the Council of the European Union, 1993) festgelegt.

Wie die Konformitätsbewertung durchzuführen ist, hängt von dem mit einem Medizinprodukt verbundenen potenziellen Risiko ab. Basierend auf der Risikobewertung, die in der entsprechenden Richtlinie festgelegt ist, werden die Geräte in Produktklassen eingeteilt (mit Ausnahme von aktiven implantierbaren Geräten, die nicht weiter nach Risikokriterien aufgeschlüsselt werden). Diese Produktklassen bestimmen den Konformitätsbewertungsprozess und ob eine so genannte *Benannte Stelle* in diesen Prozess einbezogen werden muss.

Die Richtlinie 93/42/EWG des Rates für andere medizinische Geräte legt in ihrem Anhang IX vier Kategorien fest: I, IIa, IIb und III.

Da die oben genannten Richtlinien in nationales Recht übersetzt werden müssen, wird dies für Deutschland durch das Gesetz über Medizinprodukte (Bundesgesetzblatt, 1994) realisiert.

Die vorgelegten Richtlinien des Rates werden durch die Medizinprodukteverordnung ersetzt (siehe Abschnitt 2.3).

2.3 Verordnung über Medizinprodukte (MDR)

Die Verordnung über Medizinprodukte (Medical Device Regulation, MDR) regelt die wichtigsten Formalitäten für Medizinprodukte innerhalb der Europäischen Union (European Parliament and the Council of the European Union, 2017). Sie trat am 25. Mai 2017 in Kraft und wird am 26. Mai 2021 obligatorisch (das Datum wurde aufgrund der COVID-19-Pandemie um ein Jahr verschoben). Die MDR ersetzt unter anderem die Richtlinie über Medizinprodukte (MDD; Richtlinie 93/42/EWG), die in Deutschland durch das Medizinproduktegesetz (MPG) umgesetzt wird.

2.4 Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM)

Das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) ist die zuständige Aufsichtsbehörde für Arzneimittel und Medizinprodukte in Deutschland. Es untersteht der Aufsicht des Bundesministeriums für Gesundheit (BMG). Die Hauptaufgaben des BfArM im Bereich der Medizinprodukte sind (BfArM):

- Zentrale Erfassung, Bewertung und Beurteilung auftretender Risiken bei der Anwendung von Medizinprodukten und Koordination der zu ergreifenden Maßnahmen
- Spezielle Zulassung von Medizinprodukten
- Beratung von zuständigen Behörden, Benannten Stellen und Herstellern in Fragen der Klassifizierung von Medizinprodukten und deren Abgrenzung zu anderen Produkten sowie deren Entscheidung
- Beratung der zuständigen Behörden und Benannten Stellen zu technischen und medizinischen Anforderungen und zu Fragen der Sicherheit von Medizinprodukten
- Mitarbeit in nationalstaatlichen/föderalstaatlichen Ausschüssen, Arbeitsgruppen der Europäischen Kommission sowie in nationalen, europäischen und internationalen Normungsausschüssen
- Durchführung des Konsultationsverfahrens für Medizinprodukte mit pharmazeutischen Teilen auf Anfrage der Benannten Stellen
- Auswertung und Bewertung von klinischen Versuchen mit Medizinprodukten und Leistungsbewertungstests der In-vitro-Diagnostik

2.5 Deutsches Institut für Medizinische Dokumentation und Information (DIMDI)

Das Deutsche Institut für Medizinische Dokumentation und Information (DIMDI) war eine staatliche Einrichtung in Deutschland. Der Aufgabenbereich wurde am 26. Mai 2020 dem BfArM übertragen.

Eine seiner Hauptaufgaben ist der Betrieb der durch das Medizinproduktegesetz vorgeschriebenen Datenbank für Medizinprodukte. Mit seiner Abfragefunktionalität wurde das Informationssystem im Rahmen der Marktanalyse zur Identifizierung von Medizinprodukten, die die in Abschnitt 3 genannten Anforderungen erfüllen, genutzt (siehe Abschnitt 3.1.1). Weitere Informationen zum System sind auf der Website des Bundesinstituts für Arzneimittel und Medizinprodukte (BfArM) zu finden.

2.6 European Databank on Medical Devices (EUDAMED)

Die Europäische Datenbank für Medizinprodukte (EUDAMED) soll es den Behörden ermöglichen, schnell auf relevante Daten von Medizinprodukteherstellern und Geräten zuzugreifen, um die Überwachung des europäischen Marktes für Medizinprodukte zu verbessern.

Die MDR sieht vor, dass sich die Hersteller oder entsprechenden Vertreiber von Medizinprodukten in EUDAMED registrieren lassen und vor dem Vertrieb von Medizinprodukten auf dem europäischen Markt Informationen über sich selbst bereitstellen müssen. Darüber hinaus muss der Hersteller, bevor ein Medizinprodukt für den europäischen Markt zugelassen werden kann, bestimmte Informationen über das Gerät bereitstellen und in die Datenbank einpflegen.

Es sei darauf hingewiesen, dass zum Zeitpunkt der Erstellung dieses Artikels die Entwicklung der Datenbank und ihrer Schnittstellen noch nicht abgeschlossen ist.

2.7 Betriebsarten von Medizinprodukten

Das Bundesamt für Sicherheit in der Informationstechnik hat eine Cyber-Sicherheitsempfehlung für Hersteller von netzwerkfähigen Medizinprodukten veröffentlicht (BSI, 2018).

Das Dokument wurde mit den nachfolgend erläuterten Absichten veröffentlicht. Erstens soll es als begleitender Leitfaden für die Umsetzung der regulatorischen Anforderungen dienen. Zweitens soll es die Entwicklung und Wartung von Medizinprodukten mit dem Schwerpunkt IT-Sicherheit unterstützen. Drittens soll es helfen IT-Sicherheitsfragen aus Risikoanalysen, die im Rahmen der Konformitätsbewertung durchgeführt werden, zu reduzieren.

Das Dokument unterscheidet zwischen mehreren Betriebsarten, die von den meisten Geräten unterstützt werden:

- Medizinischer Betriebsmodus: Verwendung für den vorgesehenen medizinischen Zweck
- Gerätekonfigurationsmodus: Das Gerät wird für seinen medizinischen Zweck konfiguriert (einschließlich patientenspezifischer Parameter).
- Technischer Servicebetriebsmodus: Installation von Updates des Herstellers oder von Drittanbietern sowie Kalibrierung oder grundlegende Einstellungen des Geräts.

Wie im Dokument angegeben, können sich die verschiedenen Modi gegenseitig beeinflussen. Wenn z. B. während des technischen Servicebetriebs Malware installiert wird, kann dies auch den medizinischen Betrieb beeinflussen. Dennoch ist die Unterscheidung zwischen diesen verschiedenen Modi wesentlich, um das mit einer bestimmten Schwachstelle verbundene Patientenrisiko zu bewerten. Wenn eine Schwachstelle nur während des technischen Wartungsmodus auftreten kann, müsste ein Angreifer zunächst einen Mechanismus identifizieren, um das Gerät in diesen Modus zu versetzen.

2.8 Das Common Vulnerability Scoring System (CVSS)

Das Common Vulnerability Scoring System (CVSS) ist ein Rahmenwerk zur Bewertung der Kritikalität einzelner Schwachstellen. Es wurde vom Forum of Incident Response and Security Teams entwickelt (FIRST, 2019).

2.8.1 Grundlagen des CVSS

Das CVSS definiert eine Metrik zur Berechnung von drei verschiedenen Scores, die jeweils eine eigene Aussage haben. Die Scores werden als *Base Metrics (Basis-Metrik)*, *Temporal Metrics (zeitliche Metrik),* und *Environmental Metrics (Umgebungs-Metrik)* bezeichnet. Die Basis-Metriken bestimmen den allgemeinen Schweregrad der Schwachstelle und ändern sich nach ihrer Zuweisung nicht mehr. Die zeitlichen Metriken beschreiben, wie komplex und zeitaufwändig es für einen Angreifer ist, die Schwachstelle auszunutzen. Die zeitlichen Metriken können sich im Laufe der Zeit ändern. Dies kann z. B. passieren, wenn der Exploit-Code für eine Schwachstelle öffentlich zugänglich gemacht wird. Die dritte Metrik beschreibt die Auswirkungen der Schwachstelle in einer bestimmten Einsatzumgebung und kann sich daher für verschiedene Umgebungen ändern. Die drei Metriken werden kombiniert, um eine CVSS-Bewertung zu erhalten. Dieser CVSS-Score spiegelt den Schweregrad einer Schwachstelle zu einem bestimmten Zeitpunkt in einer bestimmten Umgebung wider.

Weitere Informationen über die Berechnung des CVSS-Scores sind in den öffentlich zugänglichen Dokumenten (FIRST, 2019) zu finden.

Es wird darauf hingewiesen, dass das CVSS-Score-System entwickelt wurde, um den Schweregrad von Schwachstellen für Informationssysteme in Unternehmen zu bewerten. Daher spiegelt es den Schweregrad der Schwachstellen medizinischer Geräte nicht angemessen wider, da die Auswirkungen einer Schwachstelle auf die Patientensicherheit nicht ausreichend in das Ratingsystem integriert sind. Aus diesem Grund hat die MITRE Corporation im Auftrag der FDA Anstrengungen unternommen, um das CVSS-Bewertungssystem für medizinische Geräte anzupassen (Chase & Coley, 2019). Diese Anpassung ändert nicht die Berechnung des CVSS-Scores, sondern führt einen Fragebogen ein, auf dessen Grundlage einzelne Parameter der Metriken bestimmt werden sollen. Es ist jedoch zu beachten, dass dieses Dokument zum Zeitpunkt der Erstellung als Entwurf eingestuft ist.

2.8.2 Verwendung des CVSS-Bewertungssystems

Im Rahmen des Projekts wurde das CVSS-Bewertungssystem (Version 3) zur Bewertung aller identifizierten Schwachstellen verwendet. Diese wurden dann während des CVD-Prozesses (Coordinate Vulnerability Disclosure) jedem entsprechenden Hersteller mitgeteilt. Das CVSS-Bewertungssystem ist jedoch aus den folgenden Gründen nicht in diesem Dokument enthalten:

- Da der Veröffentlichungsprozess zum Zeitpunkt der Abfassung dieses Dokuments noch nicht abgeschlossen ist, sind mehrere Security Advisories mit CVSS-Bewertungen noch nicht veröffentlicht worden. Es muss berücksichtigt werden, dass die Schwachstellen während dieses Prozesses mit den Herstellern diskutiert werden und möglicherweise zusätzliche Informationen zur Verfügung gestellt werden, die sich auf die Bewertung mittels CVSS auswirken. Wenn eine CVSS-Bewertung in dieses Dokument aufgenommen würde, könnte sie daher von der endgültigen Bewertung abweichen, die zusammen mit der Sicherheitsberatung vorgelegt wurde. Da dieses Dokument keine widersprüchlichen Informationen zu diesen Security Advisories enthalten sollte, werden hier keine CVSS-Bewertungen angegeben.
- Das CVSS-Bewertungssystem verwendet einen *quantitativen* Ansatz, um den Schweregrad einer Schwachstelle zu bestimmen. Den Parametern der verschiedenen CVSS-Metriken werden Werte

zugewiesen, um eine CVSS-Gesamtbewertung zu erhalten. Dies ermöglicht einen einfachen Vergleich des Schweregrads verschiedener Schwachstellen, ist aber in der Regel schwieriger zu verstehen als ein *qualitativer* Ansatz, bei dem beschreibende Begriffe verwendet werden, um den Schweregrad der Schwachstelle zu definieren.

2.9 Sicherheit: Security vs. Safety

Die deutsche Sprache verwendet das gleiche Wort *Sicherheit* als Übersetzung für die englischen Begriffe *Security* und *Safety*. Diese Begriffe haben unterschiedliche Bedeutungen, die nicht mit dem Wort "Sicherheit" alleinig angemessen beschrieben werden können (so, dass andere Wörter verwendet werden müssen, um den genauen Kontext zu beschreiben). Daher werden die Begriffe *Security* und *Safety*, wie sie in diesem Dokument verwendet werden, erklärt und ihre Unterschiede hervorgehoben.

Der Begriff *Security* bezeichnet den Schutz einer Entität vor äußeren Bedrohungen. Wenn also eine gewisse Schwachstelle für eine Entität besteht (z. B. ein medizinisches Gerät im Kontext dieses Dokuments), verringert dies die Sicherheit des Geräts, da es nicht gegen die Bedrohungen geschützt ist, die durch die Ausnutzung der Schwachstelle ermöglicht würden. Es sei an dieser Stelle angemerkt, dass es, abgesehen von sehr einfachen Systemen, unmöglich ist, die Sicherheit eines Geräts nachzuweisen, d. h. es gibt keine Methode oder keinen Algorithmus, um zu bestimmen, ob eine Entität gegen alle externen Bedrohungen geschützt ist. Im Gegensatz dazu kann durch die Identifizierung nur einer einzigen Schwachstelle für eine Entität nachgewiesen werden, dass das Gerät nicht sicher ist (gegen die Bedrohungen, die die Ausnutzung der Schwachstelle ermöglicht).

Dennoch kann manchmal die Aussage getroffen werden, dass ein Gerät sicher ist oder dass es ein hohes Sicherheitsniveau aufweist. Dies bedeutet nicht, dass das Gerät im Allgemeinen sicher ist, sondern dass die Zeit und der Aufwand, die verwendet wurden, um eine Komponente mit Hilfe einer bestimmten Beurteilungsmethode auf Schwachstellen zu analysieren, zu keinem aussagekräftigen Ergebnis geführt hat. Wenn also mehr Zeit darauf verwendet wird, eine Komponente oder ein System auf Schwachstellen zu analysieren, wird es wahrscheinlicher, dass Schwachstellen gefunden werden. Um die Ergebnisse einer IT-Sicherheitsprüfung zu beurteilen, ist es daher wichtig zu erkennen, wie viel Zeit für diese Beurteilung aufgewendet wurde.

Oft wird die Abkürzung IT (Informationstechnologie) oder der Begriff *Cyber* dem Begriff Sicherheit vorangestellt, d. h. IT-Sicherheit oder Cyber-Sicherheit, um ausschließlich die Sicherheit einer Entität zu bezeichnen, die von IT-bezogenen Bedrohungen betroffen ist (wie z. B. ein Angriff auf die Kommunikationsprotokolle eines elektronischen Geräts). Im Nachfolgenden werden wir daher den Begriff IT-Sicherheit verwenden.

Der Begriff *Safety* bezeichnet den Schutz eines Individuums vor internen und externen Bedrohungen, die sich negativ auf das Wohlbefinden des Individuums auswirken. Im Gegensatz zum Begriff IT-Sicherheit umfasst der Begriff *Safety* auch interne Bedrohungen. Die Fehlfunktion eines medizinischen Geräts (die nicht durch äußere Einflüsse verursacht wird) kann das Wohlbefinden eines Patienten beeinträchtigen, wenn die sie einen kritischen Teil der Gerätefunktionalität betrifft. Daher müssen solche internen Bedrohungen eingeschlossen werden. Im Nachfolgenden wird für *Safety* der Begriff Patientensicherheit verwendet.

Weiterhin umfasst die Definition nur solche Bedrohungen, die das Wohl der gesamten Entität beeinträchtigen. In Bezug auf externe Bedrohungen sind patientensicherheitsbezogene Angelegenheiten als Unterkategorie von IT-sicherheitsbezogenen Problemen zu verstehen. Das bedeutet, dass sich ein IT-Sicherheitsproblem prinzipiell auf die Patientensicherheit auswirken kann, beispielsweise wenn ein medizinisches Gerät durch die Ausnutzung einer Schwachstelle durch einen externen Angreifer unbrauchbar wird. Da das medizinische Gerät beispielsweise eine Funktion erfüllt, die für das Wohlergehen des Patienten unerlässlich ist, hat das IT-Sicherheitsproblem in diesem Fall eine Auswirkung auf die

Patientensicherheit. Wenn ein externer Angreifer die Schwachstelle jedoch nur ausnutzen kann, um Konfigurationsdaten des Geräts zu lesen, was keine direkten Auswirkungen auf das Wohlergehen des Patienten hat, dann besteht lediglich ein IT-Sicherheitsproblem.

Als Teil des CVD-Prozesses (Coordinated Vulnerablity Disclosure, siehe Abschnitt 2.11), bei dem eine Schwachstelle einem Hersteller gemeldet wird, ist es wichtig zu klären, ob ein IT-Sicherheitsproblem auch Auswirkungen auf die Patientensicherheit hat. Dieser Schritt kann manchmal nicht vom Finder allein durchgeführt werden, da zusätzliche Informationen zur Bewertung des Problems notwendig und ohne die Unterstützung des Herstellers nur schwer zu erhalten sind. Daher ist es für die Bewertung hilfreich, wenn die Hersteller eine Erklärung mit klaren Argumenten, die für den Finder verständlich sind, abgeben, in der sie klarstellen, ob das gemeldete Problem Auswirkungen auf die Patientensicherheit hat oder nicht.

2.10 Schutzziele: Vertraulichkeit, Integrität und Verfügbarkeit

Informationssicherheitsstandards, wie die ISO/IEC 27001 (ISO/IEC, 2013) verwenden oft spezielle Kategorien, um die Auswirkungen einer Schwachstelle besser klassifizieren zu können. Diese umfassen gewöhnlich Vertraulichkeit, Integrität und Verfügbarkeit. Im vorliegenden Dokument werden diese Kategorien, gemäß ihrer Definition aus der entsprechenden ISO/IEC-Norm, bei der Beschreibung des Risikos der identifizierten Schwachstellen verwendet.

Die ISO/IEC-Normen (ISO/IEC, 2018) definieren Vertraulichkeit als "Eigenschaft, dass Informationen nicht unbefugten Personen, Organisationen oder Prozessen zur Verfügung gestellt oder offengelegt werden". Als Beispiel wäre hier eine Schwachstelle, die einem Angreifer unautorisierten Zugang zu Daten auf einem System zu erhalten ermöglicht, zu nennen. Die Schwachstelle wirkt sich folglich auf die Vertraulichkeit der Daten dieses Systems aus.

Die ISO/IEC-Normen definieren den Begriff Integrität als "Eigenschaft der Genauigkeit und Vollständigkeit". Mit anderen Worten bedeutet dies, dass sichergestellt ist, dass Informationen nicht von unbefugten Personen manipuliert werden können. Dies schließt sowohl Informationen ein, die gespeichert sind, als auch Informationen, die gerade kommuniziert werden. Wenn ein Gerät beispielsweise über einen Update-Mechanismus verfügt, bei dem ein Firmware-Image zur Verfügung gestellt werden kann, wäre ein Angreifer möglicherweise in der Lage das Firmware-Image zu verändern und durch ein eigenes ersetzen. Wenn das Firmware-Image nicht durch zusätzliche Maßnahmen, wie eine kryptographische Signatur und eine entsprechende Signaturprüfung, geschützt ist, kann die Integrität der Firmware durch das Gerät nicht gewährleistet werden, was dazu führt, dass das Firmware-Image manipuliert werden kann.

Verfügbarkeit wird als "Eigenschaft, auf Anforderung durch eine autorisierte Stelle zugänglich und nutzbar zu sein " durch die ISO/IEC-Normen definiert. Für ein medizinisches Gerät spielt der Faktor Verfügbarkeit eine wichtige Rolle. Sobald das Gerät nicht mehr verfügbar, beziehungsweise verwendbar ist, z. B. aufgrund eines Angriffs, kann sich dies direkt auf die Patientensicherheit auswirken.

2.11 Das Coordinated Vulnerability Disclosure (CVD)

Die koordinierte Veröffentlichung von Schwachstellen (CVD) wird definiert als "der Prozess des Sammelns von Informationen von Schwachstellenfindern, die Koordinierung des Austauschs dieser Informationen zwischen den relevanten Interessengruppen und die Veröffentlichung der Existenz von Schwachstellen und ihrer Abhilfemaßnahmen gegenüber verschiedenen Interessengruppen, einschließlich der Öffentlichkeit" (Carnegie Mellon University, 2017).

Selbst in einem vermeintlich sicheren System können Schwachstellen niemals vollständig ausgeschlossen werden. Daher ist der professionelle Umgang mit Schwachstellen ein integraler Bestandteil der

Produktlebenszyklus-Aktivitäten des Herstellers. Wenn externe Parteien Schwachstellen melden, führen die meisten Unternehmen bereits koordinierte Veröffentlichungen dieser Schwachstellen durch.

In der IT-Sicherheitsbranche werden Veröffentlichungsfristen von bis zu 90 Tagen, von der Meldung bis zur Veröffentlichung der Schwachstellen, festgelegt. Ein Hersteller kann ein CVD nur dann erfolgreich (d. h. wiederholbar und zuverlässig) durchführen, wenn ein klar definierter Reaktionsprozess etabliert ist. Diese Prozesse müssen in nachvollziehbarer und transparenter Weise im Vorfeld der Schwachstellenmeldungen festgelegt werden, damit die Fehler umgehend behoben werden können.

An einem CVD-Prozess sind mehrere Instanzen, wie Schwachstellenfinder, Schwachstellenmelder, Hersteller und Koordinatoren beteiligt. Ein CVD erfordert ein hohes Maß an Kommunikation zwischen allen Beteiligten. Der Prozess sollte durch vertrauensvollen gegenseitigen Austausch und kontinuierliche Zusammenarbeit gestaltet sein. Alle Entitäten vereinbaren, dass sämtliche Informationen zu Schwachstellen vertraulich zu behandeln sind, bis der Veröffentlichungsprozess abgeschlossen ist.

Eine koordinierte Veröffentlichung von Informationen über Schwachstellen kann in verschiedene Phasen unterteilt werden. Zunächst entdeckt ein Finder eine oder mehrere Schwachstellen in einem Produkt. Danach reicht der Finder einen Schwachstellenbericht beim Produktanbieter oder bei einem externen Koordinator ein. In der dritten Phase führt der betroffene Hersteller zunächst eine Validierung und dann eine Triage der Schwachstellen durch. Danach wird ein Patch-Plan, ein Zeitplan für einen Software-Patch oder temporäre Maßnahmen entwickelt. Zum Schluss werden die Schwachstelle und ihr Patch-Plan der Öffentlichkeit bekannt gegeben.

Es ist ein branchenübergreifend anerkanntes Verhalten, entsprechend der Best Practices, dass die Schwachstellenfinder ein Veröffentlichungsdatum von 90 Tagen, von der Benachrichtigung des Herstellers bis zur Veröffentlichung der Informationen über die Schwachstelle, vorgeben. Notwendige Fristverlängerungen können nach dem Ermessen der Finder gewährt werden, wenn der Hersteller die Verzögerung rechtfertigen kann. (Carnegie Mellon University, 2017) In den USA empfiehlt die FDA einen Zeitraum von 60 Tagen im Falle von Schwachstellen in Medizinprodukten, die die Patientensicherheit beeinträchtigen können (FDA, 2016).

Die Art und Weise der Veröffentlichung von Schwachstellen liegt im Ermessen des Finders. Häufig werden Blog-Einträge oder White Paper veröffentlicht, um die Öffentlichkeit über die Entdeckungen zu informieren. Diese Blog-Beiträge enthalten in der Regel ausführliche technische Erläuterungen zur Identifizierung der Schwachstellen. Ferner werden die vorgeschlagenen Behebungen und die vom Hersteller ergriffenen Maßnahmen vorgestellt. Außerdem ist es eine weitere Best Practice, Schwachstellen sogenannte Common Vulnerabilities and Exposures (CVE) zuzuordnen. Diese CVE enthalten auf einfache und strukturierte Weise Informationen über die identifizierte Schwachstelle und das betroffene Produkt. Jeder CVE wird eine eindeutige ID-Nummer zugewiesen und alle CVE werden in der MITRE-Datenbank gespeichert.

2.12 Coordinated Vulnerability Disclosures im Projekt ManiMed

Im Gegensatz zu standardmäßigen CVD-Verfahren, werden im Projekt ManiMed Medizinprodukte bewertet. Es könnte ein Risiko für Patienten betstehen, wenn ein CVD-Verfahren nicht gründlich geplant und durchgeführt wird. Es wurde daher stets der Ansatz verfolgt, dass mit technischen Details und Zeitpunkten für die Veröffentlichung von Informationen verantwortungsvoll umgegangen wurde. Sowohl eine IT-Sicherheits-, als auch eine Patientensicherheitsrisikobewertung wurden vom Projektteam gefordert, da der Hersteller verpflichtet ist, die eigenen Produkte auf beides zu prüfen – IT-Sicherheit und Patientensicherheit. Für Schwachstellen, die die physische Gesundheit eines Patienten beeinträchtigen könnten, war die Zusammenarbeit mit dem BfArM ein wichtiger Teil des Verfahrens.

Im Folgenden werden alle Standardschritte erläutert, die während eines jeden CVD-Prozesses durchgeführt wurden. Jeder Hersteller wurde gleichbehandelt, um Marktverzerrungen zu vermeiden.

Nach der Sicherheitsprüfung des jeweiligen Medizinproduktes kontaktierte das Projektteam den Hersteller. Dieser Kontakt war sehr einfach herzustellen, da der Hersteller bekannt war und in den meisten Fällen die Geräte und/oder ein Prüflabor zur Verfügung stellte.

Zunächst wurde der Hersteller über alle Erkenntnisse informiert. Zu diesem Zweck wurde jedem Hersteller ein vollständiger und detaillierter Bericht der IT-Sicherheitsprüfung für sein Gerät oder System zur Verfügung gestellt. Alle Berichte wurden in englischer Sprache verfasst, um die Kommunikation innerhalb der multinationalen Strukturen der meisten Hersteller zu erleichtern. Um eine schnelle und effektive Abhilfe zu ermöglichen, wurde in jedem Bericht Folgendes beschrieben:

- detaillierte Erklärung aller bewerteten Systeme
- Beschreibungen aller Schwachstellen
- vollständiger Proof-of-Concept-Code
- entwickelte Exploits
- beispielhafte Videos, die z. B. von Abstürzen aufgenommen wurden.

In einem zweiten Schritt wurden die Berichte und Ergebnisse mit den verantwortlichen Teams der Hersteller diskutiert. Es wurden Maßnahmen zur Behebung der Schwachstellen und ein Zeitplan für die Umsetzung erörtert sowie ein Veröffentlichungsdatum festgelegt.

Der dritte Schritt umfasste die Kontaktaufnahme mit der CISA (Cybersecurity and Infrastructure Security Agency), einer Behörde der Vereinigten Staaten mit der Aufgabe, die Cyber-Sicherheit zu verbessern. Gemeinsam wurden CVE und Security Advisories zugewiesen und veröffentlicht, um die Transparenz zu erhöhen. Eine Veröffentlichung von Schwachstellen zeigt, dass ein Hersteller über potenzielle Mängel und mögliche Verbesserungen seiner Geräte Bescheid weiß und sich dahingehend kontinuierlich verbessert. Im Gegensatz zu CVE ermöglichen es Security Advisories den Herstellern ihre Risikoanalyse und Maßnahmen sowie die implementierten Korrekturen darzulegen. Darüber hinaus ermöglichen CVE eine öffentliche Bezugnahme auf Sicherheitslücken in Berichten, Diskussionen und Security Advisories. Die meisten Hersteller schätzten die Veröffentlichung der Schwachstellen, da sie eine treibende Kraft für die Priorisierung und Umsetzung von Patches beim Betreiber darstellt. Vor der Veröffentlichung wurde jede CVE-Beschreibung dem Hersteller, mit der Bitte um Stellungnahme übergeben, um eine Veröffentlichung koordiniert vorzunehmen.

Es stand den Herstellern frei, bereits vor diesem Dokument eigenständig Advisories zu veröffentlichen. Jeder Hersteller hatte die Wahl, ob er und der Name seines Produkts in diesem Dokument genannt werden dürfen oder ob er lieber anonym bleiben möchte. Ein Abschlussschreiben des BSI an den Hersteller markierte das Ende der Veröffentlichung. Es erlaubte den Herstellern, ihre Teilnahme am Projekt ManiMed öffentlich zu zeigen, ohne ihre geprüften Produkte als "vom BSI geprüft" oder "vom BSI zertifiziert" zu bewerben. Nach dem CVD-Prozess können die Schwachstellen auf IT-Sicherheitskonferenzen öffentlich diskutiert werden und für Publikationen im Zusammenhang mit dem ManiMed-Projekt verwendet werden. Im Hinblick auf Best Practices sind CVE und Security Advisories öffentlich zugänglich, um Transparenz zu schaffen und das Bewusstsein für IT-Sicherheit zu erhöhen. Die Liste der Sicherheitshinweise und CVE aus dem Projekt ManiMed kann in Abschnitt 8.1 eingesehen werden.

3 Marktanalyse

Dieses Kapitel umfasst die Marktanalyse für Medizinprodukte, die im Rahmen des Projekts ManiMed mittels IT-Sicherheitsprüfungen untersucht wurden. Um geeignete Geräte für solche Prüfungen auszuwählen, wurden die folgenden Anforderungen festgelegt:

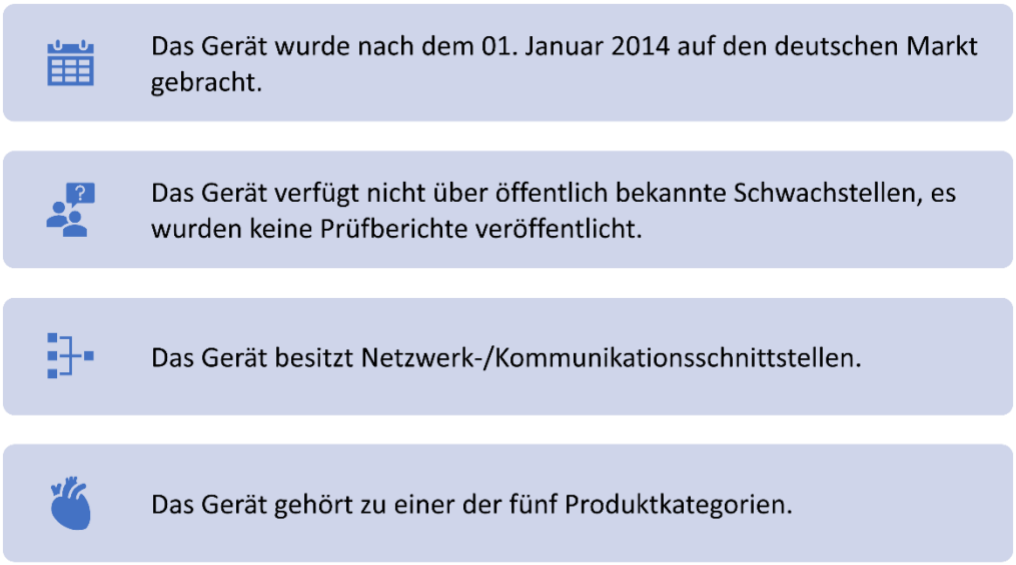

Abbildung 2: Anforderungen an medizinische Geräte im Rahmen der Marktanalyse

Diese vier Anforderungen müssen für Geräte, die einer IT-Sicherheitsprüfung unterzogen werden, erfüllt werden, abgesehen davon, dass die ausgewählten Gerätekategorien aufgrund ihrer Auswirkungen auf die Patientensicherheit auf ein hohes Maß an IT-Sicherheit angewiesen sind.

Allerdings könnten diese Auswahlkriterien auch zu gewissen Verzerrungen der Ergebnisse der Sicherheitsprüfungen geführt haben, die wie folgt aussehen:

- Das Datum (1. Januar 2014) wird zwar als angemessen erachtet, sodass nur Geräte einbezogen werden, die über neuartige Kommunikationsschnittstellen verfügen, welche von Schwachstellen betroffen sein können. Geräte, die aber vor diesem Datum in Deutschland auf den Markt gebracht werden, können ebenfalls solche Schnittstellen aufweisen, waren jedoch von der Analyse ausgeschlossen.
- Auch der Ausschluss von Geräten, bei denen Schwachstellen bereits in der Vergangenheit veröffentlicht wurden oder die Teil einer veröffentlichten Sicherheitsprüfung waren, könnte zu einer Verzerrung dieser Bewertung führen. Dies wird damit begründet, dass diese Geräte neben den bereits veröffentlichten Schwachstellen noch weitere Sicherheitsschwachstellen aufweisen könnten, wodurch sich die Gesamtsumme der auffindbaren Schwachstellen reduziert. Dennoch könnten die Geräte neben den bereits veröffentlichten Schwachstellen zusätzliche Schwachstellen aufweisen. Andererseits, wenn bisher keine Sicherheitslücken veröffentlicht wurden, könnte dies bedeuten, dass entweder der Hersteller selbst intensive Sicherheitsprüfungen vor der Markteinführung durchführt oder dass das Gerät noch keiner Prüfung unterzogen wurde. Die Marktanalyse berücksichtigt diese Punkte nicht.

Die folgenden zu untersuchenden Kategorien (aufgelistet in Abbildung 3) wurden vor Beginn des Projekts ausgewählt:

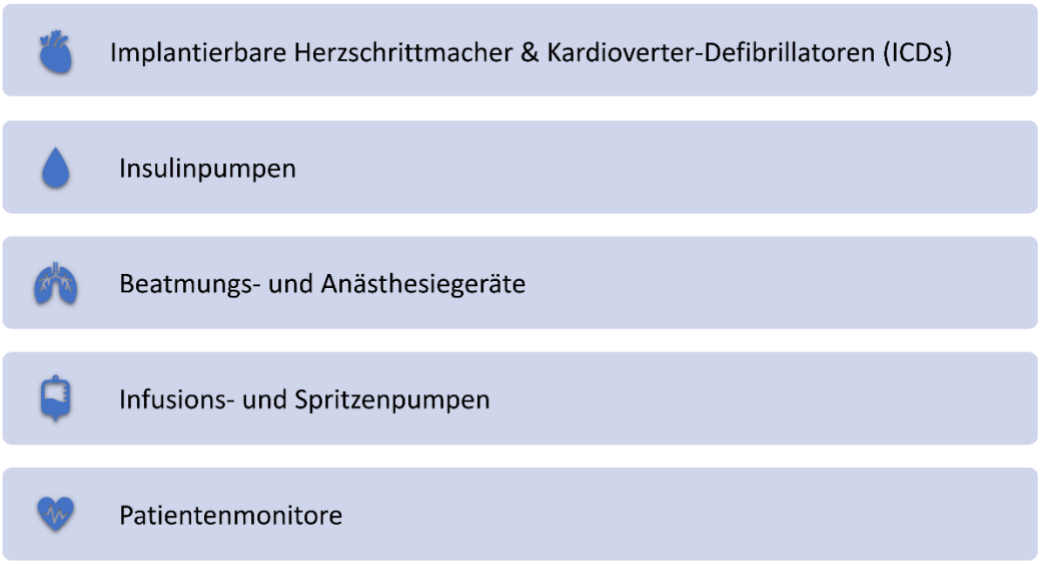

Abbildung 3: Kategorien von Medizinprodukten für die Marktanalyse

Alle ausgewählten Kategorien entsprechen Geräten, die im Falle von Sicherheitsproblemen einen kritischen Einfluss auf die Patientensicherheit haben könnten.

Für die Suche nach Produkten, die die in Abbildung 2 aufgeführten Anforderungen erfüllen und zu einer der in Abbildung 3 aufgeführten Kategorien gehören, wurden mehrere Quellen herangezogen, die in Abschnitt 3.1 dargestellt sind. Für jede Produktkategorie sind die Ergebnisse dieser Suche als Flussdiagramme in Abschnitt 3.2 dargestellt. Weitere Informationen zu den Auswahlkriterien, die in den verschiedenen Iterationen der Suche verwendet wurden, sind dort zu finden. Ausführliche Informationen über die bewerteten Produkte und die Ergebnisse der Prüfungen sind in Abschnitt 4 enthalten.

3.1 Informationsquellen

Die folgenden Quellen wurden für die Marktanalyse herangezogen:

- Datenbank für Medizinprodukte-Anzeigen
- Anfrage an medizinische Einrichtungen
- Öffentliche Informationen von Medizinprodukteherstellern
- Internetrecherche
- Fragebogen an Hersteller

Die verschiedenen Quellen werden im Folgenden näher beschrieben.

3.1.1 Datenbank für Medizinprodukte-Anzeigen (MPA)

Das DIMDI betreibt ein Medizinprodukte-Informationssystem, das z. B. für die Meldung an die zuständigen Behörden nach § 33 des Medizinproduktegesetzes (Bundesgesetzblatt, 1994) verwendet wird. Der öffentliche Teil dieses Informationssystems enthält die Datenbank Medizinprodukte-Anzeigen (MPA). Zum Zeitpunkt der vorliegenden Untersuchung (04. Juni 2019) umfasste die Datenbank seit Beginn der

Datenerfassung im Jahr 2002 105.730 Medizinprodukte. Diese Zahl ändert sich ständig, da die Datenbank täglich aktualisiert wird.

Anfragen an die Datenbank werden über die SmartSearch-Schnittstelle des DIMDI gestellt. Diese Schnittstelle ermöglicht einzelne Felder der Datenbank zu selektieren und Suchanfragen zu kombinieren. Bestimmte Felder weisen einen festen Bereich möglicher Werte auf, die über einen Index abgefragt werden können. Darüber hinaus ist die Suche mit Wildcards für Freitextfelder möglich. Die Resultate einer Abfrage können über eine Watchlist im XML-Format exportiert werden. Der Zugriff auf die MPA-Datenbank erfolgt über das vom BfArM zur Verfügung gestellte Feld Medizinprodukte-Informationssystem (BfArM).

Nicht alle für den deutschen Markt zugelassenen Medizinprodukte sind in der Datenbank enthalten. Es liegt nahe, dass eine unvollständige Synchronisation diese Diskrepanz zu anderen Medizinprodukte-Datenbanken in der Europäischen Union verursacht. Wenn z. B. das erste Inverkehrbringen eines Medizinproduktes in einem anderen Staat der EU erfolgte, wird es wahrscheinlich nur in der entsprechenden nationalen Datenbank registriert. Darüber hinaus registrieren einige Hersteller keine Komplettsysteme in diesen Datenbanken, sondern legen verschiedene Komponenten und Module separat ab, was es schwierig macht alle notwendigen Teile eines Produkts zu finden. Daher wurden zusätzliche Quellen zur Identifizierung von Medizinprodukten auf dem deutschen Markt, wie unten beschrieben, verwendet.

3.1.2 Anfragen an medizinische Einrichtungen

Um abzuschätzen, welche medizinischen Geräte von Einrichtungen in Deutschland verwendet werden, wurden Anfragen an ausgewählte Einrichtungen mit der Bitte geschickt, Informationen über deren Bestand an Medizinprodukten zu liefern. Die Vorlage der Anfragen befindet sich in Abschnitt 8.

3.1.3 Öffentliche Informationen von Herstellern

Als dritte Quelle wurden Informationen, die von Medizinprodukteherstellern veröffentlicht wurden, zur Identifizierung weiterer Geräte verwendet. Sowohl Online-Suchmaschinen, als auch die MPA-Daten und die Anfrage an die medizinischen Einrichtungen wurden genutzt, um Medizinprodukthersteller der verschiedenen Kategorien zu identifizieren. Anschließend wurde das Geräteportfolio des Herstellers hinsichtlich geeigneter Geräte analysiert. Anhand der verfügbaren Spezifikationen wurde festgestellt, ob das Produkt über eine Netzwerkfunktionalität oder andere vielversprechende Schnittstellen verfügt.

3.1.4 Internetrecherche

Abgesehen von den Informationen, die von Medizinprodukteherstellern veröffentlicht wurden, wurden Ausstellerlisten von relevanten Medizininformatik- und Medizinproduktmessen verwendet, um die Anzahl der Hersteller für die Marktanalyse zu maximieren. Diese Suche wurde überwiegend online durchgeführt. Sie umfasst die Digital Medical Expertise & Applications (DMEA) und die MEDICA. Beide Messen sind international anerkannt und die größten in ihren jeweiligen Branchen, was den Vorteil hat, dass die Aussteller auf diesen Messen einen bedeutenden Prozentsatz des globalen Medizinproduktemarktes repräsentieren.

Darüber hinaus wurden die jüngsten technischen Fortschritte im medizinischen Bereich durch Sichtung wissenschaftlicher Publikationen und Fallstudien sowie praktische Auswertungen nationaler und internationaler Pilotprojekte in die Analyse einbezogen. So wurde beispielsweise PubMed (NCBI) als eine der Quellen für diese Untersuchung herangezogen. PubMed ist eine englische, textbasierte Metadatenbank für medizinische und wissenschaftliche Artikel. Die Datenbank wird vom National Center for Biotechnology

Information (NCBI) innerhalb der National Library of Medicine (NLM) durch das National Institute of Health (NIH) der USA entwickelt und betrieben.

Eine weitere Quelle ist die Deutsche Nationalbibliothek (DNB), die als zentrale Archivbibliothek für alle in deutscher Sprache publizierten Medienwerke (DNB) fungiert.

Auf diesem Weg konnten keine weiteren Geräte identifiziert werden, d. h. dass alle Geräte bereits mit Hilfe anderer Quellen gefunden werden konnten.

3.1.5 Fragebögen an Hersteller

In Einzelfällen, in denen nur begrenzte Informationen über Produkte verfügbar waren, wurde ein Fragebogen an die Hersteller geschickt. Der Inhalt des Fragebogens ist in Abschnitt 8.3 aufgeführt.

3.2 Ergebnisse

Die folgenden Abschnitte enthalten die Ergebnisse der Marktanalyse. Die Auswahl der Geräte für jede Kategorie basiert auf der im vorherigen Kapitel vorgestellten Quelle. Der gesamte Auswahlprozess folgt den in Abbildung 4 dargestellten Schritten.

Die Grundauswahl an Medizinprodukten, die über die Internetrecherche und die DIMDI-Datenbankrecherche identifiziert wurden und die Antworten auf die an die Betreiber gesendeten Anfragen sind in Abbildung 4 dargestellt. Anschließend wurden die Geräte hinsichtlich ihrer Kommunikationsschnittstellen bewertet und Geräte aussortiert, die keine relevanten Kommunikationsschnittstellen besitzen. Für die übrigen Geräte wurde evaluiert, ob bereits Schwachstellen oder Berichte über IT-Sicherheitsprüfungen veröffentlicht wurden. Falls nicht, wurden diese Geräte in die Vorauswahl aufgenommen. Waren mehr als fünf Geräte übrig, wurden in einem letzten Schritt die Hersteller nach weiteren Details zu den Geräten befragt. Anhand der Details wurde eine priorisierte Liste von Geräten für die Prüfung erstellt. Es wird darauf hingewiesen, dass ausgewählte Geräte in Abschnitt 4 aus technischer Sicht näher beschrieben werden.

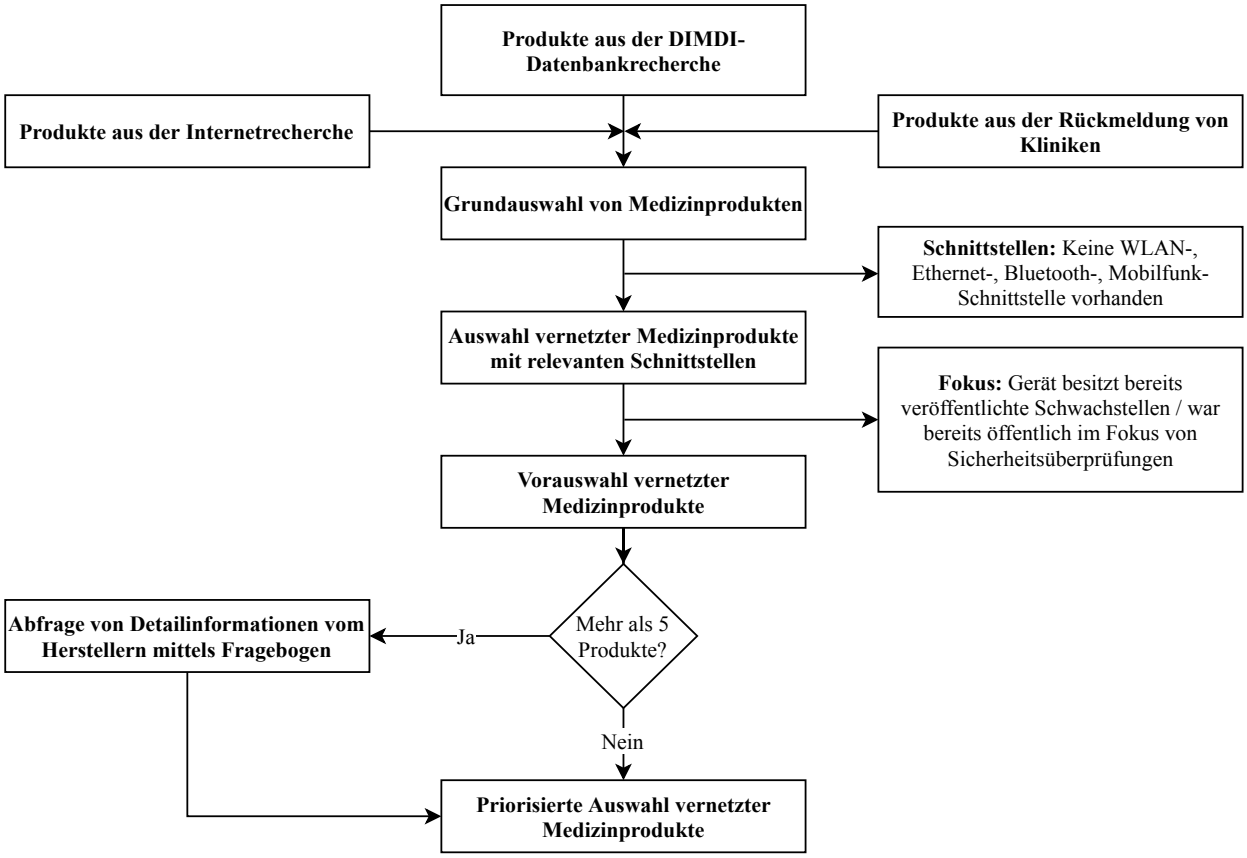

Abbildung 4: Abbildung des während der Marktanalyse durchgeführten Gesamtauswahlprozesses.

3.2.1 Implantierbare Herzschrittmacher und implantierbare Kardioverter-Defibrillatoren (ICDs)

Für die Marktanalyse wurde die in Abschnitt 3.1.1 beschriebene Datenbank über Medizinprodukte-Anzeigen (MPA) als Grundlage verwendet. Die Analyse konzentrierte sich dabei auf in Deutschland zugelassene Herzschrittmacher, die in den letzten fünf Jahren Zugang zum Markt erhalten haben. Abbildung 5 zeigt den Auswahlprozess von Herzschrittmachern mit den zugehörigen Auswahlkriterien in einem Flussdiagramm. Die Kriterien *Änderungsdatum*, *Art der Meldung* und *Kategorie* sind strenge Ausschlusskriterien dieser Datenbankrecherche.

Wie in Abbildung 5 dargestellt, ergab die Suche mit der MPA-Datenbank 19 potenzielle Geräte. Nach einer manuellen Überprüfung dieser Geräte wurde jedoch festgestellt, dass die Geräte keine Schnittstellen enthielten, die eine Untersuchung im Rahmen einer IT-Sicherheitsprüfung rechtfertigen. Zudem ist in dieser Kategorie jedes einzelne Teil des Herzschrittmachersystems separat aufgeführt. Das endgültige implantierte Produkt ähnelt eher einem Baukastensystem, um Flexibilität und Kompatibilität zwischen mehreren Produkten derselben Produktfamilie zu ermöglichen und die Zulassung zu erleichtern.

Die an medizinische Einrichtungen gerichteten Anfragen erzielten keine weiteren Geräteinformationen.

Schließlich wurde der Jahresbericht 2016 des Deutschen Herzschrittmacher- und Defibrillatorregisters (IQTIG, 2016) konsultiert, da er eine Liste enthält, die die Anzahl der implantierten Herzschrittmacher pro Hersteller in den Jahren 2014, 2015 und 2016 quantifiziert. Eine solche Liste war im Bericht 2017 nicht enthalten, sodass der Bericht 2017 nicht zur Gewinnung dieser Daten herangezogen werden konnte.

3.2.1.1 Ergebnisse

Auf der Grundlage der im Bericht enthaltenen Informationen (insbesondere der Marktverteilung der Hersteller) wurden für die Prüfung die folgenden Hersteller-Systeme herangezogen:

- **Biotronik**: Rivacor 7 VR-T DX, Renamic Neo, Cardio Messenger Smart
- **Medtronic:** CareLink SmartSync Device Manager System

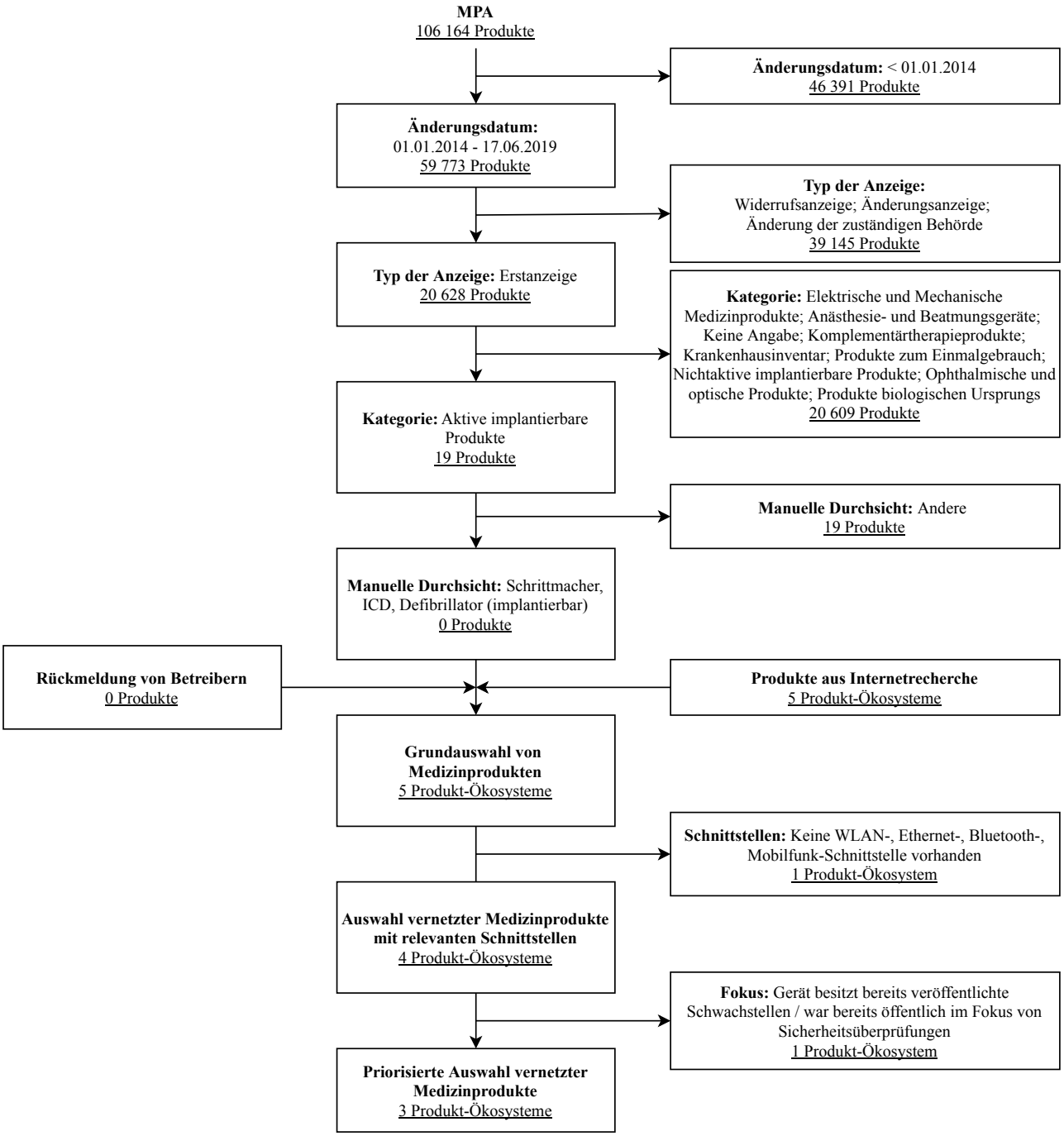

Abbildung 5: Flussdiagramm zur Veranschaulichung des Auswahlprozesses für implantierbare Herzschrittmacher.

3.2.2 Insulinpumpen

Im Fokus der Analyse stehen in Deutschland zugelassene ambulante Insulinpumpen. Abbildung 6 zeigt das für Insulinpumpen angewandte Auswahlverfahren mit den zugehörigen Auswahlkriterien in einem Flussdiagramm. Die Kriterien *Änderungsdatum*, *Art der Meldung*, *Kategorie* und *Nomenklatur* waren strenge Ausschlusskriterien für diese Datenbankrecherche. Diese Ergebnisse wurden nach einer manuellen Überprüfung um die Ergebnisse der Internetrecherche und Rückmeldungen zu den Geräten der Betreiber erweitert. Sie wurden nach den Ausschlusskriterien gefiltert, um eine priorisierte Liste der Geräte zu erhalten.

Wie in Abbildung 6 dargestellt, wurden nach Anwendung der Ausschlusskriterien bei der Datenbankrecherche acht Geräte identifiziert, welche die Anforderungen erfüllten. Die an medizinische Einrichtungen gesendeten Anfragen identifizierten keine weiteren Geräte.

Für die Internetrecherche wurden Patientenportale, Internetforen und Informationswebseiten systematisch nach Produktlisten und Produktübersichten durchsucht. Es wurden vier Insulinpumpen identifiziert, die nach dem 1. Januar 2014 für den deutschen Markt zugelassen wurden und nicht in der MPA-Datenbank des DIMDI gelistet sind.

Insgesamt konnten nach Auswertung aller drei Quellen zwölf Geräte identifiziert werden. Diese Geräte wurden weiter auf ihre potentielle Angriffsoberfläche hin untersucht, d. h. ob diese Geräte irgendwelche Kommunikationsschnittstellen implementiert haben. So reduzierte sich die Anzahl auf sechs Geräte. Nach Ausschluss von Produkten, für die Schwachstellen veröffentlicht wurden, blieben insgesamt vier Geräte übrig.

3.2.2.1 Ergebnisse

Bei der Auswahl der Geräte für die IT-Sicherheitsprüfung wurde solchen Pumpen Priorität eingeräumt, die mit einer mobilen Anwendung gesteuert werden können, im Vergleich zu Pumpen, bei denen nur Daten über die Anwendung gelesen werden können. Insgesamt wurden für die IT-Sicherheitsprüfung die folgenden Insulinpumpensysteme ausgewählt:

- **SOOIL:** DANA Diabecare RS, AnyDANA-i & AnyDANA-a mobile Applikationen
- **Ypsomed:** mylife YpsoPump, mylife App, mylife Cloud

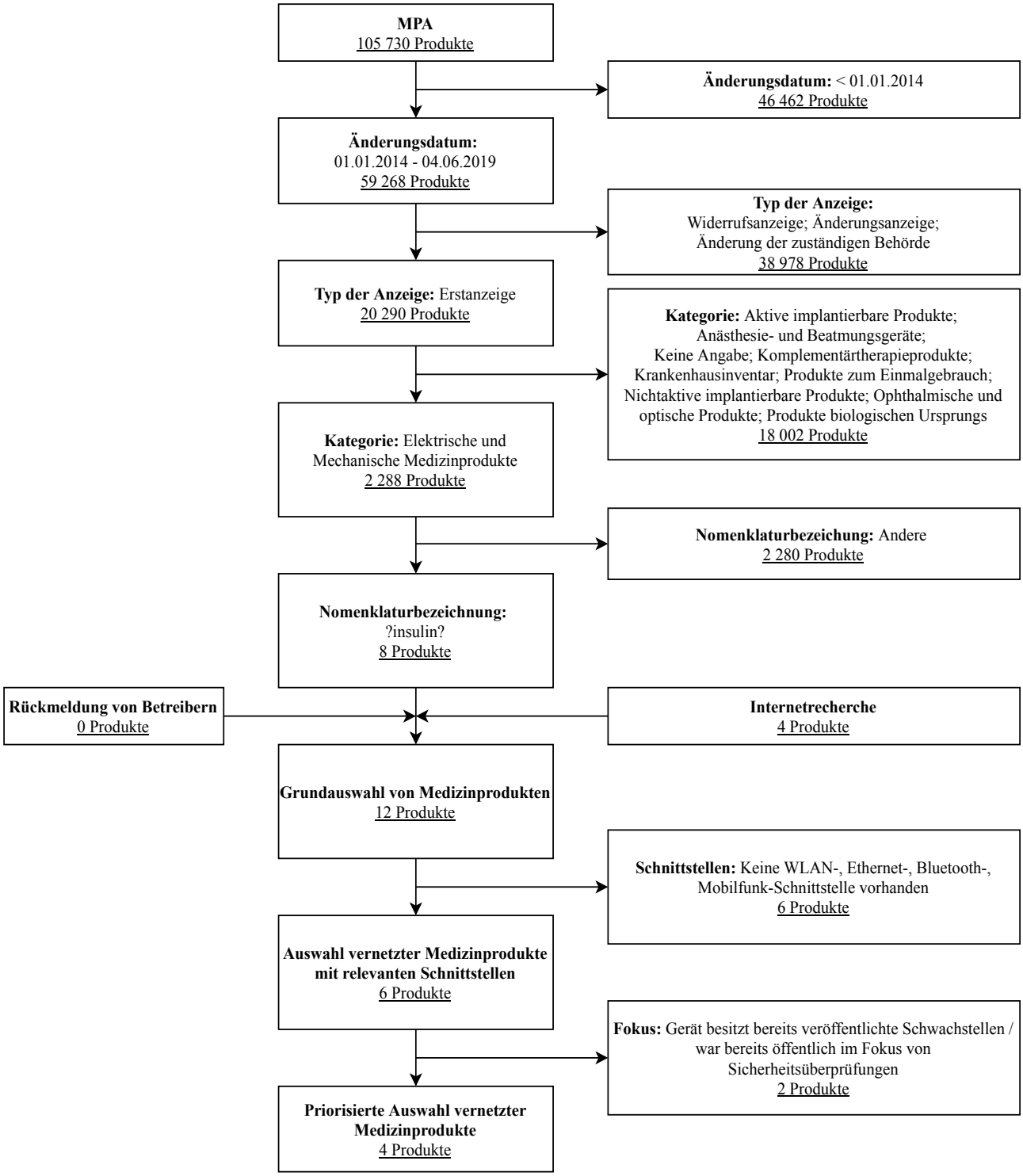

Abbildung 6:Flussdiagramm zur Veranschaulichung des Auswahlverfahrens für Insulinpumpen.

3.2.3 Beatmungsgeräte

Die Analyse konzentrierte sich auf Beatmungs- und Anästhesiegeräte, die in Deutschland zugelassen sind. Luftbefeuchter, Heizgeräte und Gasverteiler blieben unberücksichtigt. Abbildung 7 zeigt das für Beatmungsgeräte angewandte Auswahlverfahren mit den zugehörigen Auswahlkriterien in einem Flussdiagramm. Die Kriterien *Änderungsdatum*, *Art der Meldung*, *Art des Produkts*, *Kategorie* und *Medizinprodukteklasse* waren strenge Ausschlusskriterien für die Datenbankrecherche. Diese Ergebnisse wurden nach einer manuellen Überprüfung um die Ergebnisse der Internetrecherche und die Rückmeldungen von Betreibern zu den Geräten erweitert. Zwei Ausschlusskriterien filterten diese Ergebnisse weiter: *Schnittstellen* und *Fokus von Sicherheitsprüfungen*. Nach Einholung weiterer Informationen anhand von Fragebögen, die an die Hersteller geschickt wurden, wurde eine priorisierte Liste dieser Geräte erstellt.

Wie in Abbildung 7 dargestellt, wurden nach Anwendung der Ausschlusskriterien auf die Datenbankrecherche 56 Geräte identifiziert, die die Anforderungen erfüllen.

Darüber hinaus wurden drei klinische Beatmungsgeräte als Antwort auf die an klinische Einrichtungen gesendete Anfrage gemeldet, von denen zwei hinsichtlich ihres Auftretens auf dem deutschen Markt in Frage kamen. Beide Geräte wurden bereits durch die Suche in der MPA-Datenbank identifiziert.

Für die Internet-Recherche wurden Beatmungsgeräte auf Websites von z. B. Medizintechnikmessen wie der MEDICA (MEDICA, 2019) nach Geräten durchsucht, die noch nicht in der Ergebnismenge enthalten waren. Dabei wurden 20 Geräte identifiziert, die als mögliche Kandidaten in Frage kamen, aber nicht in der MPA-Datenbank aufgeführt waren. Es ist zu erwähnen, dass auch Geräte aufgenommen wurden, für die kein konkretes Datum der Zulassung für den deutschen Markt ermittelt werden konnte.

Daher wurden 78 Produkte identifiziert, nachdem alle drei Quellen genutzt wurden. Diese Geräte wurden weiter auf ihre potentielle Angriffsoberfläche hin untersucht, d. h. ob diese Geräte irgendwelche Kommunikationsschnittstellen implementiert haben. Dies ergab eine Gesamtzahl von 31 Geräten. Darüber hinaus wies keines der Geräte öffentlich bekannte Schwachstellen auf, sodass keines der Geräte ausgeschlossen werden konnte.

3.2.3.1 Ergebnisse

Bei der Auswahl der Geräte für die IT-Sicherheitsprüfung wurden der Grad der vom Hersteller beworbenen Funktionen zur Gerätevernetzung und das Feedback der Betreiber berücksichtigt. Insgesamt wurde das HAMILTON-T1-Beatmungsgerät der Hamilton Medical AG für die IT-Sicherheitsprüfung ausgewählt.

Es war ursprünglich geplant, dass im Rahmen des ManiMed-Projekts zwei Beatmungsgeräte geprüft werden. Aus Rücksicht auf die Situation und die Umstände, die mit der Covid-19-Pandemie einhergingen, wurde vom Test eines zweiten Beatmungsgeräts abgesehen.

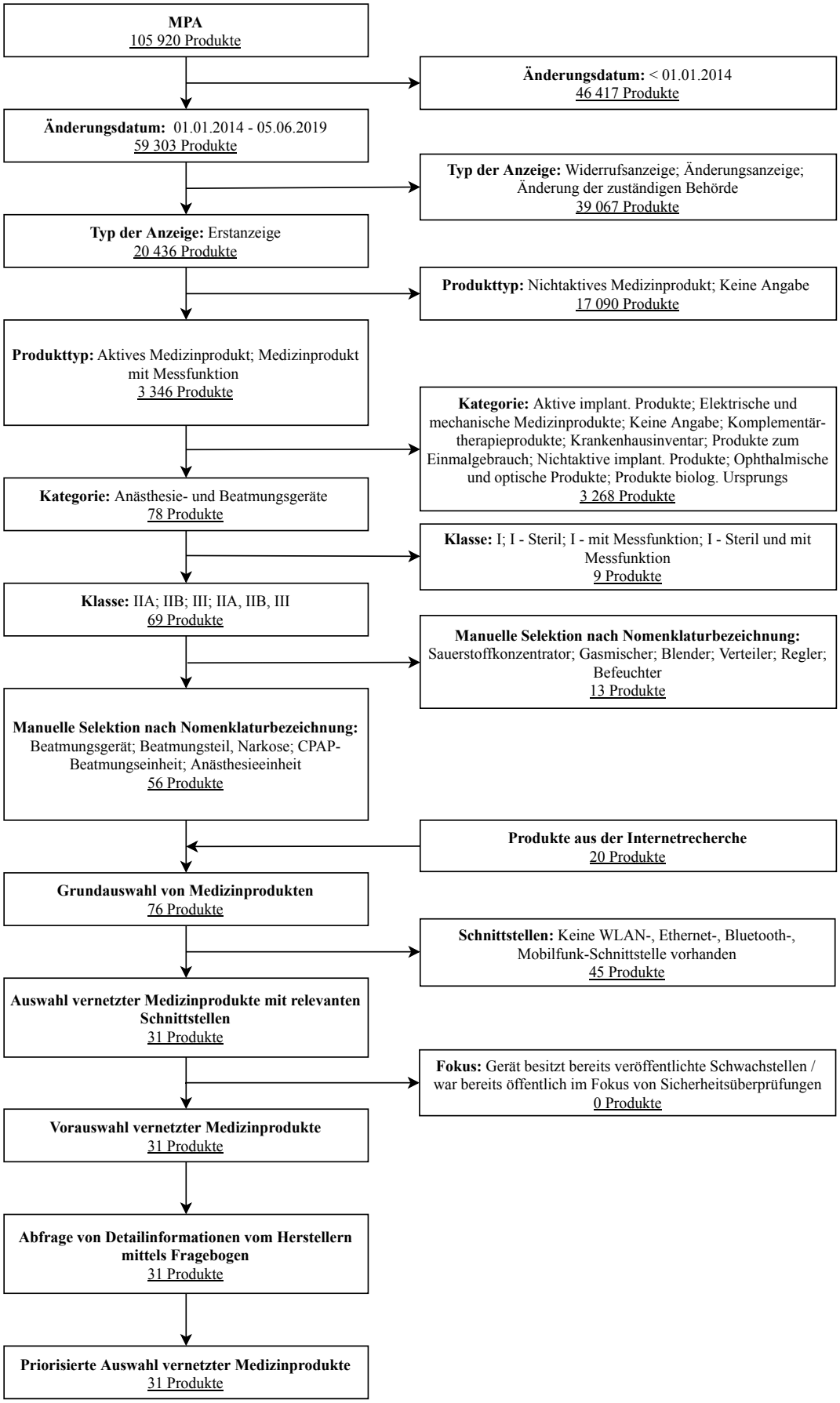

Abbildung 7: Flussdiagramm zur Veranschaulichung des Auswahlverfahrens für Beatmungsgeräte.

3.2.4 Infusions- und Spritzenpumpen

Die Analyse konzentriert sich auf Spritzen- und Infusionspumpen. Abbildung 8 zeigt das für Spritzen- und Infusionspumpen angewandte Auswahlverfahren mit den zugehörigen Auswahlkriterien in einem Flussdiagramm. Die Kriterien *Änderungsdatum*, *Art der Meldung* und *UMDNS-Code* waren strenge Ausschlusskriterien für diese Datenbankrecherche. Diese Ergebnisse wurden nach einer manuellen Überprüfung um die Ergebnisse der Internetrecherche und Rückmeldungen zu den Geräten der Betreiber erweitert. Sie wurden dann nach den Ausschlusskriterien *Schnittstellen* und *Fokus von Sicherheitsprüfungen* gefiltert. Nach Einholung weiterer Informationen mit Hilfe von Fragebögen, die an die Hersteller geschickt wurden, wurde eine priorisierte Liste der Geräte in der Ergebnismenge erstellt.

Wie in Abbildung 8 dargestellt, erfüllte keines der in der Datenbank aufgeführten Geräte alle Anforderungen.

Die an medizinische Einrichtungen versendeten Fragebögen ergaben sieben klinische Infusionsgeräte und Spritzenpumpen. Zusätzlich wurden im Rahmen der Internetrecherche verschiedene Websites, z. B. Medizintechnikmessen wie die MEDICA (MEDICA, 2019), besucht. Darüber hinaus lagen zu Beginn der Recherche bereits Rückmeldungen von Betreibern vor, sodass die dort verwendeten Geräte als Ausgangspunkt genutzt werden konnten. Es wurden 34 Geräte identifiziert, die nicht in der MPA-Datenbank des DIMDI verzeichnet sind. Es ist zu beachten, dass auch Geräte enthalten sind, für die kein spezifisches Datum der Zulassung für den deutschen Markt ermittelt werden konnte. Darüber hinaus wurden die meisten Infusionssysteme vor 2014 auf den Markt gebracht und werden regelmäßig durch neue Pumpen erweitert. Daher wurde das Marktzugangskriterium nicht als strenges Ausschlusskriterium herangezogen, da sonst keine Geräte für die IT-Sicherheitsprüfung zur Verfügung gestanden hätten.

Infusions- und Spritzenpumpen werden im klinischen Kontext selten allein eingesetzt, da häufig mehrere Medikamente und Infusionen parallel mit verschiedenen Pumpen verabreicht werden. Aus diesem Grund verfügen sie außer Infrarot- und seriellen Schnittstellen über keine zusätzlichen Netzwerkschnittstellen. Stattdessen werden sie in Docks zusammengefasst, die dann eine gemeinsame Netzwerkschnittstelle für alle Pumpen bieten. Aus diesem Grund wurden die vernetzten Infusions- und Spritzenpumpen in diesem Projekt in Kombination mit ihrer Systemumgebung analysiert. Damit die Geräteserie in der Ergebnismenge der Suche verbleiben konnte, wurde mindestens eine Netzwerkschnittstelle, z. B. WLAN, Ethernet, RFID / NFC oder Bluetooth zur Anbindung an ein zentrales System, wie zum Beispiel ein Patientendatenmanagementsystem (PDMS), benötigt. Um diese Schnittstellen zu filtern, wurden technische Gerätedatenblätter, Flyer und Handbücher verwendet. Insgesamt ergaben sich daraus sieben Geräte-Ökosysteme. Zwei dieser Ökosysteme hatten bereits Schwachstellen veröffentlicht, sodass insgesamt fünf von ihnen für die Prüfung in Frage kamen.

3.2.4.1 Ergebnisse

Bei der Auswahl der Geräte für die IT-Sicherheitsprüfung wurden Infusions- und Spritzenpumpen auf Grundlage des Feedbacks der Betreiber und der vorhandenen Schnittstellen priorisiert. Netzwerkschnittstellen, wie Ethernet und WLAN, wurden zuerst priorisiert, gefolgt von USB- und seriellen Schnittstellen. Um zwischen Geräten mit ähnlichen Schnittstellen wählen zu können, wurde die Anzahl der von den teilnehmenden Betreibern erworbenen Geräte berücksichtigt.

In Kapitel 3.2.3.1 wurde erwähnt, dass vom Test eines zweiten Beatmungsgeräts abgesehen wurde. Aus diesem Grund wurde stattdessen ein drittes Infusionssystem für IT-Sicherheitsüberprüfung ausgewählt:

- **B. Braun Melsungen AG:** Space System
- **Anonym:** Infusionssystem #1
- **Anonym:** Infusionssystem #2

Zusätzlich wurde ein Managementsystem für Spritzen- und Infusionspumpen getestet:

- **COPRA System GmbH:** Copus (Copra Pump Management System)

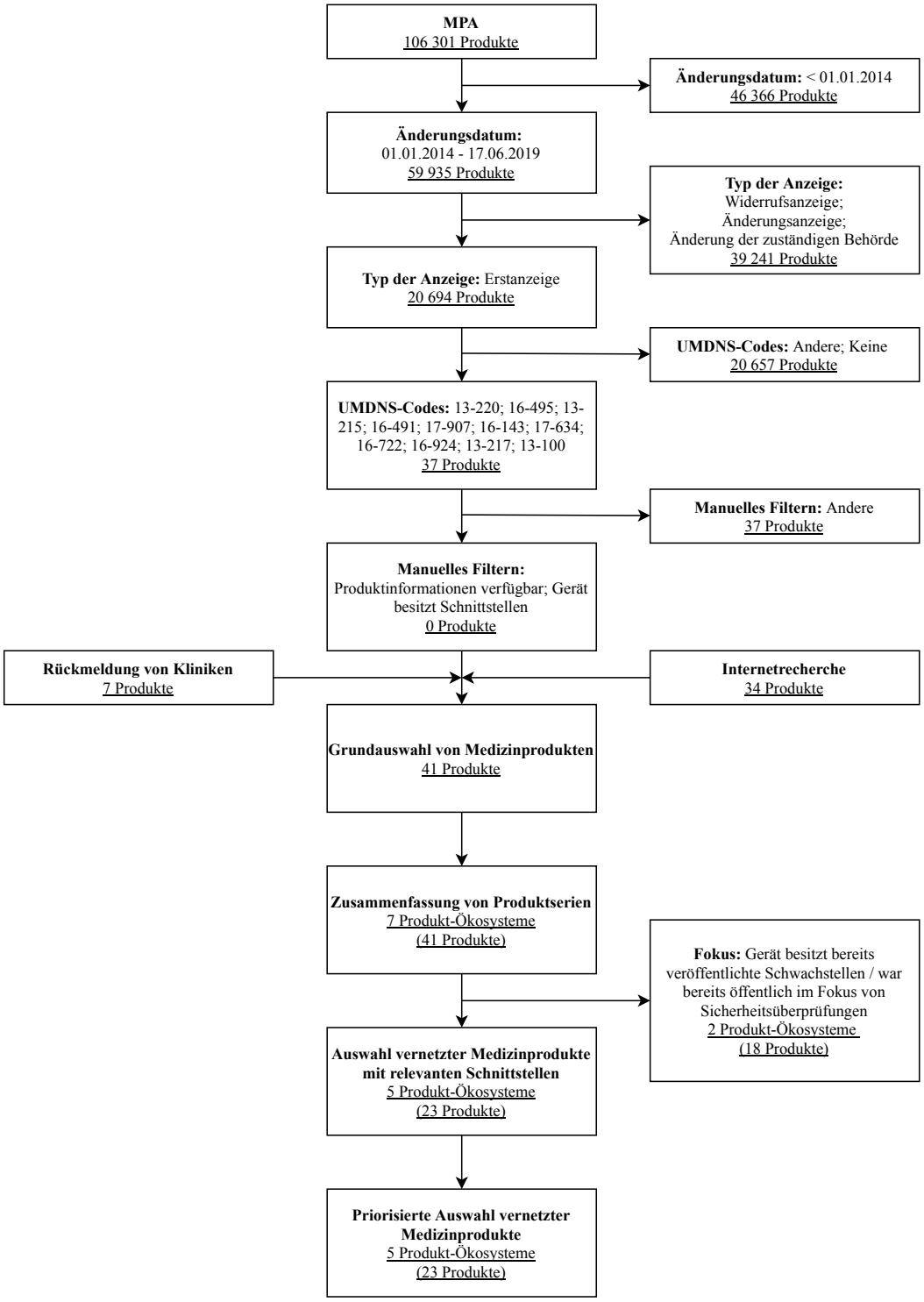

Abbildung 8: Flussdiagramm zur Veranschaulichung des Auswahlverfahrens für Infusions- und Spritzenpumpen.

3.2.5 Patientenmonitore

Die Analyse konzentriert sich auf in Deutschland zugelassene Patientenmonitore. Reine EKG- und EEG-Geräte seien hier nicht miteingeschlossen. Das Diagramm in Abbildung 9 zeigt den für die Patientenmonitore angewandten Auswahlprozess zusammen mit den zugehörigen Auswahlkriterien in einem Flussdiagramm. Die Kriterien *Änderungsdatum*, *Art der Meldung* und *UMDNS-Code* waren strenge Ausschlusskriterien für diese Datenbankrecherche. Diese Ergebnisse wurden nach einer manuellen Überprüfung um die Ergebnisse der Internetrecherche und Rückmeldungen zu den Geräten der Betreiber erweitert. Sie wurden dann nach den Ausschlusskriterien *Schnittstellen* und *Fokus von Sicherheitsprüfungen* gefiltert. Nach Einholung weiterer Informationen mit Hilfe von Fragebögen, die an die Hersteller geschickt wurden, wurde eine priorisierte Liste der Geräte in der Ergebnismenge erstellt.

Wie in Abbildung 9 dargestellt, blieben acht Geräte übrig, nachdem jedes Ausschlusskriterium angewendet wurde. Darüber hinaus wurden zum Zeitpunkt der Abfassung dieser Betrachtung fünf klinische Patientenmonitore von Betreibern gemeldet, vier davon wurden jedoch vor 2014 auf den Markt gebracht und kamen daher nicht für Tests in Frage. Infolgedessen wurde nur ein weiteres Gerät aus den Rückmeldungen von Betreibern mitaufgenommen.

Für die Internetrecherche wurden weitere Patientenmonitore auf den Webseiten von Medizintechnikmessen, wie der MEDICA, gesucht. Es konnten 18 Geräte identifiziert werden, die nach dem 1. Januar 2014 für den deutschen Markt zugelassen wurden und nicht in der MPA-Datenbank des DIMDI gelistet waren.

Insgesamt ergaben die drei Quellen zusammen 27 Geräte. Zu vier Geräten waren jedoch bereits Schwachstellen veröffentlicht worden und acht weitere Geräte besaßen keine relevanten Netzschnittstellen, sodass die Suche zu einer Gesamtzahl von 15 Patientenmonitoren führte.

3.2.5.1 Ergebnisse

Ein priorisierender Faktor war das Datum des Marktzugangs, sodass neuere Geräte gegenüber älteren bevorzugt wurden. Außerdem wurden Geräte mit einer zentralen Verwaltungssoftware gegenüber Geräten ohne eine solche Lösung bevorzugt. Darüber hinaus hatten eine erweiterte Netzwerkfunktionalität, wie z. B. die zentrale Benutzerverwaltung über z. B. LDAP oder standardisierte Kommunikationsschnittstellen, wie HL7-Standards oder ADT, eine höhere Priorität. Geräte für den Einsatz in spezialisierten Anwendungsgebieten, wie z. B. Geräte, die während der Magnetresonanztomographie eingesetzt werden können, wurden weniger bevorzugt, da sie aufgrund der limitierenden Umgebungsbedingungen in der Regel weniger Schnittstellen aufweisen.

Insgesamt wurden die folgenden Patientenmonitore für die IT-Sicherheitsprüfung ausgewählt:

- **Innokas Yhtymä Oy:** VC 150 Patient Monitor
- **Philips**: IntelliVue MX850, Patient Information Center iX

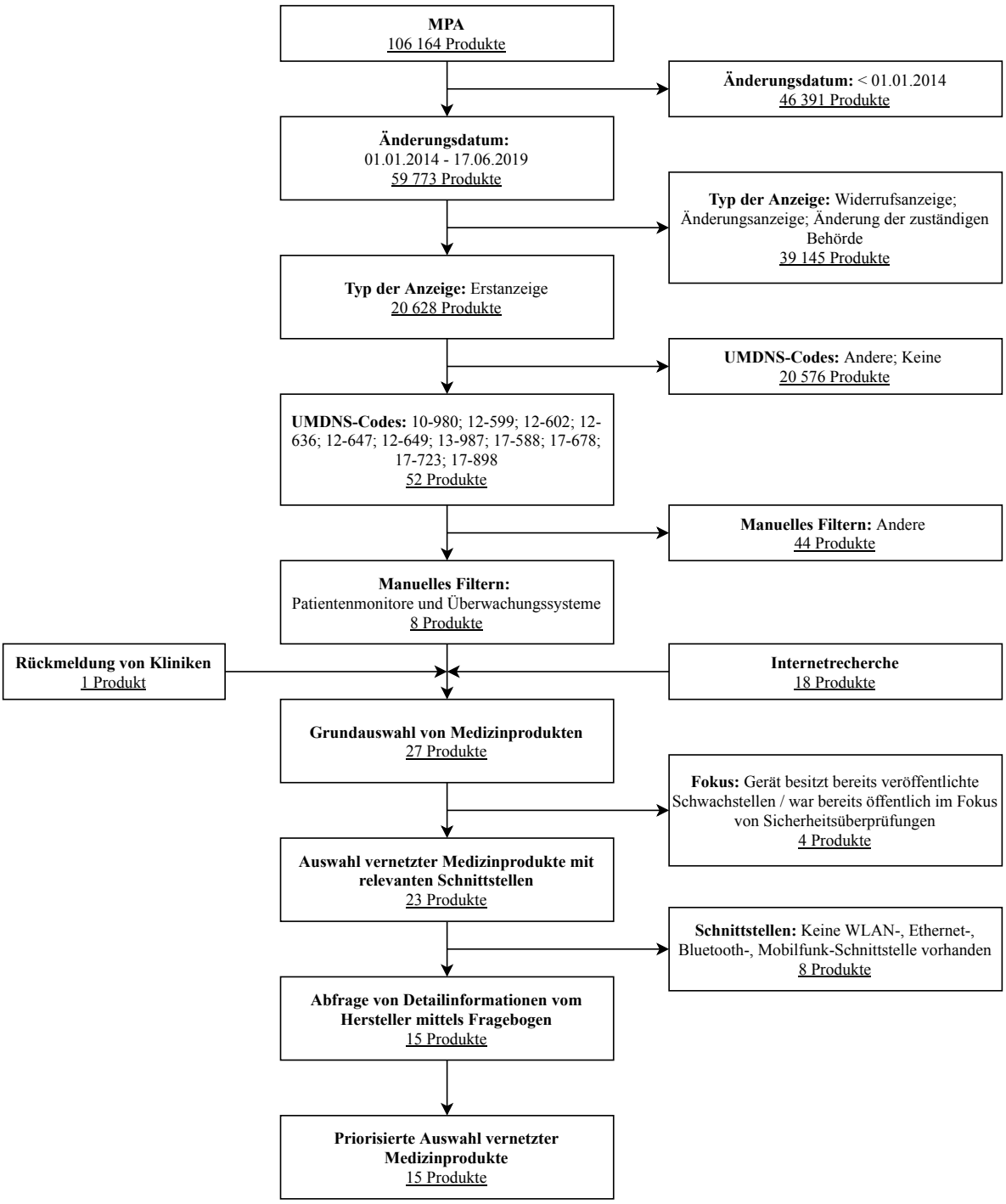

Abbildung 9: Flussdiagramm zur Veranschaulichung des Auswahlverfahrens für Patientenmonitore.

4 Ergebnisse der IT-Sicherheitsuntersuchungen

In diesem Abschnitt werden sowohl der Umfang der IT-Sicherheitsprüfungen, als auch die jeweiligen Ergebnisse nach Kategorien geordnet dargestellt. Die Reihenfolge entspricht nicht der Reihenfolge der Prüfungen. Nach einer kurzen Charakterisierung der Einsatzumgebung des Medizinprodukts und des medizinischen Verwendungszwecks werden die identifizierten Schwachstellen erläutert. In der Regel wurde ein Black-Box-Ansatz verfolgt. Um diesen Teil einem breiteren Publikum zugänglich zu machen (siehe Abschnitt 1.3), werden die Ergebnisse ohne technisch tiefergehende Details beschrieben. Es ist wichtig zu erwähnen, dass die meisten der aufgedeckten Schwachstellen die Patientensicherheit nicht beeinträchtigt haben und zum Zeitpunkt der Veröffentlichung dieses Berichts in den Geräten nicht mehr vorhanden sind. Die verbleibenden Schwachstellen sollen in den nächsten Monaten behoben werden, was hauptsächlich auf den Projektplan und erst kürzlich durchgeführte Prüfungen zurückzuführen ist.

Eine technische Erläuterung der jeweiligen Schwachstellen findet sich in den zugehörigen ICSMAs, den CVE und den veröffentlichten White Papers oder Blog-Einträgen sowie in den Vorträgen, die in Abschnitt 8.1 aufgeführt sind. Die Beurteilungsmethodik und das Festlegen des Testumfangs werden in Abschnitt 7 erläutert. Für jede Prüfung wurde ein Aufwand von etwa 20 Personentagen benötigt. Die Erfahrungen mit den CVD-Prozessen sind in Abschnitt 5 beschrieben.

Da es sich bei Medizinprodukten um streng regulierte Produkte handelt und sie nur von geschultem Personal bedient werden dürfen, muss erwähnt werden, dass die in diesem Projekt beurteilten Produkte in der Regel nicht privat erworben werden können. Folglich wurden im Projekt ManiMed Geräte entweder vom Hersteller mit einem Testvertrag zur Verfügung gestellt oder von Projektgeldern gekauft. Die Hersteller stellten die Mehrzahl der Geräte zur Verfügung. Der Umfang der zusätzlich übermittelten Informationen (Benutzerkonten, Firmware-Updates, Zubehör, Dokumentation, Quellcode, usw.) war bei allen Prüfungen unterschiedlich.

4.1 Untersuchte Produkte

In der folgenden Tabelle sind die Medizinproduktsysteme aufgeführt, die in diesem Projekt untersucht wurden. Jeder Hersteller entschied, ob er und das Produkt namentlich genannt werden dürfen oder ob er lieber anonym bleiben will.

Abschnitt	Hersteller	Produkt
4.2.2	Biotronik SE & Co. KG	Rivacor 7 VR-T DX, Renamic Neo, Cardio Messenger Smart
4.2.3	Medtronic plc	CareLink SmartSync Device Manager System
4.3.2	SOOIL Development Co., Ltd	DANA Diabecare RS, anyDANA-a, AnyDANA-i
4.3.3	Ypsomed AG	mylife YpsoPump, mylife App, mylife Cloud
4.4.2	Hamilton Medical AG	HAMILTON-T1
4.5.2	Innokas Yhtymä Oy	VC 150 Patient Monitor
4.5.3	Philips Medizin Systeme Böblingen GmbH	IntelliVue MX850, Patient Information Center iX
4.6.2	B. Braun Melsungen AG	SpaceCom, Infusomat Space, Perfusor Space
4.6.3	*Anonymer Hersteller*	*Infusionssystem #1*
4.6.4	*Anonymer Hersteller*	*Infusionssystem #2*
4.6.5	COPRA System GmbH	Copus (Copra Pump Management System)

Tabelle 2: Untersuchte Produkte

4.2 Implantierbare Herzschrittmacher und implantierbare Kardioverter-Defibrillatoren (ICDs)

In diesem Abschnitt werden, nach einer kurzen Beschreibung der Eigenschaften der Geräte und der Umgebung, in der sie eingesetzt werden, die Sicherheitsprüfungen von zwei Herzschrittmachern und ihren medizinischen Systemen erläutert.

4.2.1 Produktmerkmale und Nutzungsumgebung

Ein Standardschrittmacher stimuliert kontinuierlich den Herzmuskel und verursacht eine Herzkontraktion, wenn der Eigenrhythmus des Herzens langsam ist oder gänzlich fehlt. Im Gegensatz dazu überwacht ein implantierbarer Kardioverter-Defibrillator (ICD), ähnlich wie externe Defibrillatoren, den Eigenrhythmus des Herzens und gibt einen elektrischen Schock ab, um einen normalen Herzschlag wiederherzustellen. Im Folgenden werden im Zusammenhang mit dem Begriff Herzschrittmacher beide Geräte betrachtet. Herzschrittmacher werden in die höchste Risikoklasse III der Medizinprodukte (European Parliament and the Council of the European Union, 2017) eingestuft, da sie aktive, implantierbare medizinische Geräte sind und besondere funktionelle Anforderungen haben. Aufgrund der außergewöhnlichen Sicherheitsanforderungen sind während des gesamten Entwicklungsprozesses strenge Validierungs- und Verifizierungsschritte einzuhalten.

Herzschrittmacher werden in den Körper von Patienten implantiert und verfügen nicht über Benutzerschnittstellen oder ähnliche Konnektivität, die für die Verwendung durch Patienten vorgesehen sind. Bei periodischen Untersuchungen werden von Fachärzten Telemetrie- und Überwachungsprotokolle verwendet, um die Herzschrittmacher mit sogenannten Programmierern zu konfigurieren und zu parametrieren. Da die implantierten Herzschrittmacher nicht über kabelgebundene Verbindungen konfiguriert und ausgelesen werden können, erfolgt diese Kommunikation bei den Routineuntersuchungen über Funkfrequenzprotokolle mit niedriger Reichweite. Die entsprechenden Frequenzen liegen bei etwa 30

kHz für die induktive Nahfeldkommunikation oder im MICS-Band zwischen 402-405 MHz, das weltweit für die Kommunikation mit implantierbaren medizinischen Geräten reserviert ist. Manchmal erfolgt die Kommunikation über Bluetooth Low Energy (BLE). Neuere Geräte unterstützen die Übertragung von Telemetriedaten sowie von EKG-Messungen über sogenannte Home-Monitoring-Einheiten an einen Facharzt über das Internet.

4.2.2 Biotronik SE & Co. KG - Rivacor 7 VR-T DX, Renamic Neo, Cardio Messenger Smart

In diesem Abschnitt geht es um die IT-Sicherheitsprüfung des Herzschrittmachers Rivacor 7 VR-T DX, eines Prototypen des Programmiergeräts Renamic Neo, und der Home Monitoring Unit Cardio Messenger Smart, die medizinische Daten vom Herzschrittmacher an ein Cloud-Backend des deutschen Herstellers Biotronik SE & Co. KG (im Folgenden als Biotronik bezeichnet) weiterleitet.

4.2.2.1 Umfang des Tests

Die folgenden Geräte wurden getestet: Zwei Rivacor 7 VR-T DX-Herzschrittmacher, eine Renamic Neo-Programmiereinheit und die Cardio Messenger Smart Home Monitoring Unit. Im Rahmen der Prüfung wurden die exponierten Schnittstellen der verschiedenen Geräte sowie deren Kommunikation analysiert. Da die Geräte verschiedene Arten von Schnittstellen exponieren, mussten die Schnittstellen jeweils mit verschiedenen technischen Ansätzen geprüft werden. Das Cloud-Backend war nicht im Umfang der Prüfung enthalten.

Abbildung 10: Ein Biotronik Rivacor 7 VR-T DX. Herzschrittmacher (links), eine Biotronik Cardio Messenger Smart Home Monitoring Unit (Mitte), und ein Biotronik Renamic Neo Programmierer. (Quelle: Biotronik)

4.2.2.2 Ergebnisse

Bei der Prüfung des Programmiergeräts wurden einige Abstürze der Benutzeroberfläche festgestellt. Es ist anzumerken, dass es während der Prüfung nicht möglich war aus der Nutzeroberfläche auf das zugrundeliegende Betriebssystem auszubrechen. Somit wurde auf diese Weise keine Kontrolle über das Betriebssystem der Programmiereinheit erreicht.

Abgesehen von festgestellten Abstürzen ergab die Prüfung keine weiteren Probleme für die Programmiereinheit. Es ist anzumerken, dass das Testobjekt ein Produktprototyp war. Die identifizierten Abstürze sind daher wahrscheinlich mit dem Prototypzustand der Software verbunden.

Bei der Prüfung der Home Monitoring Unit konnten keine Schwachstellen festgestellt werden. Es ist anzumerken, dass diese Einheit nur eine kleine Angriffsfläche bietet. Diese Angriffsfläche besteht aus drei Teilen, einem USB-Port für die Stromversorgung, einem Modem für die mobile Kommunikation mit dem Cloud-Backend und einem Chip für die Funkkommunikation mit dem Herzschrittmacher. Die PIN der SIM-Karte der Home Monitoring Unit wurde durch Analyse der Kommunikation zwischen der Home Monitoring Unit und der SIM-Karte identifiziert.

Durch die Verwendung eines Faraday'schen Käfigs und einer Base Transceiver Station (BTS) war es möglich, die Home Monitoring Unit mit einer von den Prüfern kontrollierten GSM-Netzwerkinfrastruktur zu verbinden. Durch diesen Aufbau war es möglich, SMS direkt an das Gerät zu senden. Die gesendeten Nachrichten führten zu keinem ausnutzbaren Verhalten.

Die Prüfung konzentrierte sich auf die Kommunikation des Herzschrittmachers mit der Programmiereinheit und der Home Monitoring Unit. Die Prüfung ergab, dass der Herzschrittmacher die Daten des Herzmonitors über ein Radiofrequenzprotokoll an den Cardio Messenger Smart und den Renamic Neo übertrug. Zur Konfiguration des Herzschrittmachers mit dem Programmierkopf ist ein niederfrequentes Signal erforderlich. Mit einem Software Defined Radio (SDR) ist es möglich, beliebige Signale zu erfassen und diese mittels digitaler Signalverarbeitungstechniken (DSP) zu demodulieren. Für diesen Aufbau wurde eine USRP mit speziellen LFRX/LFTX Boards zusammen mit einer Ferritschleifenstabantenne zur Erfassung der Niederfrequenzsignale verwendet.

4.2.2.3 Auswirkungen

Aufgrund der Komplexität des Reverse Engineerings eines nicht standardisierten Funkprotokolls war es nicht möglich, das Funkprotokoll neu zu implementieren oder die Funkkommunikation während der Prüfung nach Aufzeichnung erneut abzuspielen. Insgesamt wurden keine Schwachstellen von mittlerer oder hoher Kritikalität identifiziert. Der Hersteller hat alle Probleme, die zu Systemabstürzen führten, innerhalb kurzer Zeit behoben und keine Auswirkungen auf die Patientensicherheit festgestellt.

4.2.3 Medtronic plc - CareLink SmartSync Device Manager System

In diesem Abschnitt geht es um die Sicherheitsprüfung von zwei Medtronic Azure-Herzschrittmachern und dem CareLink SmartSync Device Manager-System des amerikanisch-irischen Herstellers Medtronic plc (im Folgenden Medtronic genannt). Das System ermöglicht es Ärzten Bluetooth-fähige implantierte Herzgeräte mit einer iPad-App zu programmieren und zu überwachen.

4.2.3.1 Umfang des Tests

Bei den getesteten Systemen handelte es sich um das Medtronic CareLink SmartSync Device Manager-System mit zwei Azure-Herzschrittmachern, den Patientenkonnektor und die Basis des CareLink

SmartSync Device Managers sowie das zugehörige iPad und die mobile Anwendung. Im Rahmen der Untersuchung wurden die exponierten Schnittstellen der verschiedenen Geräte sowie deren Kommunikation analysiert. Da die Geräte mehrere verschiedene Arten von Schnittstellen exponieren, mussten die Schnittstellen mit verschiedenen Werkzeugen untersucht werden. Das Cloud-Backend war nicht im Umfang es Tests enthalten. Der Hersteller stellte neben den Geräten auch Handbücher, Firmware-Updates sowie den Quellcode für die iPad-App, den Patientenkonnektor und die Basis zur Verfügung.

4.2.3.2 Ergebnisse

Bei der Prüfung des Medizinprodukte-Ökosystems konnten drei Pufferüberläufe (buffer overflow) im Patientenkonnektor sowie ein Integer-Überlauf identifiziert werden. Die Überläufe könnten zu Problemen, wie Segmentierungsfehlern führen, wenn das Programm versucht zu Speicheradressen zu springen, die keine gültigen Anweisungen oder Speicherbereiche enthalten und auf die nicht zugegriffen werden darf. Das Überschreiben von Kontrollflussdaten könnte auch ausgenutzt werden, um die Kontrolle über die Anwendung zu übernehmen.

Die Wahrscheinlichkeit einer erfolgreichen Ausnutzung hängt in hohem Maße von den Maßnahmen zur Verhinderung der Ausnutzung dieser Überläufe ab. Das Vorhandensein dieser Funktionen konnte während der Prüfung jedoch nicht überprüft werden. Eine Überprüfung des Quellcodes ergab, dass die anfällige Komponente eine Berechnung auf der Grundlage von Benutzereingaben durchführt, um zu bestimmen, wie viel Speicher für einen Puffer zuzuweisen ist. Bei großen Werten kann es zu einem Integer-Überlauf kommen.

Abbildung 11: Das Testlabor des Medtronic CareLink SmartSync Device Manager-Systems, bestehend aus der Basiseinheit (rechts), einem Handheld (unten Mitte) und einem iPad mit der App (links) sowie einem Herzschrittmacher (oben Mitte). (Quelle: BSI)

4.2.3.3 Auswirkungen

Ergebnisse wurden im Rahmen eines Code Reviews ermittelt. Eine Beurteilung, ob die Schwachstellen ausgenutzt werden können, wurde nicht durchgeführt. Nach Angaben des Herstellers hindern die bestehenden Sicherheitsmechanismen Angreifer daran, die identifizierten Schwachstellen auszunutzen. Der Hersteller stellte kein Risiko für Patienten fest und stellte ein Update für das System zur Verfügung, wodurch alle gemeldeten Schwachstellen behoben wurden.

4.3 Insulinpumpen

In diesem Abschnitt werden die Sicherheitsprüfungen von zwei Insulinpumpen und ihren medizinischen Systemen nach einer kurzen Beschreibung der Eigenschaften der Geräte skizziert.

4.3.1 Produktmerkmale und Nutzungsumgebung

Eine Insulinpumpe ist ein aktives medizinisches Gerät, das zur Verabreichung von Insulin bei der Behandlung von Diabetes mellitus (Typ-1-Diabetes) verwendet wird. Diabetes mellitus ist eine Autoimmunkrankheit und beruht auf dem Mangel an Insulin aufgrund der Zerstörung der insulinproduzierenden Beta-Zellen in den Langerhans-Inseln der Bauchspeicheldrüse. Eine Insulinpumpe ist, im Gegensatz zu mehrfachen täglichen Insulininjektionen, eine weniger invasive Alternative und ermöglicht eine flexiblere Insulintherapie. Die kontinuierliche subkutane Insulininfusionstherapie (CSII) mit Insulinpumpen zielt darauf ab, eine automatisierte und bedarfsgerechte Insulinabgabe über dünne Schläuche subkutan, ohne Injektionen, zu ermöglichen. Nach Angaben des von der Deutschen Diabetes-Gesellschaft (DDG) veröffentlichten Gesundheitsberichts Diabetes 2020 (DDG, 2019) leben in Deutschland schätzungsweise 32.000 Kinder und Jugendliche sowie 340.000 Erwachsene mit Typ-1-Diabetes. Es wird geschätzt, dass etwa 45.000 Menschen in Deutschland eine Insulinpumpe nutzen, aber zuverlässige Quellen für diese Zahl fehlen.

4.3.2 SOOIL Development Co., Ltd. – DANA Diabecare RS System

Dieser Abschnitt beschreibt die Sicherheitsprüfung des Insulinpumpensystems DANA Diabecare RS des koreanischen Herstellers SOOIL Development Co., Ltd. (im Folgenden SOOIL genannt).

Die Insulinpumpe DANA Diabecare RS ist die zentrale Komponente dieses Therapiesystems und kann mit einer Applikation für die mobilen Betriebssysteme Android und iOS über eine Bluetooth Low Energy (BLE)-Schnittstelle angesteuert werden. Das Gerät ist nicht für den Einsatz in Closed-Loop-Systemen vorgesehen.

4.3.2.1 Umfang des Tests

Die Untersuchung umfasste das Bluetooth Low Energy (BLE) Kommunikationsprotokoll der SOOIL DANA Diabecare RS Insulinpumpe und die mobilen AnyDANA Anwendungen. Die Prüfung war ein Black-Box-Penetrationstest ohne Quellcode. Für den Test standen zwei Pumpen des Herstellers zur Verfügung sowie öffentlich zugängliche Dokumentation.

4.3.2.2 Ergebnisse

Während der Prüfung wurden verschiedene Probleme identifiziert, die die Sicherheit dieses Geräts beeinträchtigen könnten. Zunächst wird im Handbuch des Geräts empfohlen, schwache PINs für die

Bildschirmsperre des Geräts zu verwenden, um die Nutzung zu vereinfachen. Darüber hinaus haben alle Pumpen dieselbe Standard-PIN gesetzt. Die von den Benutzern gewählte PIN wird auch ohne Authentifizierung über die Bluetooth Low Energy (BLE)-Schnittstelle bekannt gegeben. Ein Angreifer mit physischem Zugang zur Pumpe und im Besitz der PIN ist in der Lage, eine Pumpe zu entsperren, die Pumpenkonfiguration zu ändern und einen Insulinbolus zu verabreichen. Darüber hinaus ist die Arzt-PIN für den Zugriff auf das Arztmenü der Pumpe für alle Pumpen gleich und kann ohne Kontaktaufnahme mit dem Support nicht geändert werden. Ein Angreifer mit Zugriff auf diese PIN und physischem Zugang zu einer Pumpe ist in der Lage, die Konfiguration der Pumpe, wie z. B. die maximale tägliche Insulindosis, zu ändern.

Außerdem wurden mehrere Prüfungen identifiziert, die nur durch die mobilen Anwendungen durchgeführt werden und daher umgangen werden können. Die PIN für die Tastatursperre des Geräts wird nur von mobilen Anwendungen validiert, nicht aber von der Pumpe selbst. Ein Angreifer kann die Überprüfung bei der Kommunikation mit der Pumpe auslassen.

Alle kryptographischen Schlüssel und ihr Schlüsselmaterial, das für die Verschlüsselung von BLE-Nachrichten auf Anwendungsebene verwendet wird, werden deterministisch, z. B. in Abhängigkeit von der Uhr der Insulinpumpe generiert und über Klartext-BLE-Nachrichten übertragen. Zudem beruht die Authentifizierung der kommunizierenden Partei nur auf dem Besitz des Pairing-Keys, der ebenfalls bei jeder Kommunikationsinitiierung im Klartext übertragen wird. Darüber hinaus verfügt das zusätzlich zur BLE implementierte Protokoll über keine Maßnahmen gegen das erneute Abspielen von Kommunikationsmitschnitten.

Eine detaillierte technische Diskussion der Ergebnisse der Prüfung kann einem öffentlichen Paper (Suleder, 2020) sowie einem Video, das die Ausnutzung der Schwachstellen zeigt, entnommen werden (ERNW Research GmbH, 2020).

4.3.2.3 Auswirkungen

Die Kombination der identifizierten Schwachstellen versetzt einen Angreifer in die Lage die Insulinpumpe zu übernehmen. Um einen Angriff durchzuführen, muss sich ein Angreifer in unmittelbarer Nähe der Insulinpumpe aufhalten und die Kommunikation zwischen einer DANA Diabecare RS-Insulinpumpe und einer verbundenen mobilen Applikation belauschen. Ein Pairing auf BLE-Ebene ist nicht erforderlich. Danach können Angreifer alle Funktionalitäten nutzen, die über BLE bereitgestellt werden. Der Hersteller räumte ein, dass dies die Patientensicherheit beeinflussen kann.

Abbildung 12: Die Insulinpumpe DANA Diabecare RS, nachdem ein Angreifer die BLE-Sitzung übernommen und mehrere Insulinboli verabreicht hat (veranschaulicht durch blaue Tinte). (Quelle: ERNW)

Der Hersteller stellte umgehend ein Update für die Insulinpumpe zur Verfügung, wodurch alle identifizierten Schwachstellen behoben wurden. Die Field Safety Notice (FSN) wurde im März angekündigt und im Mai 2020 durch das BfArM (SOOIL Development Co. Ltd, 2020) aktualisiert. Um potentielle Risiken mit Bezug auf die Patientensicherheit vorübergehend zu verringern, empfahlt der Hersteller, die BLE-Funktionalität der Insulinpumpe zu deaktivieren, indem sie in den Flugmodus versetzt wird. Im Flugmodus kann der therapeutische Zweck der Insulinpumpe erhalten bleiben, da die Steuerung des Geräts über die mobile Anwendung optional ist. Darüber hinaus ist zu beachten, dass das Gerät zusätzliche Sicherheitseigenschaften, wie eine maximale Tagesdosis oder einen Bolusblock implementiert hat. Diese Einstellungen sind nur an der Pumpe konfigurierbar und können daher von einem Angreifer in unmittelbarer Nähe nicht umgangen werden.

4.3.3 Ypsomed AG – mylife YpsoPump System

In diesem Abschnitt wird die Sicherheitsprüfung des mylife YpsoPump-Systems des Schweizer Herstellers Ypsomed AG erläutert.

Die Insulinpumpe mylife YpsoPump ist die zentrale Komponente dieses Therapiesystems. Über eine Bluetooth Low Energy (BLE) Schnittstelle können Daten durch eine mobile Applikation, namens mylife App, für die Betriebssysteme Android und iOS ausgelesen werden. Die Pumpe kann nicht über BLE gesteuert werden und kann daher nicht zum Aufbau eines Closed-Loop-Systems verwendet werden. Die mylife App kann Daten an die mylife Cloud übertragen. Das System, das eine Webanwendung anbietet, soll die Kommunikation zwischen Diabetikern und medizinischem Fachpersonal mit der mylife Therapiemanagement-Lösung für Therapiedaten erleichtern.

4.3.3.1 Umfang des Tests

Die Prüfung konzentrierte sich auf das Kommunikationsprotokoll zwischen der mylife YpsoPump und der mylife Android App, die aus dem Google PlayStore bezogen wurde sowie auf die Kommunikation zwischen der mylife App und dem mylife Backend. Das mylife Backend und ein entsprechendes Web-Frontend standen nicht im Mittelpunkt der Prüfung. Zwei Insulinpumpen wurden vom Hersteller zur Verfügung gestellt, ebenso die Testzugänge und öffentlich zugängliche Dokumentation.

Abbildung 13: Eine der im Projekt ManiMed getesteten Ypsomed mylife YpsoPump Insulinpumpen. (Quelle: BSI)

4.3.3.2 Ergebnisse

Die Kommunikation zwischen der YpsoPump und der mylife App wird zusätzlich zu den BLE-Pairing-Mechanismen durch Nachweise authentifiziert, die aus öffentlich zugänglichen Informationen abgeleitet werden können. Darüber hinaus kann die Batterie der Pumpe durch nicht authentifizierte Bluetooth-GATT-Schreibvorgänge, durch welche die Pumpe vibriert, entleert werden.

Weitere Schwachstellen wurden in der Kommunikation zwischen der mylife App und dem mylife Backend identifiziert. Die mobile Anwendung und das Backend der Testumgebung kommunizierten über HTTP und übermittelten symmetrisch verschlüsselte Daten. In der Produktivinstanz erfolgte die Kommunikation über HTTPS, aber der HTTP-Endpunkt ohne Transportverschlüsselung war ebenfalls erreichbar. Der Schlüssel und der Initialisierungsvektor der symmetrischen Verschlüsselung waren im Code der mobilen Anwendung fest codiert.

Die verwendete Software und Komponenten von Drittanbietern sind teilweise veraltet und enthalten öffentlich bekannte Schwachstellen. Keine dieser Schwachstellen konnte jedoch während des Tests ausgenutzt werden. Außerdem fehlte eine Passwortrichtlinie für die mobile Anwendung und das Front-End. Beim Absenden des Registrierungsformulars wird ein Passwort-Hash zurückgegeben. Darüber hinaus konnte eine Reflexion des Benutzerpasswortes während des Anmeldeprozesses beim Downgrade der Verbindung von HTTPS auf HTTP beobachtet werden.

4.3.3.3 Auswirkungen

Die oben genannten Schwachstellen haben keinen Einfluss auf die Hauptfunktionen der Insulinpumpe. Eine Beeinträchtigung der mobilen Anwendung war zudem nicht möglich. Lediglich die Kommunikation zwischen der mobilen Anwendung und dem Backend war anfällig für Man-in-the-Middle-Angriffe. Viele der Schwachstellen wurden durch Konfigurationsänderungen behoben. Der Hersteller behob die Design- und Logikfehler, indem er das Backend, das Front-End und die mobilen Anwendungen kurzfristig aktualisierte. Der Hersteller stellte keinen Einfluss der Schwachstellen auf die Patientensicherheit fest.

4.4 Beatmungsgeräte

In diesem Abschnitt wird, nach einer kurzen Beschreibung der Eigenschaften des Geräts, die Sicherheitsprüfung eines Beatmungsgeräts beschrieben.

4.4.1 Produktmerkmale und Nutzungsumgebung

Beatmungsgeräte unterstützen Patienten, die aufgrund von Krankheit, Trauma, oder Medikamenten (z. B. Anästhetika) nicht selbstständig atmen können oder Unterstützung zur Aufrechterhaltung einer adäquaten Beatmung benötigen (WHO, 2011). Die einzelnen Geräte werden so gebaut, dass sie den Anforderungen für den stationären Einsatz in Krankenhäusern oder für den mobilen Einsatz gerecht werden. Die Geräte unterscheiden sich auch in ihren Fähigkeiten hinsichtlich der Beatmung von Erwachsenen, Kindern und Neugeborenen sowie in den möglichen Beatmungsmodi. Da Ausfälle schweren Einfluss auf die Patientensicherheit haben können, werden Beatmungssysteme als lebenskritische Systeme eingestuft. Es müssen Maßnahmen ergriffen werden, um eine hohe Zuverlässigkeit der Geräte, einschließlich ihrer Stromversorgung, zu gewährleisten. Die meisten Geräte verfügen über keine umfangreichen externen Kommunikationsschnittstellen, abgesehen von der Anschlussmöglichkeit für die Dokumentation an ein PDMS, z. B. über serielle Schnittstellen.

4.4.2 Hamilton Medical AG – HAMILTON-T1

Dieser Abschnitt erläutert die IT-Sicherheitsprüfung des HAMILTON-T1 Beatmungsgeräts des Schweizer Herstellers Hamilton Medical AG (im Folgenden Hamilton genannt). Das HAMILTON-T1 Beatmungsgerät ist ein tragbares Beatmungsgerät, das zur Verwendung in Krankenwagen, Hubschraubern und Flugzeugen zugelassen ist. Es existiert eine Konfiguration für den militärischen Einsatz.

4.4.2.1 Umfang des Tests

Neben dem HAMILTON-T1-Gerät stellte der Hersteller öffentlich zugängliche Handbücher und ein Firmware-Image zur Verfügung. Das Gerät verfügt über einen USB- und einen ungenutzten Ethernet-Anschluss.

4.4.2.2 Ergebnisse

Das HAMILTON-T1 verwendet einen PIN-Code, um in das Konfigurationsmenü des Geräts zu gelangen. Dieser Code ist im Handbuch zu finden. Durch den Zugang zum Konfigurationsmenü war es möglich, eine manipulierte Konfigurationsdatei über einen USB-Stick zu laden, was zu einem undefinierten Zustand des Geräts führte. Diese Konfigurationsdatei ist mit einer Prüfsumme gesichert. Die Prüfsumme für manipulierte Konfigurationen wird in einem Fehlerprotokoll offengelegt, das für Angreifer zugänglich ist. Alle Angriffe erfordern physischen Zugriff.

Abbildung 14: Ein HAMILTON-T1 Beatmungsgerät. (Quelle: Hamilton)

4.4.2.3 Auswirkungen

Die identifizierten Schwachstellen führten zu einer Funktionsstörung des Geräts. Infolgedessen konnte das Gerät nicht gestartet werden. Zur Wiederherstellung der Funktionsfähigkeit des Beatmungsgeräts war ein Hardware-Austausch des Logik-Platine des Geräts erforderlich. Der Hersteller identifizierte kein Risiko in

Bezug auf die Patientensicherheit. Der Hersteller stellte ein Update für das Beatmungsgerät zur Verfügung, wodurch alle kritischen Schwachstellen behoben wurden.

4.5 Patientenmonitore

In diesem Abschnitt werden, nach einer kurzen Charakterisierung der Eigenschaften der Geräte, die Sicherheitsprüfungen von zwei Patientenmonitoren und ihren medizinischen Systemen skizziert.

4.5.1 Produktmerkmale und Nutzungsumgebung

Patientenüberwachungslösungen werden zur kontinuierlichen Messung von Vitalparametern während des Transports oder Krankenhausaufenthalts von Patienten eingesetzt. Die Konnektivität und Merkmale, wie Datenspeicherung, Alarmfunktionalität und Anbindung an zentrale medizinische Informationssysteme der vermarkteten Produkte, unterscheiden sich je nach Anwendungsfall.

Patientenmonitore, die in Krankenwagen genutzt werden, sind meist nicht vernetzt und werden vom Rettungspersonal eingesetzt, um die aktuellen Vitalparameter von Patienten zu beurteilen und zu alarmieren, wenn diese Werte vorgegebene Bereiche überschreiten.

Im klinischen Umfeld werden Patientenmonitore darüber hinaus dazu verwendet, die Vitaldaten von Patienten in elektronischen Gesundheitsakten zu dokumentieren und medizinischem Fachpersonal zu helfen, fundierte Entscheidungen zu treffen. Solche Systeme zur kontinuierlichen Patientenüberwachung können in komplexen Überwachungseinrichtungen auf Intensivstationen, in Operationssälen, bei der Diagnostik oder bei der Basisüberwachung am Krankenbett eingesetzt werden. Es gibt verschiedene Produkte für den tragbaren und stationären Einsatz sowie komplexe vernetzte Systeme mit automatischer Übergabe zwischen verschiedenen Bildschirmen in Behandlungsräumen, für die Langzeitdatenanalyse und Konnektivität zu Beatmungs- und Anästhesiegeräten. Für komplexere Umgebungen werden oft spezielle Infrastrukturen, z. B. für die Datenspeicherung und die Netzwerke, benötigt.

4.5.2 Innokas Yhtymä Oy – VC150 Patient Monitor

In diesem Abschnitt wird die Sicherheitsprüfung des VC150-Systems des finnischen Herstellers Innokas Yhtymä Oy erläutert. Der VC150 Patientenmonitor ist für die Überwachung der Vitalparameter eines einzelnen Patienten oder während des innerklinischen Transports vorgesehen. Der VC150 Patientenmonitor stellt eine kleine und tragbare Alternative für stationäre und ambulante Anwendung dar. Der Monitor ist zur Verwendung bei erwachsenen, pädiatrischen oder neonatalen Patienten vorgesehen.

4.5.2.1 Umfang des Tests

Der Hersteller stellte Handbücher und eine Firmware-Update-Datei zur Verfügung. Im Rahmen der Prüfung wurde die Netzwerkfunktionalität des Geräts bewertet, die Protokolle, wie HL7 v2.x und die administrative Web-Schnittstelle sowie die auf dem Touchscreen des Geräts dargestellte Benutzeroberfläche, umfasste. Ein Labor mit einer HL7 v2.x-Messaging-Engine wurde eingerichtet, um die Schnittstelle testen zu können.

4.5.2.2 Ergebnisse

In der administrativen Web-Schnittstelle des VC150 wurde eine Stored-Cross-Site-Scripting-Schwachstelle identifiziert. Außerdem kann das Gerät per Tastendruck abgeschaltet werden. Ein Angreifer mit einem

einmaligen physischen Zugriff auf die USB-Anschlüsse kann so das System neu starten und die vom Patientenmonitor durchgeführten Messungen unterbrechen.

Das Gerät sendet HL7 v2.x-Nachrichten, wie z. B. Beobachtungsergebnisse, an HL7 v2.x-fähige elektronische Krankenakten-Systeme (EMR). Ein Benutzer mit böswilligen Absichten kann diese Nachrichten manipulieren, indem er mit einem angeschlossenen Barcode-Lesegerät HL7 v2.x-Segmente in die HL7 v2.x-Nachrichten injiziert. Somit können Angreifer Daten manipulieren, die an über das Netzwerk verbundene Systeme übertragen werden. Diese identifizierte Schwachstelle wird in einem im April 2020 veröffentlichten Blog-Beitrag detaillierter beschrieben (Suleder, 2020).

4.5.2.3 Auswirkungen

Angreifer können nicht vollständige HL7 v2.x-Nachrichten injizieren. Außerdem können Angreifer die Ziele der Nachrichten nicht kontrollieren. Es ist zu beachten, dass HL7 v2.x-Nachrichten so spezifiziert sind, dass sie nur eine begrenzte Teilmenge aller verfügbaren HL7 v2.x-Nachrichtensegmente enthalten. Netzwerkverbundene Systeme validieren normalerweise empfangene Nachrichten. Daher ist es Angreifern unter Umständen nur möglich, diese ausgewählten Segmente in eine Nachricht zu injizieren. Dies ermöglicht es jedoch den Angreifern, die sich der HL7 v2.x-Nachrichtenstrukturen bewusst sind, willkürliche Beobachtungsergebnisse zu injizieren, was zu Fehldiagnosen oder medizinischen Fehlern führen kann. Der Hersteller identifizierte kein Patientenrisiko, implementierte Korrekturen und stellte ein Update zur Verfügung.

4.5.3 Philips Medizin Systeme Böblingen GmbH – IntelliVue System

In diesem Abschnitt wird die Sicherheitsprüfung des IntelliVue-Systems der Philips Medizin Systeme Böblingen GmbH (im Folgenden Philips genannt), einer deutschen Tochtergesellschaft des niederländischen Herstellers Koninklijke Philips N.V., erläutert.

Philips IntelliVue Patientenmonitore sind für die Überwachung und Aufzeichnung mehrerer physiologischer Parameter von Erwachsenen, Kindern und Neugeborenen sowie zur Erzeugung von Alarmen für diese Parameter vorgesehen. Das Philips Patient Information Center iX (PIC iX) ist eine Echtzeit-Patientenüberwachungslösung, die physiologische Daten von Patientenmonitoren und klinischen Informationssystemen zusammenführt. Dieses Überwachungssystem ist für den Einsatz in professionellen Gesundheitseinrichtungen durch geschultes medizinisches Fachpersonal vorgesehen. Es ist nicht für den Heimgebrauch vorgesehen.

Das IntelliVue-System ermöglicht nicht nur die Kommunikation zwischen Monitoren und dem Patient Information Center iX, sondern auch die Kommunikation zwischen einzelnen Monitoren untereinander.

4.5.3.1 Umfang des Tests

Im Rahmen der IT-Sicherheitsprüfung wurden die Kommunikation zwischen einer Patient Information Center iX Überwachungsstation und zwei IntelliVue MX850 Patientenmonitoren in einer gemeinsamen Netzwerkinfrastruktur untersucht. Die Betriebssystemhärtung des PIC iX-Server-Hosts sowie die bereitgestellte Netzwerkinfrastruktur waren nicht Gegenstand dieser Prüfung.

Abbildung 15: Ein Philips IntelliVue MX850 Patientenmonitor (links) sowie eine PIC iX-Überwachungsstation (Mitte + rechts). (Quelle: Philips)

4.5.3.2 Ergebnisse

Bei der Sicherheitsprüfung der Anwendung PIC iX-Überwachungsstation konnten mehrere Cross-Site-Scripting (XSS)-Schwachstellen identifiziert werden. Darüber hinaus konnte ein Kiosk-Ausbruch identifiziert werden. Aus der Netzwerkperspektive konnte die Anwendung über ein einzelnes, speziell ausgeprägtes Paket zum Absturz gebracht werden. Der Absturz führte zu einem Neustart der Anwendung. Ein weiterer persistenter Absturz konnte beim Zertifikatsregistrierungsdienst über SCEP beobachtet werden, indem manipulierte Certificate Signing Requests (CSR) an den Dienst gesendet wurden. Weiterhin ist dieser Dienst anfällig für einen praktischen Brute-Force-Angriff, der es Angreifern ermöglicht, vertrauenswürdige Zertifikate für die Verbindung mit Patientenmonitoren zu erhalten. Der erläuterte Absturz wirkt sich nur auf den Zertifikatsregistrierungsdienst aus, welcher ausschließlich bei der Registrierung neuer Geräte gestartet wird.

Der IntelliVue MX850 Patientenmonitor prüft Zertifikate nicht ausreichend auf einen potentiellen Widerruf, wodurch Angreifer mit Zugriff auf ein vertrauenswürdiges Zertifikat eine Man-in-the-Middle-Position (MitM) zwischen dem Patientenmonitor und der Serveranwendung erhalten können. Diese Position könnte dazu verwendet werden, den Patientenmonitor zum Absturz zu bringen oder möglicherweise sogar übertragene Daten zu modifizieren. Nach dem Absturz wird der Monitor neu gestartet, was etwa 20 Sekunden dauert. In dieser Zeit werden keine Vitalparameter gemessen und an die Patient Information Center iX Überwachungszentrale übertragen.

4.5.3.3 Auswirkungen

Durch Verkettung des Absturzes der PIC iX-Anwendung, der unsachgemäßen Überprüfung des Zertifikatswiderrufs durch den Patientenmonitor sowie des Absturzes des Monitors, kann ein Angreifer, der im Besitz eines gültigen Client-Zertifikats ist, einen anhaltenden Denial-of-Service-Angriff (DoS) auf das IntelliVue-Überwachungssystem durchführen. Philips hat bisher keine Berichte über die Ausnutzung dieser Probleme oder über Vorfälle aus der klinischen Anwendung erhalten, die mit diesem Problem in Zusammenhang stehen könnten. Der Hersteller identifizierte keine Meldungen über Risiken für Patienten.

Im Falle einer Unterbrechung der Überwachung besteht die Möglichkeit einer verzögerten Behandlung des Patienten. Doch um diese Schwachstellen erfolgreich auszunutzen, müsste sich ein Angreifer entweder physischen Zugang zu PIC iX Überwachungsstationen und Patientenmonitoren oder Zugang zum Netzwerk der medizinischen Geräte verschaffen. Der Hersteller bereitet die Veröffentlichung eines Updates zur Behebung der Schwachstellen vor.

4.6 Spritzen- und Infusionspumpensysteme

In diesem Abschnitt werden die Sicherheitsprüfungen von drei Spritzen- und Infusionspumpensystemen sowie einem Pumpenmanagementsystem nach einer kurzen Spezifizierung der Merkmale dieser Systeme vorgestellt.

4.6.1 Produktmerkmale und Nutzungsumgebung

Während der Therapie eines Patienten besteht häufig die Notwendigkeit Medikamente zu verabreichen. Viele dieser Medikamente müssen in einem bestimmten Dosisbereich verabreicht werden. Dieser Dosisbereich, in dem Medikamente am wirksamsten sind und keinen Schaden verursachen, wird in der Medizin als *therapeutisches Fenster* bezeichnet. Im Gegensatz zu manueller Verabreichung, streben Infusionssysteme danach, sichere Therapien zu gewährleisten und Dosisfehler zu beseitigen. Da Patienten unter Umständen mehrere Medikamente gleichzeitig erhalten, ist die Verabreichung mehrerer Medikamente an Patienten erforderlich. Genau hier kommen medizinische Spritzen oder großvolumige Pumpen ins Spiel. Spritzen- und Infusionspumpen sind aktive medizinische Geräte, mit denen Flüssigkeiten, wie Nährstoffe und Medikamente, in der richtigen Dosis, zur richtigen Zeit und in der richtigen Konzentration verabreicht werden, um den besten therapeutischen Nutzen zu gewährleisten. In Krankenhäusern sind diese Geräte oft in großer Stückzahl vorhanden.

Die Pumpen müssen zuverlässig und sicher sein, um Schädigungen oder sogar den Tod durch z. B. Überdosierung oder Luft im Schlauchsystem zu verhindern und sie müssen einfach zu bedienen sein, da oft mehrere Pumpen parallel arbeiten. Folglich darf nur geschultes medizinisches Personal diese Pumpen, die ihrerseits robuste Sicherheitsmechanismen und Alarmfunktionalitäten implementiert haben, bedienen und den Einsatz überwachen.

Die auf dem Markt verbreiteten Therapiesysteme bestehen aus Spritzen- und Infusionspumpen, die in einer Docking-Station (im Folgenden als Dock bezeichnet) zusammengefasst sind. Dieses Dock fungiert als Stromversorgung für die Pumpen und hat häufig eine gemeinsame Kommunikationsschnittstelle zum klinischen Netzwerk implementiert. Die verbreiteten Pumpen enthalten meist keine anderen Kommunikationsschnittstellen als diejenige, die zur Kommunikation mit dem Dock (beispielsweise über Infrarot) dient. Neuere Generationen intelligenter Infusionssysteme verfügen über verschiedene Kommunikationsschnittstellen wie z. B. WLAN. In den meisten Fällen ermöglicht ein zentrales Managementsystem die Überwachung und Konfiguration der Pumpen hinsichtlich des Transfers von Medikamentenbibliotheken und manchmal auch die Installation von Pumpen-Updates. Viele Systeme ermöglichen einen automatischen Datentransfer von verabreichten Medikamenten und Dosierungen zu angeschlossenen elektronischen Krankenakten (EMR).

4.6.2 B. Braun Melsungen AG – Space System

In diesem Abschnitt wird die Sicherheitsprüfung des Space Infusions- und Spritzensystems des deutschen Herstellers B. Braun Melsungen AG (im Folgenden B. Braun genannt) im Detail dargestellt.

Das B. Braun-Therapiesystem besteht aus verschiedenen Infusions- und Spritzenpumpen, die in Docks mit einem Kommunikationsmodul namens SpaceCom gruppiert sind. Eine zentrale Verwaltungssoftware namens OnlineSuite ermöglicht die Überwachung der Pumpen und die Konfiguration von Medikamentenbibliotheken.

4.6.2.1 Umfang des Tests

Bei den untersuchten Systemen handelte es sich um das SpaceCom-Kommunikationsmodul, zwei Infusomat Space Infusionspumpen und zwei Perfusor Space Spritzenpumpen sowie um eine zentrale Verwaltungssoftware namens Online Suite mit einer Lizenz mit vollem Funktionsumfang.

4.6.2.2 Ergebnisse

Während der IT-Sicherheitsprüfung wurden Probleme mit den Datei-Upload- und Datei-Download-Funktionen der OnlineSuite-Anwendung festgestellt. Diese Schwachstellen ermöglichten es unauthentifizierten Angreifern, beliebige Dateien von und zum OnlineSuite-Server hoch- und herunterzuladen. Diese Schwachstellen können ausgenutzt werden, um entweder einen Denial-of-Service-Angriff (DoS) der Webanwendung auszulösen oder um beliebigen Code auf dem Server auszuführen.

Abbildung 16: Das B. Braun Melsungen Space-System bestand aus einer SpaceStation mit einem SpaceCom-Kommunikationsmodul, einer Infusomat Space Infusionspumpe und drei Perfusor Space Spritzenpumpen. (Quelle B. Braun Melsungen AG)

In der administrativen Webschnittstelle der SpaceCom wurden mehrere Probleme bezüglich des Sitzungsmanagements und der Authentifizierung identifiziert. Die Anwendung ist anfällig für einen Session-Fixation-Angriff, der es einem Angreifer erlaubt, Session Tokens für Benutzer zu fälschen.

In der Webanwendung wurden mehrere Injektions-Schwachstellen wie zum Beispiel Cross-Site-Scripting (XSS) und nicht validierte Weiterleitungen identifiziert. Darüber hinaus ist die Anmeldeseite anfällig für XPath-Injektionen, die es Angreifern ermöglichen, Benutzernamen und Passwort-Hashes zu extrahieren. Eine authentifizierte Datei-Upload-Schwachstelle, in Kombination mit einem nicht validierten symbolischen Link und lokalen Privilegienerweiterungen, ermöglicht es Angreifern Befehle als Root-Benutzer auszuführen.

Firmware-Updates werden mit einem Hash, der im Header des Updates enthalten ist, vor Änderungen geschützt. Ein Angreifer kann Firmware-Updates manipulieren und eigenständig gültige Prüfsummen berechnen.

4.6.2.3 Auswirkungen

Die Schwachstellen führen zu einer Kompromittierung sowohl der OnlineSuite als auch des SpaceCom-Moduls. Angreifer könnten Angriffe auf weitere angeschlossene Systeme wie z. B. elektronische Krankenakten-Systeme (EMR) vorbereiten. Die Integrität oder Funktion der Infusions- und Spritzenpumpen wird nicht beeinträchtigt. Der Hersteller identifizierte kein Patentrisiko. Sowohl für die OnlineSuite als auch für das SpaceCom-Modul wurden Updates bereitgestellt.

4.6.3 Anonymisiertes Infusionssystem #1

In diesem Abschnitt wird die Sicherheitsprüfung eines Infusionssystems vorgestellt. Dieses System kann aus einer zentralen Managementkomponente, einem Dock und Infusionspumpen bestehen. Die Pumpen können auch unabhängig voneinander, ohne eine zentrale Managementkomponente, funktionieren. Das zentrale Management kann Informationen zu Infusionen von allen Pumpen und Docks sammeln und aggregieren. Das Dock ermöglicht die Gruppierung einzelner Pumpen und die Aktualisierung von Medikamentenbibliotheken an den Pumpen.

4.6.3.1 Umfang des Tests

Gegenstand der Prüfung war die Kommunikation innerhalb der Laborumgebung, die zwei Pumpen, zwei Docks sowie die zentralen Anwendungen und eine API umfasste. Nicht in den Umfang der Sicherheitsprüfung fielen die Härtung der vom Hersteller gelieferten Netzwerkumgebung sowie die Härtung des Server-Hosts.

4.6.3.2 Ergebnisse

Bei der Prüfung des Medizinproduktesystems wurden mehrere Schwachstellen identifiziert. Die Analyse der Pumpe ergab nur ein geringfügiges Problem. Für die API der zentralen Komponente wurde ein Directory Listing und die Offenlegung der Spezifikation der Web Services identifiziert.

Für das Dock wurden mehrere schwere Schwachstellen festgestellt. Es wird ein veralteter Webserver mit mehreren öffentlich bekannten Schwachstellen verwendet. Zusätzlich bietet das Dock sowohl eine durch Transportverschlüsselung geschützte, als auch eine ungeschützte Schnittstelle. Außerdem kann das Gerät durch nicht authentifizierte, speziell gestaltete HTTP-Anfragen unerreichbar gemacht werden. Die Stromversorgung des Geräts wird dadurch nicht beeinträchtigt. Darüber hinaus verfügt die Verwaltungsschnittstelle über ein unsicheres und defektes Session-Management sowie fehlende Zugriffskontrollen. Die Web-Anwendung implementiert Authentifizierungs- und Sitzungsverwaltungsmechanismen nur auf der Client-Seite und schützt daher die Authentifizierungsattribute nicht ausreichend.

Die von der zentralen Komponente verwendeten Webanwendungen sind anfällig für mehrere Cross-Site-Scripting (XSS)-Schwachstellen.

Darüber hinaus enthält eine Webanwendung festkodierte Anmeldeinformationen des Service-Benutzers. Das Front-End der Anwendung verweigert die Verwendung dieser Anmeldedaten mit Hilfe von Mechanismen, die nur auf der Client-Seite implementiert sind.

4.6.3.3 Auswirkungen

Nicht authentifizierte Angreifer, die entweder physischen Zugriff auf das Dock oder Zugriff auf das Krankenhausnetzwerk haben, können das Dock über speziell gestaltete HTTP-Anfragen dauerhaft unerreichbar machen. Keine der identifizierten Schwachstellen verursacht Schaden für den Patienten oder könnte zum Abgreifen von Pateienten- oder Gesundheitsdaten führen. Der Hersteller plant ein Update für Q1/2021 und will damit alle identifizierten Schwachstellen beheben.

4.6.4 Anonymisiertes Infusionssystem #2

Dieser Abschnitt beschreibt die IT-Sicherheitsprüfung eines Systems, das verschiedene Infusions- und Spritzenpumpen umfasst, die in Docks mit einem Kommunikationsmodul gruppiert werden können. Eine externe Kommunikationsschnittstelle ermöglicht die Überwachung von Pumpen und die Konfiguration von Medikamentenbibliotheken oder die kontinuierliche Übertragung von Infusionsdaten an klinische Systeme.

4.6.4.1 Umfang des Tests

Bei den untersuchten Systemen handelte es sich um das bereitgestellte Dock sowie um alle externen Schnittstellen, eine Spritzenpumpe und eine Infusionspumpe.

4.6.4.2 Ergebnisse

Bei der Prüfung des Medizingerätesystems wurden mehrere Schwachstellen identifiziert. Mehrere Pufferüberläufe, sowohl in den Netzwerkdiensten des Docks, als auch in der Firmware der Pumpe, konnten identifiziert werden. Grundlegende Funktionen zur Ausnutzung von Schwachstellen wie Position Independent Executable (PIE) und die Verwendung von Stack-Cookies fehlten. Außerdem wurden die Debug-Symbole nicht entfernt.

Bei der Kommunikation zwischen dem Gerät und mehreren Diensten wurde keine Transportverschlüsselung verwendet. Übermittelte Anmeldedaten wurden in einem reversiblen Format übertragen und gespeichert. Darüber hinaus prüfte das Dock auf Basis des zugrundeliegenden Protokolls nicht die Identität der kommunizierenden Parteien, wie zum Beispiel externer Informationssysteme.

4.6.4.3 Auswirkungen

Die Pufferüberläufe könnten dazu führen, dass Kontrollflussdaten überschrieben werden, um die Kontrolle über die Anwendung zu übernehmen und beliebigen Code auszuführen. Ein Angreifer könnte diese Schwachstelle ausnutzen, um das Programm zum Absturz zu bringen oder beliebigen Code auszuführen. Die Wahrscheinlichkeit einer erfolgreichen Ausnutzung hängt in hohem Maße von den vorhandenen Funktionen zur Erschwerung der Ausnutzung ab, die entweder in die Anwendung einkompiliert sind, wie z. B. nicht ausführbare Stacks oder Stack-Canaries, und von den Maßnahmen, die von der Ausführungsumgebung angewendet werden, wie z. B. die Adressraum-Layout-Randomisierung (ASLR). Ein Pufferüberlauf wurde während der Bewertung beispielhaft ausgenutzt, was zu nicht authentifizierter, Remote Code Execution (beliebiger Ausführung von Code) führte.

Der Hersteller hat in enger Zusammenarbeit sowohl mit dem Prüfteam als auch mit dem PDMS-Hersteller alle verbesserungsbedürftigen Punkte angesprochen und adressiert. Neben der Eliminierung der Pufferüberläufe wurden auch die Mitigationsfunktionen PIE, Stack-Cookies aktiviert und die Debug-Symbole entfernt.

Die fehlende Identitätsprüfung für die Kommunikation der Parteien im Protokoll zu externen Informationssystemen könnte es Angreifern ermöglichen, die Systeme mit vorgetäuschten Geräten zu überfluten und vorhandene Pumpen oder externe Systeme wie ein PDMS vorzutäuschen.

Es war keine Manipulation der Pumpen möglich, weder an den Infusionsparametern, noch am Infusionsstatus, noch an der Software oder den Einstellungen der Medikamentenbibliothek. Der Hersteller identifizierte kein Patientenrisiko.

4.6.5 COPRA System GmbH – Copus (Copra Pump Management System)

In diesem Abschnitt wird die Prüfung des Pumpenmanagementsystems "Copus" des deutschen Herstellers COPRA System GmbH (im Folgenden als COPRA bezeichnet) detailliert beschrieben.

Das Pumpenmanagementsystem, das als Middleware zwischen Pumpensystemen von Drittanbietern und einem PDMS arbeiten soll, bietet eine Vielzahl von externen Kommunikationsschnittstellen, die es ermöglichen, Pumpen zu überwachen und Infusionsdaten kontinuierlich an klinische Systeme zu übertragen.

4.6.5.1 Umfang des Tests

Bei den untersuchten Systemen handelte es sich um die Copus REST- und Websocket-APIs, Copus WardViewer, Copus Cockpit-Anwendung und eine externe Schnittstelle zu einem Infusionspumpensystem.

4.6.5.2 Ergebnisse

Bei der Prüfung des Pumpenmanagementsystems, das sich zum Zeitpunkt der Bewertung noch im Prototypenzustand befand, wurden mehrere Schwachstellen identifiziert.

Die REST-API unterstützt keine Transportverschlüsselung, und die Authentifizierung gegenüber dem Dienst ist nur über HTTP Basic Authentication möglich. Außerdem wurde eine API für die Websocket-Kommunikation identifiziert, die nicht authentifiziert ist.

Darüber hinaus wurden festkodierte Benutzeranmeldeinformationen für diese Dienste identifiziert, die zur automatischen Authentifizierung gegenüber der REST-API mit der Copus WardViewer-Anwendung verwendet werden. Es sei nochmals darauf hingewiesen, dass der Prüfgegenstand ein Produktprototyp war. Diese Mechanismen sind wahrscheinlich mit dem Prototypenzustand der Software verbunden.

Zusätzlich zu diesen Erkenntnissen konnte eine Schwachstelle bezüglich des Protokolls zwischen den Docks und dem Informationssystem Copus identifiziert werden. Das Copus-Cockpit hat keine Möglichkeit, die Identität der kommunizierenden Parteien zu überprüfen. Zudem fehlt dieser Schnittstelle die Möglichkeit zur Transportverschlüsselung. Diese Ergebnisse können nicht allein der Copus-Schnittstelle zugeschrieben werden, da auf der Client- und Serverseite größere Designänderungen in der Schnittstellenspezifikation vorgenommen werden müssten.

4.6.5.3 Auswirkungen

Das Copus-Cockpit hat keine Möglichkeit, die Identität der kommunizierenden Parteien zu überprüfen. Server können durch Angreifer mit falschen Docks überflutet werden und vorhandene Pumpen können von einem Angreifer vorgetäuscht werden. Dies kann zu manipulierten Infusionsdaten führen, die im Copus dokumentiert und an angeschlossene PDMS-Systeme weitergeleitet werden. Die Übertragung von Daten im Klartext könnte es Dritten ermöglichen, auf sensible Informationen, wie z. B. Pumpen- und Infusionsdaten

zuzugreifen. Die Schwachstellen in den Copus-Authentifizierungsmechanismen über die REST- und WebSocket-APIs sowie die Umgehung der Authentifizierung über festkodierte Anmeldedaten könnten ebenfalls unbefugten Dritten den Zugriff auf sensible Informationen, z. B. Pumpen- und Infusionsdaten, ermöglichen.

All diese Probleme wurden von COPRA und dem Hersteller des Infusionssystems während der Evaluationsphase analysiert und teilweise direkt gelöst. In einem ersten Konzept wurde die Kommunikation zwischen den Docks und Copus verschlüsselt und durch Client- und Server-Zertifikate gesichert.

Darüber hinaus wurden alle kritischen Informationen, wie z. B. Zugangsdaten, aus den Softwareprodukten entfernt. Für die COPRA-interne Kommunikation wird in Zukunft das HTTPS- oder WSS-Protokoll für verschlüsselte Kommunikation verwendet. Darüber hinaus werden alle für die Kommunikation verwendeten Schlüssel durch neue ersetzt.

Keine der identifizierten Schwachstellen kann die Sicherheit eines Patienten beeinflussen. Die meisten Schwachstellen wurden sofort behoben.

5 Erfahrungen aus CVD-Prozessen

In diesem Abschnitt werden die Erfahrungen aus elf koordinierten Veröffentlichungsprozessen, (Coordinated Vulnerability Disclosure Processes, CVDs) im Projekt ManiMed beschrieben und in drei verschiedene Kategorien bezüglich der Reife im Umgang mit identifizierten Schwachstellen unterteilt und nachfolgend vorgestellt.

Nach den Erfahrungen der Autoren erleichtern und vereinfachen geeignete CVD-Rahmenwerke und -Regeln die Prozesse, insbesondere wenn der Hersteller keine Kenntnis von ebendiesen hat. Dieses Rahmenwerk sollte einen Leitfaden zur Einrichtung sicherer Kommunikationskanäle durch den Austausch von S/MIME-Zertifikaten oder PGP-Schlüsseln enthalten. Ferner können Regeln für die Zusammenarbeit festgelegt werden, z. B. Fristen für die Beantwortung von Anfragen, beteiligte Personen und eine Rolle als "Manager des CVD-Prozesses". Statussitzungen sollten regelmäßig geplant werden. Im Idealfall stellt jeder Hersteller aktiver Medizinprodukte öffentliche Kontaktinformationen zur Verfügung, um Schwachstellen zu melden und effiziente CVD-Prozesse zu ermöglichen.

Es sollten Prozessergebnisse, wie eine eingehende Analyse der gemeldeten Schwachstellen, vorgeschlagene Behebungen oder Schadensminimierungen, eine Analyse des Restrisikos und ein Zeitplan für die Entwicklung und Einführung des Patches festgelegt werden. Die Parteien sollten sich im späteren Prozess auf Veröffentlichungen der Schwachstellen und andere öffentliche Mitteilungen, wie Advisories einigen. Ferner kann eine genaue Erklärung über Behebungen und Schadensminimierungen auf rein technischer Ebene den Herstellern helfen, die gefundenen Schwachstellen zu beheben. Dies und die oben genannten Punkte können bei jedem CVD-Prozess unterschiedlich sein. Hersteller, die mit diesen Prozessen vertraut sind und bereits über ein ausgereiftes Verfahren oder einen Rahmen für den Umgang mit Schwachstellen verfügen, erleichtern den CVD-Prozess. Häufig veröffentlichen Hersteller eine koordinierte Erklärung zum CVD von Schwachstellen, in der sie auf Regeln, Verfahren und Verpflichtungen der Hersteller hinweisen, sodass die meldenden Parteien wissen, was sie zu erwarten haben.

Bei Medizinprodukten müssen die Hersteller analysieren, ob gemeldete Sicherheitslücken die wesentliche Leistung des Geräts oder die Patientensicherheit beeinträchtigen können. Sicherheitsforscher können beobachtetes unbeabsichtigtes Geräteverhalten nachweisen, aber allein der Hersteller kann und darf die Bewertung des Sicherheitsrisikos durchführen.

Theoretisch konnten im Verlauf des Projekts ManiMed drei verschiedene Kategorien hinsichtlich der Reife des Veröffentlichungsprozesses beobachtet werden. Obwohl diese verschiedenen Kategorien eine gewisse Unterscheidbarkeit nahelegen, lagen die tatsächlichen Erfahrungen mit einzelnen Herstellern zwischen verschiedenen Kategorien. Insbesondere konnten Veränderungen im Laufe der Zeit beobachtet werden. Einige Hersteller starteten gut und zeigten eine hohe Reife im Umgang mit Veröffentlichungsprozessen, aber gegen Ende veränderten sich die Kommunikation und Beteiligung erheblich. Andere wiederum begannen mit erheblichen Schwierigkeiten, überzeugten aber gegen Ende durch einen vorbildlichen Umgang mit Schwachstellen. Insgesamt zeigt das Projekt, dass alle teilnehmenden Hersteller großen Wert auf Sicherheit, Gefahrenabwehr und kontinuierliche Verbesserung legen und nicht abgeneigt waren, ihre eigenen Prozesse in Frage zu stellen.

5.1 Kategorie 1: Hoher Reifegrad

Bei dieser Art von CVD-Prozessen sind die Hersteller erfahren oder vertraut mit CVD-Prozessen. Sie haben das Know-how, um die Analyse intern zu koordinieren, ungeplante Bugfixes und Sicherheitspatches zu implementieren und auszurollen. Angemessene Zeitpläne der CVD-Aufgaben und weiterer Schritte werden vorgestellt sowie proaktiv Kontaktpersonen festgelegt. In den meisten Fällen sind explizit Mitarbeiter beteiligt, die das CVD-Verfahren überwachen und koordinieren. Es wird eine schnelle Antwort, einschließlich detaillierter technischer Beschreibungen der Behebungspläne, vorgelegt. Der Prozess wird vom Hersteller selbst vorangetrieben und erfordert keine weiteren externen Impulse durch das Projektteam. Die diskutierten Themen sind die Publikation, die Zuweisung von CVEs und die Veröffentlichung eines Security Advisories.

5.2 Kategorie 2: Mittlerer Reifegrad

Hier geben die Hersteller in der Regel zu, unerfahren mit den jeweiligen Prozessen zu sein und bitten um entsprechende Hilfe. Das Projektteam stellt sowohl den technischen Teams als auch den Entscheidungsträgern Informationen über die Prozesse zur Verfügung. Manchmal ist ein besonderes Coaching erforderlich, z. B. um zu erklären, warum die Freigabe von Patches für Medizinprodukte-Ökosysteme, die bald abgelöst würden, immer noch eine nicht zu vernachlässigende Option sein kann und in bestimmten Fällen sogar notwendig ist. Die Prozesse basieren auf professioneller und transparenter Kommunikation. Am Ende stellen die freigegebenen Patches eine technisch angemessene und saubere Behebung aller identifizierten Schwachstellen in einer längeren, aber angemessenen Zeit dar.

5.3 Kategorie 3: Niedriger Reifegrad

Die Unerfahrenheit im Umgang mit Sicherheitslücken ist in dieser Kategorie sehr ausgeprägt. Der Prozess beginnt in der Regel mit einer anfänglichen Motivation und freiwilligen Teilnahme, die dann in einen stagnierenden Fortschritt übergeht und sogar in künstlichen Verzögerungen enden kann, die sich durch zweideutige Aussagen über zukünftige Aktionen manifestieren.

Um die Sache noch komplizierter zu machen, wenden einige Hersteller eine strikte Informationspolitik an, die den Austausch vertraulicher Informationen verbietet. Unter diesem Umstand kann es schwierig sein, einen CVD-Prozess zu managen, da oft nicht alle identifizierten Schwachstellen auf einmal beseitigt werden. Zur Priorisierung der Schwachstellen wird fast immer eine Restrisikoanalyse oder Aufwandsabschätzung durchgeführt. Die Hersteller können eine Teilmenge der Schwachstellen akzeptieren, da ihre Kritikalität zu gering oder der Aufwand zur Behebung hoch ist. Einem Hersteller bei der Einschätzung zu helfen, ob eine Schwachstelle sofort behoben werden muss oder ob ein potentielles Risiko bis zu einer zukünftigen größeren Veröffentlichung akzeptiert werden kann, ist unter der oben erwähnten strengen Informationspolitik nahezu unmöglich.

Folglich leiden diese Prozesse im Allgemeinen unter verschiedenen Quellen von Verzögerungen. Diese können so einfach sein, wie das Finden eines verantwortlichen Ansprechpartners innerhalb des Unternehmens oder es handelt sich um viel kompliziertere interne Prozesse. Daher sind diese Prozesse in der Regel langwieriger, als bei Herstellern, die eine höhere Reife im Umgang mit Veröffentlichungen aufweisen.

6 Zusammenfassung und Ausblick

Dieses Kapitel umfasst die Durchführung, die Erfahrungen und die Ergebnisse des Projekts und gibt damit einen Ausblick auf mögliche weitere Prüfungen oder sogar Projekte. Zunächst wird das Fazit der Marktanalyse und die daraus gezogenen Schlussfolgerungen, insbesondere auf den Prozess der Sammlung von Informationen über Medizinprodukte, dargelegt. Des Weiteren wird auf die Durchführung und die Ergebnisse der Sicherheitsprüfungen eingegangen, wobei der Schwerpunkt auf der Beantwortung der folgenden Fragen liegt:

1. Ist der aktuelle Stand der veröffentlichten Informationen ausreichend, um diese Technologien, einschließlich der Kommunikationsschnittstellen, in Medizinprodukten zu erfassen?
2. Was lässt sich aus den Ergebnissen der Sicherheitsprüfungen über die allgemeine IT-Sicherheitslage der vernetzten Medizinprodukte ableiten und was sind allgemeine Empfehlungen zur Verbesserung der IT-Sicherheitslage?
3. Welche Vorkehrungen können die Hersteller treffen, um eine rechtzeitige und effiziente Reaktion auf ein Sicherheitsproblem ihrer medizinischen Geräte zu gewährleisten? Wie hoch ist der derzeitige Reifegrad der IT-Sicherheit?

Nach dem Fazit zu den Ergebnissen der Sicherheitsprüfungen folgt noch ein Fazit zu den CVD-Prozessen und abschließend folgt ein Ausblick.

6.1 Fazit der Marktanalyse

Wie in Abschnitt 3.1.1 bereits erwähnt, diente die MPA-Datenbank als Quelle für Informationen über Medizinprodukte. Sobald die Verordnung über Medizinprodukte (MDR) in Kraft tritt, wird EUDAMED die zentrale Datenbank sein, in der Informationen über Medizinprodukte während des Zulassungsverfahrens für den europäischen Markt zur Verfügung gestellt werden müssen. Im Projekt wurde die Datenbank EUDAMED jedoch nicht verwendet.

Bei der Sammlung der für dieses Projekt verwendeten Daten wurden einige Probleme bezüglich der MPA-Datenbank festgestellt. Erstens liefert die Datenbank keine technischen Informationen über die Kommunikationsschnittstellen der medizinischen Geräte. Der Hauptgrund für die Marktanalyse bestand darin, medizinische Geräte mit einer geeigneten Angriffsoberfläche zu identifizieren (z. B. drahtlose Kommunikationsschnittstellen, wie Bluetooth oder physikalische Schnittstellen, wie USB). Diese Informationen konnten nicht aus der Datenbank abgerufen werden und mussten auf anderen Wegen gesammelt werden, z. B. über die von der FDA bereitgestellten Datenblätter (falls das Gerät dort gelistet ist). Die Bereitstellung solcher Informationen wäre nicht nur für den im Rahmen dieses Projekts durchgeführten Datenerfassungsprozess wertvoll, sondern auch für Patienten mit technischem Interesse, um die Kommunikationsschnittstellen in einer bestimmten Medizinproduktekategorie verstehen zu können. Es bleibt abzuwarten, inwieweit die Datenbank EUDAMED solche Informationen bereitstellen kann. Aus Sicht der Autoren ist jedoch eine Datenbank mit technischen Informationen über die Kommunikationsschnittstellen für verschiedene Zielgruppen nützlich. Die Informationen, die in einer solchen Datenbank für ein medizinisches Gerät enthalten sein sollten, sind die Art der Schnittstellen (d. h. USB 3.0, Ethernet) und ein Verweis auf das technische Datenblatt der Schnittstellen.

Darüber hinaus wurde bei der Informationsbeschaffung mit Hilfe der MPA-Datenbank festgestellt, dass nicht unbedingt alle auf dem deutschen Markt zugelassenen Geräte in dieser Datenbank aufgeführt sind. Als Gründe dafür konnten Produktfamilien identifiziert werden, die Produkte nach dem Baukastenprinzip aufbauen, um Flexibilität und Kompatibilität zwischen mehreren Produkten derselben Produktfamilie zu ermöglichen, was dazu führte, dass die einzelnen Teile separat aufgelistet wurden. Darüber hinaus erfasst die Datenbank nur unzureichend medizinische Software, die als *Software as Medical Device* (SaMD)

zertifiziert ist. Andere Möglichkeiten, nicht alle Produkte zu identifizieren, könnten darin bestehen, dass ausschließlich der Zugang zum öffentlichen Teil der Datenbank für Privatpersonen möglich ist.

6.2 Fazit der IT-Sicherheitsprüfungen

Insgesamt wurden den Herstellern im Rahmen des Projekts mehr als 150 Schwachstellen gemeldet. Bei der Prüfung stellte sich heraus, dass die Schwachstellen häufig in der begleitenden Infrastruktur, selten jedoch in Medizinprodukten zu finden waren. Beispielsweise wurden Infusionspumpen in der Regel als robust eingestuft, da sie ihre Funktion unabhängig vom Zustand der Infrastruktur erfüllen, d. h. auch dann, wenn die Infrastruktur ausfällt. Allerdings waren die Docks für die Pumpen in der Regel weniger gesichert, sodass dort vermehrt Schwachstellen festgestellt werden konnten. Dies ist zum einen zu erwarten, da die Docks in der Regel mehr Kommunikationsschnittstellen wie z. B. Ethernet-Ports zur Verfügung stellen. Andererseits kommunizieren diese Stationen in der Regel direkt mit den Pumpen und bieten einem Angreifer eine Schnittstelle für einen möglichen Zugang zu den Pumpen. Häufig werden die Infrastrukturkomponenten als Zubehör für medizinische Geräte klassifiziert. Diese Einstufung erleichtert spätere Modifikationen, kann aber auch zu der Ansicht führen, dass die Sicherheit der Infrastrukturkomponenten weniger kritisch ist. Dennoch sollte darauf hingewiesen werden, dass die Sicherheitsprüfung eines Medizinprodukts immer auch die zugehörigen Infrastrukturkomponenten umfassen sollte, um eine realistische Einschätzung der Sicherheit des Produkts in seiner Betriebsumgebung zu erhalten.

Es wird darauf hingewiesen, dass die Ergebnisse der IT-Sicherheitsprüfungen möglicherweise verzerrt, beziehungsweise beeinflusst wurden. Da die Teilnahme der Hersteller am Projekt freiwillig war, wurde erwartet, dass diejenigen Hersteller am ehesten kooperieren würden, die bereits einen gewissen Reifegrad in ihren IT-Sicherheitsprozessen aufweisen. Um dieser Verzerrung vorzubeugen, nahm das ManiMed-Projektteam nach Abschluss der Marktanalyse Kontakt mit den Anbietern auf, anstatt, dass diese sich für eine Prüfung ihrer Geräte bewerben. Des Weiteren war eines der Projektziele, dass die teilnehmenden Anbieter dabei unterstützt werden, vorhandene Verbesserungsmöglichkeiten in ihren IT-Sicherheitsprozessen zu identifizieren und diese Lücken zu schließen. Auch wenn nicht erfasst wurde, ob und wie sehr eine mögliche Verzerrung bestand, so hat das Projekt den teilnehmenden Anbietern sicherlich geholfen, ihre IT-Sicherheit insgesamt zu verbessern. Insofern wirkte sich das Projekt also insgesamt positiv auf die teilnehmenden Anbieter aus.

Wie in Abschnitt 6.1 erwähnt, kann aufgrund der Auswahlkriterien für Medizinprodukte eine weitere Verzerrung vorliegen. Obwohl diese Auswahlkriterien sorgfältig gewählt wurden und die Gerätekategorien kritische Funktionalitäten enthalten, können diese Kriterien nicht gewährleisten, dass die durchgeführten Sicherheitsprüfungen für den gesamten deutschen Medizinproduktemarkt gelten. Daher sei an dieser Stelle darauf hingewiesen, dass dies nicht die Absicht des Projekts war, die gesamte Medizinprodukte-Landschaft in Deutschland zu testen. Ziel war es jedoch, eine grobe Schätzung der IT-Sicherheitslage des deutschen Medizinproduktemarktes zu erhalten, auf deren Grundlage weitere Überlegungen angestellt werden können.

Die Sicherheitsbewertungen haben auch gezeigt, dass die IT-Sicherheitslage von Hersteller zu Hersteller sehr unterschiedlich ist und stark vom Reifegrad des einzelnen Herstellers abhängt. Daher stellt sich die Frage, wie der Reifegrad und das IT-Sicherheitsverhalten der verschiedenen Anbieter auf ein gleich hohes Niveau gehoben werden kann. Dies hängt zum einen sicherlich vom gesetzlichen Rahmen ab, der Anforderungen definiert, auf deren Grundlage Medizinprodukte für den Markt zugelassen werden. Zum anderen hängt dies von der Motivation des Herstellers ab, sich mit Themen der IT-Sicherheit proaktiv auseinanderzusetzen. Diese Motivation zeigt, ob Anbieter einen sicheren Produktlebenszyklus für ihre Produkte, in Kombination mit einer rechtzeitigen und effektiven Reaktion auf offengelegte Schwachstellen, implementiert haben und durchsetzen können, nicht nur, weil es gesetzlich vorgeschrieben ist.

Insgesamt zeigt die große Zahl der während des Projekts identifizierten Schwachstellen einige Verbesserungsmöglichkeiten im Bereich der Medizinprodukte auf. Verschiedene Parteien, wie z. B. Regulierungsbehörden und Hersteller sollten sich verstärkt darum bemühen das Sicherheitsniveau der Produkte zu erhöhen.

6.3 Häufig auftretende Probleme

Um Hersteller und Betreiber medizinischer Geräte in diesem Bestreben zu unterstützen und die IT-Sicherheit insgesamt zu verbessern, werden im Folgenden häufig auftretende Probleme aufgezeigt, die bei den Sicherheitsprüfungen festgestellt wurden und es werden Strategievorschläge gemacht, wie diese behoben werden können.

6.3.1 Verschiedene Arten von Schwachstellen

Es ist nicht ungewöhnlich, dass Sicherheitslücken aufgrund von Diskrepanzen zwischen dem spezifizierten und dem realen Verhalten eines sozio-technischen Systems entstehen. Diese Diskrepanz lässt sich bei Dokumentations- und Spezifikationsreviews kaum feststellen. Bewährte Mittel sind externe Penetrationstests, bei denen ein komplexes, aktives Medizinprodukt vor dem produktiven Einsatz tiefgehend untersucht wird. Abhängig von der Gerätefunktionalität werden externe medizinische und nicht-medizinische, drahtlose und drahtgebundene Netzwerkschnittstellen, Bluetooth- und USB-Schnittstellen, Update-, Wartungs- und Konfigurationsmechanismen auf Schwachstellen untersucht und bestehende Sicherheitsmaßnahmen auf ihre Wirksamkeit hin überprüft. Bei diesen Tests können Design-, Implementierungs- und Konfigurationsfehler beobachtet werden. Schwachstellen können daher in drei Klassen eingeteilt werden: Design-, Implementierungs- und Konfigurationsfehler (Boehm, 1984).

Konfigurationsfehler können auf jeder Ebene der Anwendung auftreten, z. B. bei Netzwerkdiensten, Betriebssystemen, Plattformen und Webservern. Typische Beispiele für Konfigurationsfehler sind Standardkonten, schwache Konfigurationen von kryptographischen Bibliotheken und Mechanismen oder die Preisgabe von Informationen, wie Versionsnummern oder Fehlermeldungen. Diese Fehler hängen von der spezifischen Betriebsumgebung ab und sind oft mit anderen Betriebsdefiziten, wie veralteter Software verbunden. Die Schwachstellen lassen sich leicht beheben, indem die Konfiguration geändert wird und Updates und Patches bereitgestellt werden. Die Behebung kann angemessen, aber nicht ausreichend sein, da sie durch grundlegende fehlende Mechanismen verursacht werden. Diese Schwachstellen beleuchten fehlende Konfigurations- und Betriebskonzepte, wie z. B. eine angemessene Härtung über alle Teile der Anwendung und Prozesse hinweg, um den Systemstatus kontinuierlich zu bewerten und aufrechtzuerhalten, z. B. durch ein angemessenes Patch-Management. Es wird hier deutlich, dass eine geteilte Verantwortung zwischen Herstellern und Betreibern medizinischer Geräte unerlässlich ist.

Implementierungsfehler können auftreten, wenn sich das spezifizierte und das reale Verhalten einer Funktionalität aufgrund eines Codierungsproblems unterscheiden. Beispielsweise ist eine Anwendung anfällig für Angriffe, wenn vom Benutzer bereitgestellte Daten von der Anwendung nicht validiert, gefiltert, auf ihre Länge geprüft oder bereinigt und daher unsicher verarbeitet werden. Der anfällige Code muss modifiziert oder erweitert werden, um diese Probleme zu beheben, was schwierig sein kann, wenn Schnittstellen zu Bibliotheken oder andere Anwendungsschnittstellen (API) geändert werden müssen. Diese Bemühungen resultieren entweder in einem Patch oder sie werden bei den regelmäßigen Aktualisierungen, in Form von Updates, angewendet. Aus diesen Mängeln zu lernen, indem man defensive und sichere Programmiertechniken, in Kombination mit Unit- und Integrationstests einführt, ist ein Schritt, um die Software-Entwicklungskultur innerhalb einer Organisation so zu verändern, dass sicherer Code mit einer Feedbackschleife im Zuge des sicheren Produktlebenszyklus produziert wird.

Schwachstellen, die Designfehler darstellen, können auftreten, wenn Mechanismen oder Schnittstellen ohne einen dedizierten Sicherheitsfokus entworfen werden oder wenn Mechanismen umgangen oder unwirksam gemacht werden können. Häufig entstehen diese Probleme aufgrund unsicherer Interaktionen zwischen Komponenten und Entitäten in Kommunikationssystemen, von denen angenommen wird, dass sie untereinander vertrauenswürdig sind. Die Komplexität der Behebung von Designfehlern hängt von den betroffenen Teilen des Systems ab. Einzelne Bibliotheken oder Anwendungen lassen sich möglicherweise leichter modifizieren, als Kommunikationsschnittstellen zu externen Systemen oder Umgebungen, da diese die jeweiligen Schnittstellen ebenfalls ändern müssen, um Kompatibilitätsprobleme zu vermeiden.

Bei der Behebung und Abschwächung von Schwachstellen sollte die Kritikalität dieser stets beachtet werden. Eine Kundeninformation oder eine vorübergehende Maßnahme können zunächst ausreichend sein, bis im Anschluss daran permanente Abhilfemaßnahmen ergriffen werden können. In einigen Fällen müssen mehrere Schwachstellen zusammen behoben werden, wenn sie das Produkt als Ganzes bedingen. Oftmals werden aber nicht alle identifizierten Schwachstellen auf einmal beseitigt. Zur Priorisierung der Schwachstellen wird fast immer eine Restrisikoanalyse oder Aufwandsabschätzung durchgeführt. Eine Teilmenge der Schwachstellen könnte akzeptiert werden, wenn ihre Kritikalität zu gering oder der Aufwand zur Behebung zu hoch ist.

6.3.2 Das Patch Management

Ein wichtiges Thema ist das Patch-Management, das bei Medizinprodukten und in fast allen IT-Bereichen auftritt. Bei Medizinprodukten kann das Patch-Management jedoch eine kritischere Rolle spielen, wenn die Ausnutzung einer Schwachstelle eines Geräts den Patienten schaden könnte. Hier stellt sich die Frage, wie ein Patch sicher auf die von einer Schwachstelle betroffenen Geräte ausgerollt werden kann. Der Prozess der Veröffentlichung der Schwachstelle und der sichere Entwicklungsprozess des Patches werden in Abschnitt 6.4 diskutiert. An dieser Stelle sollte jedoch erwähnt werden, dass beide Prozesse auch für die rechtzeitige Bereitstellung eines Patches unerlässlich sind. Im Folgenden wird nur der Schritt der Bereitstellung des Patches für die Geräte fokussiert.

Der Ausroll-Prozess des Patches besteht aus mehreren Teilschritten:

- Entwicklung und Validierung des Patches
- Sicheres Bereitstellen des Patches
- Ankündigung des Patches
- Sicheres Einspielen des Patches

Natürlich können diese Schritte von der Art des Geräts, das aktualisiert werden muss, abhängig sein. So ist es beispielsweise bedeutend einfacher, einen Patch für einen Patientenmonitor, der einen Aktualisierungsmechanismus bietet, durch Einstecken eines USB-Sticks mit der neuen Firmware oder über das Internet anzuwenden, als ein Implantat im Körper eines Patienten zu aktualisieren. Je nach Gerätetyp und Komplexität des Patch-Prozesses muss auch festgelegt werden, wer überhaupt berechtigt sein sollte ein solches Update durchzuführen. Dabei ist zu berücksichtigen, dass durchschnittliche Personen oftmals nicht über Sicherheitsupdates für ihre Geräte informiert ist, d. h. diese Personen sollten nicht für die Bereitstellung eines solchen Patches verantwortlich sein. Daher gibt es zwei Möglichkeiten: Entweder stellt geschultes Personal den Patch über einen Bereitstellungsmechanismus zur Verfügung oder das Gerät führt automatische Aktualisierungen über die Verbindung zum Internet durch. Es ist jedoch zu beachten, dass die zweite Option eine sichere Infrastruktur erfordert, die für solche automatischen Aktualisierungen verwendet wird.

Dennoch gibt es allgemeine Richtlinien, die bei diesem Prozess befolgt werden sollten. Im vorigen Absatz wurde bereits erwähnt, dass der Patch sicher bereitgestellt werden sollte. Das bedeutet, dass die Patch-Datei mit einem privaten Schlüssel, auf den nur der Hersteller Zugriff hat, kryptographisch signiert werden sollte. Natürlich muss das Gerät, auf das der Patch angewendet werden soll die Signatur der Firmware

kryptographisch verifizieren. Diese Überprüfung stellt sicher, dass Unbefugte die Patch-Dateien nicht manipulieren können und es werden nur vom Hersteller freigegebene Patch-Dateien angewendet. Dies setzt jedoch voraus, dass der Hersteller eine Public-Key-Infrastruktur unterhält und Verfahren für den Fall entwickelt, dass der entsprechende private Schlüssel kompromittiert wird. Als zusätzliche Maßnahme kann die Patch-Datei auch in verschlüsselter Form bereitgestellt werden. Da jedoch der kryptographische Schlüssel zum Entschlüsseln der Patch-Datei auf dem Gerät vorhanden sein muss, hindert diese Maßnahme einen raffinierten Angreifer in der Regel nicht daran an die entschlüsselte Patch-Datei zu gelangen, da er beispielsweise den Schlüssel über spezielle Hardware aus dem Speicher auslesen kann. Daher ist das Signieren der wichtigste Teil, da dieses belegt, dass die Patch-Datei von einer vertrauenswürdigen Quelle stammt.

Wenn ein Mechanismus zur Bereitstellung und Überprüfung signierter Patch-Dateien nicht implementiert werden kann, wäre eine andere Strategie, dass die Patch-Datei auf einer HTTPS-gesicherten Website, deren Domäne unter der Kontrolle des Anbieters steht, bereitgestellt wird. Die Bereitstellung der Datei auf diese Weise impliziert, dass der Hersteller die Datei so zur Verfügung hat, wie sie auf seiner Website vorhanden ist. Ein Nachteil ist jedoch, dass wenn die Patch-Datei dem Gerät zur Verfügung gestellt wird, das Gerät die Gültigkeit der Patch-Datei nicht mehr überprüfen kann, da keine kryptographische Signatur vorhanden ist. Wenn die Datei kompromittiert wird, nachdem sie von der entsprechenden Website heruntergeladen wurde (beispielsweise, wenn das zum Herunterladen der Datei verwendete Gerät kompromittiert ist), kann das Gerät eine solche Änderung nicht erkennen.

Betroffene Patienten müssen darüber informiert werden, dass ein Patch auf ihre Geräte aufgespielt werden soll. Daher muss im Voraus ein Kommunikationskanal eingerichtet werden, um sicherzustellen, dass Patienten und Betreiber erreicht werden können, die das betroffene Medizinprodukt verwenden. Schließlich sollte eine solche Ankündigung auch beinhalten, was die Patienten tun müssen, damit der Patch angewendet werden kann. Es sollte erwähnt werden, dass dieser Prozess auch je nach Art des Medizinprodukts unterschiedlich ablaufen kann. Geräte, die in der Regel nur in Krankenhäusern verwendet werden und nicht direkt im Besitz des Patienten sind, können andere Kommunikationskanäle erfordern, als beispielsweise Insulinpumpen, die der Patient ständig an sich trägt.

Insgesamt sollten die Hersteller vor der Freigabe eines Medizinprodukts ein detailliertes Verfahren für das Patch-Management entwickeln, um sicherzustellen, dass diese schnell und sicher eingeführt werden können. Bei der Festlegung eines solchen Prozesses müssen mehrere Faktoren berücksichtigt werden, z. B. die Bereitstellung des Patches, wer den Patch installiert und wie überhaupt kommuniziert wird, dass ein entsprechender Patch verfügbar ist.

6.3.3 Die Betriebsumgebung

Ein weiterer nicht zu vernachlässigender Punkt ist, dass oftmals nicht genau definiert ist, in welchen Umgebungen Medizinprodukte betrieben werden sollen. Daher kann es Diskrepanzen zwischen den Betriebsumgebungen, welche die Hersteller annehmen und den Betriebsumgebungen, die bei den Betreibern vorzufinden sind, geben. Ein Hersteller kann beispielsweise davon ausgehen, dass sein Produkt in einer isolierten Netzwerkumgebung betrieben wird, in der keine anderen Geräte vorzufinden sind, wobei er davon ausgeht, dass in diesem Fall keine anderen Geräte mit den Diensten des Medizinprodukts kommunizieren können. Der Betreiber des medizinischen Geräts kann und sollte jedoch davon ausgehen, dass das Gerät in jedem Netzwerk betrieben werden kann und dass seine Sicherheit nicht von der Sicherheit der Netzwerkumgebung abhängt. Diese Diskrepanz in den Annahmen kann zu schwerwiegenden Sicherheitsproblemen führen. Wenn zum Beispiel ein Krankenhausnetzwerk nicht segmentiert ist, können häufig alle Geräte untereinander kommunizieren. Es kann ebenfalls der Fall sein, dass das Gastnetzwerk von Patienten direkt eingebunden ist, d. h. Patienten, die sich mit ihren Laptops oder mobilen Endgeräten mit dem Gastnetzwerk verbinden, können, wenn keine Segmentierung vorliegt, auf die entsprechenden Geräte zugreifen. Unter der Annahme, dass die von Medizinprodukten angebotenen Dienste so konzipiert

wurden, dass die Geräte in einem isolierten Netzwerk betrieben werden, wird die Sicherheit der Geräte beeinträchtigt, wenn z. B. keine Authentifizierung vorhanden ist.

Manchmal wird die Minimierung dieser Designfehler durch anspruchsvolle Sicherheitsanforderungen an die Betriebsumgebung, als einzige Verteidigungsstrategie, erreicht. Dieser Ansatz verlagert den Aufwand der Gewährleistung der Sicherheit des Systems auf den Betreiber, was nicht akzeptabel ist, da es nicht die Aufgabe des Betreibers ist, ein unsicheres System sicher zu machen und im Widerspruch zu den jeweiligen Designkonzepten *Defense-in-Depth* und *Security-by-Design* steht.

Daraus folgt, dass die Hersteller klare Richtlinien für die Umgebungen, in denen die Geräte betrieben werden, bereitstellen müssen. Die Hersteller sollten immer davon ausgehen, dass das Gerät in einer ungesicherten Umgebung betrieben wird und dass die Dienste des Geräts erreicht werden können. Daher müssen die Dienste durch obligatorische Schutzmaßnahmen geschützt werden, die einem *Defense-in-Depth*-Ansatz folgen, wie beispielsweise Authentifizierungs- und Autorisierungsmechanismen. Die Hersteller sollten die Sicherheitsimplikationen, die sich aus dem Betrieb des Geräts in einer unsicheren Umgebung ergeben, klar darlegen, damit dies für die Betreiber ersichtlich ist.

Dennoch sollten Betreiber eine Segmentierung ihres Netzwerks, als zusätzliche Verteidigung, in Betracht ziehen, um Netzwerke, in denen Medizinprodukte eingesetzt werden, isolieren zu können. Eine Segmentierung verringert das Risiko, dass ein ungesicherter Dienst eines Medizinprodukts unnötig exponiert wird. Die Ausgestaltung von Netzwerksegmenten und ihre Zusammenschaltung über Firewalls mit entsprechenden Regeln kann je nach Größe des Netzwerks und der Anzahl der Geräte einen erheblichen Aufwand bedeuten.

6.3.4 Authentifizierung, Autorisierung und Zugriffskontrolle

Authentifizierungsmechanismen stellen bei verschiedenen Arten von Medizinprodukten oft ein Problem dar. Wie oben erwähnt, existieren diese Mechanismen möglicherweise nicht, insbesondere dann nicht, wenn der Hersteller davon ausgeht, dass das Gerät in einer sicheren Umgebung betrieben wird. Die Implikationen, die sich aus diesen Annahmen ergeben, werden in Abschnitt 6.3.3 erläutert.

Zudem kann der Authentifizierungsmechanismus schwach sein oder sogar Schwachstellen aufweisen, die es ermöglichen, ihn zu umgehen. Dieser Mechanismus stellt in der Regel den Zugang zu den Kernfunktionen des Geräts dar. Er sollte in Sicherheitsprüfungen detailliert analysiert werden, sodass Schwachstellen innerhalb des Produktlebenszyklus identifiziert werden können.

Drittens kann die Verwaltung von Authentifizierungsfaktoren, wie Passwörtern, ein Problem darstellen, da oftmals Geräte über Standardkonten mit Standardpasswörtern verfügen oder da die Betreiber nicht verpflichtet werden, diese Passwörter bei oder nach der Bereitstellung des Produkts zu ändern. Manchmal ist es auch nicht möglich, solche Konten zu deaktivieren oder ihre Passwörter neu zu konfigurieren. Angreifer können folglich diese Standardkonten mit ihren Standardpasswörtern verwenden, um auf die Geräte zuzugreifen.

Daher sollten Hersteller Mechanismen implementieren, die eine Änderung solcher Passwörter während der Bereitstellungsphase des Geräts erzwingen. Hierbei können jedoch gerätespezifische Überlegungen eine Rolle spielen. Eine Verkomplizierung und Überdimensionierung der Sicherheitsmechanismen kann zu Situationen führen, in denen ein Nutzer nicht auf wesentliche Gerätefunktionen zugreifen kann. Daher kann nicht einfach vorgeschrieben werden, dass alle Geräte über geeignete Mechanismen verfügen müssen.

Es wird zumeist davon ausgegangen, dass die Authentifizierungsfaktoren während der Einrichtung des Geräts geändert werden. In diesem Fall muss ein Verfahren zur Verteilung dieser Faktoren an das nutzende Personal etabliert sein. Infolgedessen müssen diese Mechanismen angemessen und effektiv sein, stellen aber oft einen Kompromiss zwischen IT-Sicherheit und medizinischer Funktionalität dar. Dieser Kompromiss sollte gut durchdacht sein. Eine Diskussion, die auf den verschiedenen Betriebsmodi eines Geräts wie Konfigurationsmodus, Wartungsmodus und medizinischer Betriebsmodus basiert, löst

komplexe Sicherheitsprobleme oft auf, sodass kleinere Probleme mit weniger komplexen, aber sichereren Lösungen entstehen. Das BSI-Dokument "Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte" (BSI, 2018) wäre hier zu empfehlen.

6.3.5 Kommunikationsprotokolle

Während der IT-Sicherheitsprüfungen wurde festgestellt, dass jeder Hersteller seinen eigenen Satz an teilweise proprietären Kommunikationsprotokollen für Schnittstellen zur Verbindung mit externen Geräten mitbringt. Häufig waren proprietäre Protokolle in großem Umfang implementiert worden. Diese herstellergebundenen Umgebungen führen aufgrund systematischer Inkompatibilität zu einer großen Vielfalt an Kommunikationsprotokollen, die in derselben Umgebung für ähnliche Zwecke verwendet werden.

Einerseits macht es diese Vielfalt schwierig klare Sicherheitsrichtlinien für die verwendeten Kommunikationsprotokolle aufzustellen. Andererseits kann der Bedarf an spezifischen Protokollen mangels Verfügbarkeit standardisierter Lösungen notwendig sein. Darüber hinaus können Betreiber in öffentlichen Ausschreibungen kaum IT-Sicherheitsanforderungen fordern und spezifizieren, wenn es sich bei den angebotenen Lösungen um Black Boxes handelt, deren Sicherheitsmechanismen und Protokolle nicht ohne weiteres geprüft und bewertet werden können. Diese fehlende Transparenz verschlechtert die Situation mit jedem neu betriebenen System. Dennoch würde eine Reihe von standardisierten Kommunikationsprotokollen mit präzisen IT-Sicherheitsanforderungen den Spielraum für Missverständnisse oder fehlerhafte Implementierungen, die zu Schwachstellen führen können, verringern. Insgesamt müssten solche Bemühungen im Zuge der Interoperabilität von Geräten und Gerätesystemen auf einer gemeinsamen Anstrengung aller beteiligten Parteien beruhen.

6.4 Fazit der CVD-Prozesse

In diesem Abschnitt werden die Erfahrungen aus den Veröffentlichungsprozessen vorgestellt und Schlussfolgerungen gezogen, insbesondere jene, die als grundlegend für die Durchführung koordinierter Veröffentlichungen von Schwachstellen und als wichtig für die Verbesserung der IT-Sicherheit von Medizinprodukten angesehen werden.

Das koordinierte Verfahren zur Veröffentlichung von Schwachstellen, das von den Autoren befolgt wurde, wird von Sicherheitsforschern üblicherweise zur Meldung von Schwachstellen verwendet und in Abschnitt 2.11 dargestellt. Die jeweiligen Erfahrungen werden in Abschnitt 5 vorgestellt. Es kann daraus geschlussfolgert werden, dass die Art und Weise, wie mit der Entdeckung von Sicherheitslücken umgegangen wird, von Hersteller zu Hersteller sehr unterschiedlich ist. Jeder CVD-Prozess ist zeitintensiv und erfordert erheblichen Aufwand und Ressourcen. Die transparente Handhabung von Schwachstellen und deren Veröffentlichung ist einer der entscheidenden Punkte in diesem Projekt sowie in jedem CVD-Prozess. IT-Sicherheit sollte Teil des Produktlebenszyklus sein und bei der Risikobewertung beachtet werden. Es könnte der Irrglaube entstehen, dass Produkte mit veröffentlichten Sicherheitslücken von minderer Qualität sind, als Produkte bisher ohne bekannte Schwachstellen. Diese Verzerrung wird als *Observation Bias* bezeichnet, da nur Hersteller wahrgenommen werden, die ihre Bemühungen und Lernprozesse aktiv kommunizieren. Im Gegensatz dazu ist der Glaube, dass das Nicht-Erkennen von Sicherheitslücken die Hersteller und ihre Produkte schützt, ein Irrglaube, da bisher noch kein Vorfall stattgefunden hat. Es lässt sich bei einigen Herstellern beobachten, dass sie Vorfälle und Schwachstellen, im Einklang mit dem Sicherheitsprinzip des Verschleierns, vertraulich zu halten versuchen. Grundsätzlich sollte jedes System und jeder Sicherheitsmechanismus als öffentlich betrachtet werden, wie das Zitat "wir sollen davon ausgehen, dass der Feind das verwendete System kennt" (Shannon, 1949) von Claude Shannon aus dem Jahre 1949 beschreibt im Zusammenhang mit seiner Arbeit über die Aussagen der Kommunikationstheorie in kryptographischen Systemen.

Zur Erleichterung und Beschleunigung der Prozesse, insbesondere wenn der Hersteller mit CVDs nicht vertraut ist, werden ein entsprechendes CVD-Rahmenwerk und entsprechende Regeln dringend empfohlen. Zusätzlich sollte der Hersteller ein transparentes Verfahren einrichten, um auf solche Sicherheitsprobleme zu reagieren und die daraus resultierenden Risiken rechtzeitig zu mindern. Zu diesem Zweck sollte der Hersteller Kontaktinformationen angeben, über die solche Probleme gemeldet werden können, in der Regel eine spezielle E-Mail-Adresse. Da die gemeldeten Probleme oft kritische Informationen über die identifizierte Schwachstelle enthalten, sollte ein sicherer Mechanismus zur Kommunikation über verschlüsselte E-Mails bereitgestellt werden, z. B. durch Verwendung eines öffentlichen PGP-Schlüssels zusammen mit der E-Mail-Adresse.

Nachdem ein Problem gemeldet wurde, sollte der Hersteller den Eingang des Problems rechtzeitig (z. B. innerhalb eines Arbeitstages) bestätigen. Der Eingang des Schwachstellenberichts sollte mehrere interne Prozesse beim Hersteller auslösen:

- Entsprechende Experten müssen konsultiert werden, um die Validität des Berichts zu prüfen
- Die Experten müssen die Maßnahmen zur Behebung der Schwachstelle festlegen
- Das von den Schwachstellen ausgehende Risiko muss bewertet werden.

Abhängig vom Risiko müssen geeignete Parteien in den Prozess einbezogen werden, z. B. wegen weiterer rechtlicher Anforderungen an die Meldung potentieller Vorfälle oder für die technische Beratung. Der Hersteller besitzt Expertenwissen für seine Produkte, sodass er eine genaue Risikoanalyse durchführen kann. Der Finder kann nur die technische Komplexität und die technischen Auswirkungen einer Schwachstelle feststellen.

Ein weiteres Ergebnis der Veröffentlichungsprozesse ist, dass die Kommunikation zwischen Herstellern und Behörden, wie BSI und BfArM, erleichtert wird und so die Prozesse beschleunigen kann. Darüber hinaus erleichtert die technische Analyse der Schwachstellen die Identifizierung von organisatorischen Maßnahmen, um das Risiko einer vorübergehenden Beeinträchtigung der Patientensicherheit zu verringern. Eine Deaktivierung von Diensten oder Netzwerkfunktionalitäten kann den therapeutischen oder diagnostischen Zweck eines Geräts beibehalten und gleichzeitig ein Zeitgewinn sein, um technische Korrekturen zu implementieren. Oftmals implementieren die Produkte bereits zusätzliche Sicherheitsvorkehrungen, die auch bei der Umsetzung temporärer Maßnahmen helfen können.

Abgesehen von einem Veröffentlichungsprozess wäre es vorteilhaft, einen rechtlichen Rahmen zu haben, der die Anforderungen dieses Prozesses formalisiert. Die derzeitigen deutschen Rechtsrahmen konzentrieren sich hauptsächlich auf Patientensicherheitsaspekte von Medizinprodukten und befassen sich mit IT-Sicherheitsproblemen nur insoweit, als sie die Patientensicherheit betreffen. Ein rechtlicher Rahmen für den Veröffentlichungsprozess aller Sicherheitsprobleme (nicht nur derjenigen, die sich auf die Patientensicherheit auswirken können) würde den Herstellern eine klare Richtung zu den erforderlichen Schritten vorgeben, wenn sie Informationen über eine Schwachstelle in ihrem Produkt erhalten.

6.5 Ausblick

Das Erreichen eines gleichmäßig hohen IT-Sicherheitsniveaus ist keine einmalige Aufgabe, sondern ein komplizierter und nicht endender Prozess. Nachfolgend wird ein Ausblick auf mögliche weitere Forschungsgegenstände und Projekte gegeben, die dazu beitragen könnten, das allgemeine IT-Sicherheitsniveau von Medizinprodukten weiter zu verbessern.

Zum einen ist es notwendig, dass Sicherheitsüberprüfungen regelmäßig und in einer angemessenen und realistischen Testumgebung durchgeführt werden, um kontinuierlich Einblick in den Zustand der IT-Sicherheit von Medizinprodukten zu haben. Das Projekt ManiMed liefert bereits jetzt wertvolle Erkenntnisse über den Zustand der IT-Sicherheit von Medizinprodukten. Es ist unerlässlich, solche Prüfungen regelmäßig (z. B. alle drei bis fünf Jahre) durchzuführen, um die Verbesserungen hinsichtlich der IT-Sicherheit zu prüfen.

Zweitens ist es für einen Gesamtüberblick des IT-Sicherheitszustands von Medizinprodukten von entscheidender Bedeutung, eine größere Auswahl an Produkten und zusätzliche Gerätekategorien sowie die dazugehörige Infrastruktur einzubeziehen. Um den Umfang eines solchen Projekts überschaubar zu halten, wäre es vermutlich sinnvoll jeder Gerätekategorie oder jeder Gruppe von Gerätekategorien (z. B. radiologische Geräte), die bewertet werden sollen, ein eigenes Projekt zu widmen. Insgesamt würde dies eine detaillierte und umfassende Aussage über die IT-Sicherheit bestimmter Gerätekategorien ermöglichen. Generell wird erwartet, dass die Hersteller solche Tests im eigenen Interesse regelmäßig selbst durchführen.

Drittens variiert die Art und Weise, wie mit der Entdeckung von Sicherheitslücken umgegangen wird, erheblich von Hersteller zu Hersteller. Ein CVD-Rahmen und Regeln, auf die sich die Hersteller einigen und an die sie sich halten, erleichtern und beschleunigen solche Prozesse. Es wäre wünschenswert, diese Prozesse auf internationaler Ebene zu harmonisieren.

Viertens wäre es wünschenswert, den Aufwand für die Festlegung klarer Sicherheitsrichtlinien für medizinische Kommunikationsumgebungen zu verringern. Die oft herstellergebundenen Umgebungen führen dazu, dass aufgrund systematischer Inkompatibilität verschiedene Kommunikationsprotokolle in derselben Umgebung für ähnliche Zwecke verwendet werden. Das Streben nach größerer Interoperabilität kann transparentere und besser beobachtbare Systeme schaffen, die eine gemeinsame Sicherheitsinfrastruktur, wie eine PKI nutzen, anstatt die Sicherheitsinfrastruktur in jeder geschlossenen Umgebung neu aufzubauen. Diese Bemühungen könnten den für den Betrieb erforderlichen Aufwand massiv reduzieren.

ManiMed ist das erste Projekt dieser Art, und die Ergebnisse sind bahnbrechend in Bezug auf die Anzahl der identifizierten Schwachstellen, die Anzahl der bewerteten Geräte und Klassen, die Zusammenarbeit und die anschließenden Veröffentlichungsprozesse. Die Projektergebnisse ermutigen Hersteller hoffentlich dazu, dass sie ihre Prozesse hinterfragen, da eine professionelle Handhabung, Kommunikation und ein sicherer Lebenszyklus das Vertrauen stärken und die Sicherheit während des gesamten Lebenszyklus des Produkts gewährleisten.

7 Methodologie der IT-Sicherheitsuntersuchungen und Umfang der Tests

Es wurde eine allgemeine Methodik und ein Anwendungsbereich für die Prüfung vernetzter Medizinprodukte erarbeitet, um dem Leser Hintergrundinformationen zu den Fragen zu liefern, die eine IT-Sicherheitsprüfung beantworten soll.

Die vorgestellten Abschnitte und Methodologien erheben weder Anspruch auf Vollständigkeit, noch sollten sie als verbindliche Lösungen betrachtet werden. Die Prüfung von Medizinprodukten ist hoch spezialisiert. Jede Prüfung ist individuell hinsichtlich der medizinischen Zweckbestimmung des Geräts, der vorhandenen Schnittstellen, der verwendeten Technologien und der Annahmen zu seiner Umgebung.

Die nachfolgenden Abschnitte werden aus der Sicht eines Penetrationstesters erklärt, der ein Gerät aus der Black-Box-Perspektive beurteilt. Es ist zu beachten, dass die Methodik nicht dazu verwendet werden kann, um zu bestimmen, wie wahrscheinlich es von vornherein ist, dass sich eine der beschriebenen Schwachstellen innerhalb des Geräts befindet. Andere Faktoren, wie z. B. ob und wie Unit-Tests mit Schwerpunkt auf Sicherheitsaspekte während des Softwareentwicklungslebenszyklus des Produkts durchgeführt werden und die Größe der Sicherheitsabteilung des Herstellers müssten einbezogen werden, um eine A-Priori-Sicherheitslagenabschätzung vornehmen zu können. Eine Cyber-Sicherheitsempfehlung für netzwerkfähige Medizinprodukte wurde vom BSI publiziert (BSI, 2018). Die vorgestellte Methodik ergänzt daher die Dokumente des BSI aus der Perspektive der Sicherheitsprüfung.

Die meisten Schritte und Tests sind direkt durch Schwachstellen motiviert, die die entsprechende Schnittstelle, Funktionalität, Anwendung oder Hardware betreffen. Einige Punkte entsprechen jedoch nicht direkt einer Schwachstelle, sondern sind zur Vorbereitung notwendig, um mehr über das Produkt zu erfahren.

Aufgrund der Komplexität von Medizinprodukten und ihrer Umgebung sollte sich eine praktische IT-Sicherheitsprüfung auf das Gerät selbst sowie seine Umgebung konzentrieren. Folglich sollte eine Sicherheitsprüfung Verbindungen zwischen den kommunizierenden Komponenten explizit betrachten, da sich Schwachstellen in Kommunikationssystemen auf andere Komponenten, Geräte oder Schnittstellen auswirken können.

7.1 Methodologie: Analyse der Angriffsoberfläche

Die Dokumentation wird bei einer Prüfung, zur Beurteilung der Angriffsfläche der Geräte, berücksichtigt, wenn sie von Herstellern zur Verfügung gestellt wird oder öffentlich zugänglich ist. Diese Dokumentation umfasst Designdokumente, wie Architekturspezifikationen, Produkt- und Softwarespezifikationen, Entwicklungsdokumentation, wie Schnittstellen, Kommunikationsflussdiagramme, Implementierungsleitfäden, Kommunikationsprotokollspezifikationen und Konformitätserklärungen für medizinische Kommunikationsstandards, wie DICOM oder HL7v2.x und mehr. Darüber hinaus sind alle verwendeten Technologiestacks und Software von Drittanbietern, Open-Source-Bibliotheken und Betriebssysteme von Interesse.

Die Phase der Informationssammlung zielt darauf ab so viele Details, wie möglich, über das Gerät und seine Umgebung zu sammeln, um seine Angriffsoberfläche für weitere Analysen zu bewerten. Zu diesem Zweck werden laufende und exponierte Dienste, verwendete Protokolle, offengelegte Technologien und ihre Versionsnummern, verwendete Betriebssysteme, das grundlegende Geräteverhalten und administrative Schnittstellen gesammelt. Außergewöhnliche Funktionalität und komplexe Mechanismen innerhalb der Geräte und ihrer Software werden für die weitergehende Analyse dokumentiert, indem die angebotene Funktionalität des Geräts oder der Anwendung untersucht wird.

Die gesammelten Informationen werden nach der Betriebsart der Software oder des Geräts kategorisiert, wie es die BSI-Empfehlung für Hersteller medizinischer Geräte vorschlägt (BSI, 2018):

A) **Betriebsart nach medizinischer Zweckbestimmung**: In dieser Betriebsart wird das Produkt für seinen medizinischen Verwendungszweck eingesetzt, wie z. B. für die Messung von Vitalparametern oder die Verabreichung von Insulin.
B) **Konfiguration des Geräts:** In dieser Betriebsart wird das Gerät für seine vorgesehene medizinische Verwendung (Zweckbestimmung) konfiguriert. Dies umfasst sowohl Sicherheitskonfigurationen, die einen sicheren technischen Betrieb gewährleisten, als auch die für den medizinischen Betriebsmodus notwendigen Einstellungen (z. B. an den Patienten angepasste Parameter).
C) **Technische Wartung:** In dieser Betriebsart werden Updates vom Hersteller oder von Drittanbietern installiert und notwendige Kalibrierungen oder Anpassungen vorgenommen.

Weiterhin werden die verschiedenen Komponenten der Kommunikationssysteme und Kommunikationsflüsse dokumentiert. Neben dem Medizinprodukt selbst kann es weitere Komponenten geben, die bei der Prüfung von Interesse sind:

- Geräte-Firmware und Software-Updates
- Mobile Anwendungen, die über WLAN, NFC, Bluetooth usw. drahtlos mit dem Gerät interagieren
- Software zur Verwaltung und Steuerung des Geräts
- Service- und Support-Software für fortgeschrittene Konfigurationen des Geräts und seiner Umgebung
- Server-Anwendungen, Netzwerk-Infrastruktur und Schnittstellen zu klinischen Systemen
- Administrative (Web-)Schnittstellen

7.2 Methodologie: Schnittstellen und Kommunikationsprotokolle

Dieser Abschnitt beschreibt Methoden zur Durchführung von Sicherheitsprüfungen von Schnittstellen in Medizinprodukten, welche durch die zunehmende Vernetzung immer weiter an Bedeutung gewinnen.

IT-Sicherheitsprüfungen können nach einem White-Box- oder einem Black-Box-Ansatz durchgeführt werden. Die Erfahrung zeigt, dass White-Box-Sicherheitsprüfungen bei der Bewertung der Angriffsfläche eines Ziels effektiver und effizienter sind und gleichzeitig den Aufwand für die Prüfung des Geräts verringern. Einem Black-Box-Ansatz zu folgen, erfordert im Allgemeinen mehr Ressourcen, um ein vergleichbares Ergebnis zu erzielen, als ein White-Box-Test. Allerdings ist die Wahrscheinlichkeit, Schwachstellen zu übersehen bei einem Black-Box-Ansatz immer noch höher und einige Probleme lassen sich möglicherweise nur vage verifizieren.

Proprietäre Kommunikationsprotokolle sind ebenfalls Teil der Prüfung. Dabei geht es um Man-in-the-Middle-Angriffe, das Abhören der Kommunikation, die verwendete Kryptographie und den Authentifizierungsprozess. Zu den durchgeführten Tests gehören unter anderem sichere Authentifizierung, sichere Kommunikation (Verschlüsselung), Authentifizierungsmechanismen, Prüfung des Sitzungsmanagements, Integritätsprüfungen. Falls erforderlich, werden Gegenstellen für Kommunikationsschnittstellen eingerichtet und in einem kleinen Labor geprüft.

Die Kommunikation basiert auf einer Fülle von standardisierten, offenen oder proprietären Kommunikationsprotokollen unter Verwendung von Schnittstellen, wie beispielsweise:

- Ethernet, WLAN & Mobilfunktechnologie
- Bluetooth & Bluetooth Low Energy (BLE)
- Universal Serial Bus (USB)
- Radio-Frequency Identification (RFID) & Near Field Communication (NFC)
- Serielle Schnittstellen (e.g., RS-232)
- Debugging-Schnittstellen (e.g., UART, JTAG)

7.3 Methodologie: Hardware und eingebettete Systeme

Die Prüfung von Hardware-Komponenten erfolgt in der Regel in zwei Schritten, die im Folgenden beschrieben werden. Abhängig von der Komplexität eines Geräts oder einer Plattform werden die Schritte auch auf jede Unterkomponente angewendet. Auf diese Weise können auch komplexe Systeme nach dem Prinzip *Teile und Herrsche* zuverlässig bewertet werden.

Ein zentraler Aspekt sind Untersuchungen an passiven und aktiven Komponenten, die innerhalb des Geräts verwendet werden sowie die Erstellung eines groben Funktionskonzepts. Es wird nach öffentlich zugänglicher Dokumentation gesucht, wobei eine Sammlung aller verwendeten Komponenten erstellt wird, um dokumentierte Schnittstellen abzubilden und potenzielle Sicherheitsmerkmale zu identifizieren. Darüber hinaus werden auffällige Pins, Kontakte und Header auf der Leiterplatte/dem Gerät identifiziert und mit den zugehörigen Chips und deren Funktion dokumentiert.

7.3.1 Aktive Analyse der identifizierten Schnittstellen

Alle identifizierten Schnittstellen werden hinsichtlich ihrer Funktionalität und Nutzung bewertet. Identifizierte Header werden für die aktive Kommunikation mit dem Gerät verwendet, wobei jede einzelne Pin-Pad-Funktion gekennzeichnet wird. Zugängliche Schnittstellen werden verwendet, um Daten zu extrahieren und mit dem Gerät zu kommunizieren. Wenn möglich, beinhaltet dies auch die Extraktion von Konfigurationsdaten und Firmware.

Ein weiterer Aspekt dieses Schrittes ist der Einsatz von Logikanalysatoren, um die Kommunikationswege der einzelnen Komponenten zu überwachen und Systembefehle und -parameter zu identifizieren.

7.3.2 Manueller Zugriff auf Speicherkomponenten

Speicherchips, die in den vorangegangenen Schritten identifiziert wurden, auf die jedoch über die verfügbaren Busse nicht zugegriffen werden konnte, werden physisch aus der Schaltung entfernt. Dann werden alle verfügbaren Daten über die vom Chip unterstützten Protokolle extrahiert.

7.4 Methodologie: Mobile Applikationen

Die meisten mobilen Anwendungen, die in medizinischen Kontexten eingesetzt werden, verarbeiten vertrauliche oder sensible Daten und kommunizieren mit Cloud-Backends oder Medizinprodukten. Mobile Applikationen werden mit dem folgenden Ansatz bewertet, der die relevantesten Aspekte abdeckt.

7.4.1 Statische Analyse

Bei der statischen Analyse werden alle Dateien, die von der Anwendung/dem Container lokal gespeichert wurden, im Detail analysiert. Zu diesem Zweck werden die Dateien extrahiert und je nach Format entpackt oder entschlüsselt. Anschließend werden alle Dateien auf potenziell kritische Informationen (z. B. Zugangsdaten, URLs) gescannt.

Für verschiedene Zustände der App wird eine statische Analyse durchgeführt. In diesem Zusammenhang lässt sich der Zustand einer Anwendung am besten durch den Unterschied zwischen einer kürzlich installierten, aber unbenutzten Version einer Anwendung beschreiben, im Gegensatz zur gleichen Anwendung, nachdem sie ein Benutzer zum ersten Mal konfiguriert und verwendet hat.

Die statische Analyse zielt darauf ab festzustellen, wie eine Anwendung sowohl mit persistenten Dateien/Daten (wie Anmeldeinformationen) als auch mit temporären Dateien umgeht.

7.4.2 Dynamische Analyse

Bei der dynamischen Analyse oder Laufzeitanalyse wird eine Anwendung/ein Container mit Debuggern oder speziellen Tools wie *snoop-it* analysiert. Während der Analyse werden Variablen, Prozesse und Funktionen während der Laufzeit manipuliert. Ein Kernaspekt der dynamischen Analyse ist die Interaktion mit der eigentlichen GUI der Anwendung, in der böswillige und fehlerhafte Eingaben verwendet werden, um potenzielle Fehler und Risiken zu identifizieren. Die dynamische Analyse bezweckt die Datenverarbeitung während der Laufzeit und die Effizienz der lokalen Zugriffskontrollen und Eingabevalidierungen zu bewerten.

7.4.3 Analyse der Kommunikation

Während der Kommunikationsanalyse wird eine Proxy-Einstellung verwendet, um alle Daten von und zu der Anwendung über einen vom Angreifer kontrollierten Proxy umzuleiten. Daten, die per HTTPS übertragen werden oder durch SSL oder TLS geschützt sind, werden, wenn möglich, entschlüsselt. Wenn die Anwendung die Proxy-Einstellungen des Geräts ignoriert, wird der Datenverkehr durch einen transparenten Proxy geleitet. Diese Kommunikationsanalyse zielt darauf ab Fehler, in Bezug auf Daten, während der Kommunikation zu identifizieren und die Menge und Art der übertragenen Daten zu bewerten.

Apps können Daten auch über andere Kommunikationskanäle, wie Bluetooth oder NFC übertragen. Die entsprechende Kommunikation durchläuft nicht den Angriffsproxy. Daher muss diese Kommunikation mit anderen Mitteln analysiert werden, z. B. durch Analyse der relevanten Funktionen der Anwendung mittels statischer Analyse (siehe Abschnitt 7.4.1). Die Kommunikation kann auch mit spezieller Hardware analysiert werden, die ein Mitschneiden des Datenverkehrs ermöglicht. Danach kann der aufgezeichnete Verkehr weiter analysiert werden.

7.4.4 Testen der Implementierung

Implementierungstests werden verwendet, um Fehler in einem Programm zu finden, indem fehlerhafte Daten (halb-) automatisiert gesendet und das Verhalten eines Systems, das diese Daten verarbeitet, geprüft wird. Dieses so genannte *Protokoll-Fuzzing* verändert die Werte eines an das Ziel gesendeten Pakets und kann Werte enthalten, mit denen die Komponente nicht umgehen kann (z. B. mit der Folge eines Absturzes). Der Implementierungstest überprüft die korrekte Verarbeitung von Paketen sowohl in der Netzwerk-, als auch in der Anwendungsschicht.

7.5 Methodologie: Web Applikationen

Web-Anwendungen werden im medizinischen Kontext, wie z. B. Patientenportalen, eingesetzt. Sie verarbeiten vertrauliche oder sensible Daten und kommunizieren mit Cloud-Backends oder Medizinprodukten in der Nähe. Darüber hinaus können administrative Web-Anwendungen zur Verwaltung der Betriebsumgebung von Medizinprodukten, wie z. B. in Krankenhausnetzwerken, existieren. In diesem Abschnitt wird der Schwerpunkt der IT-Sicherheitsprüfung verschiedener Web-Anwendungen erläutert.

7.5.1 Dokumentation und automatisierte Bewertung

Auf der Grundlage einer manuellen, simulierten Nutzung der Anwendung wird ihre Struktur dokumentiert, um potenzielle Angriffsvektoren zu identifizieren (siehe Abschnitt 7.1). Dokumentiert werden z. B. URLs, http-Request-Methoden, (Transport-) Verschlüsselung (z. B. SSL), Anfrageparameter und verwendete Cookies. Diese Dokumentation wird für alle weiteren manuellen Tests verwendet.

Eine automatisierte Bewertung wird mit Hilfe eines Web-Application-Vulnerability-Scanners durchgeführt, der die Anwendung anhand der dokumentierten Struktur untersucht. Die Ergebnisse werden manuell verifiziert und, falls erforderlich und angemessen, durch zusätzliche Tests eines erfahrenen Prüfers unterstützt, um falsch positive Ergebnisse zu eliminieren und die tatsächlichen Schwachstellen zu verifizieren.

Der automatisierte Scan umfasst *Spidering* (d. h. die Identifizierung von Endpunkten innerhalb der Anwendung durch automatisiertes Verfolgen von Links innerhalb der Anwendung) der Web-Anwendung und die Identifizierung von Parametern in Formularfeldern oder Abfrageparametern. Weiterhin werden Webserver-Schwachstellen bewertet. Grundlegende Tests für Injection-Angriffe (SQL Injection, Cross-Site Scripting, ...) und unerwünschtes Verhalten, wie z. B. das Verursachen von Anwendungsfehlern, werden durchgeführt. Potentiell anfällige Funktionalitäten, wie Datei-Uploads und -Downloads werden identifiziert und Informationen in Fehlermeldungen, Stack-Traces oder HTML-Kommentaren gesammelt.

7.5.2 Clientseitige und serverseitige Maßnahmen

Viele Web-Anwendungen implementieren Maßnahmen auf der Client-Seite. Diese prüfen, ob sicherheitsrelevante Kontrollen, die auf der Client-Seite implementiert sind, auch auf der Server-Seite vorhanden sind. Die Prüfung umfasst unter anderem URL-Parameter, HTTP-Cookies, HTTP-Header, versteckte Felder, Längenbeschränkungen in Formularfeldern oder Validierungen in Client-Skripten.

7.5.3 Authentifizierung

Die Authentifizierungsmechanismen eines Webservers oder einer Anwendung werden auf potenzielle Angriffe und Nichteinhaltung von Best Practices analysiert. Die Prüfung umfasst die folgenden Punkte, ist aber nicht beschränkt auf diese:

- Stärke der implementierten Methode(n)
- Wörterbuch- oder Brute-Force-Angriffe einschließlich angepasster Wörterbücher
- Zertifikatsprüfungen (Schlüssellänge, vertrauenswürdige CA, Chiffrierstärke, Erweiterungen)
- Verfahren zum Zurücksetzen des Passworts
- Passwort-Richtlinien
- Festcodierte Anmeldeinformationen
- Hersteller- und Dienstleistungskonten
- Man-in-the-Middle-Angriffe

7.5.4 Session Management

Das Session-Management der Web-Anwendung wird hinsichtlich der nachfolgenden Punkte analysiert:

- Vorhersagbarkeit von Session-Token
- Verschlüsselte Übertragung der Sitzungs-Token, einschließlich der Analyse auf geeignete Verschlüsselungsmethoden
- Cookie-Attribute
- Beendigung der Sitzung
- Cross-Site Request Forgery/Session Fixation

7.5.5 Zugriffskontrollen und Rollenmanagement

Implementiert eine Web-Anwendung verschiedene Benutzerrollen (z. B. Admin, Standardbenutzer, Gastbenutzer), muss geprüft werden, ob Zugriffskontrollen sorgfältig implementiert sind und auch durchgesetzt werden. Für die Durchführung dieser Tests sind mindestens zwei Benutzerkonten (A, B) für jede Rolle erforderlich. Die folgenden Tests zur Prüfung auf potentielle Rechteerweiterungen werden durchgeführt:

- Vertikale Rechteerweiterung: Sind Administratorfunktionalitäten für niedrig privilegierte oder anonyme Benutzer zugänglich?
- Horizontale Rechteerweiterung: Kann Benutzer A auf Daten von Benutzer B zugreifen?

7.5.6 Injection-Angriffe

Automatisierte Tools sind nicht in der Lage alle Schwachstellen einer Web-Anwendung aufzudecken. Daher ist es notwendig, dass alle Eingabeparameter manuell weiter analysiert werden. Manuelles Testen umfasst eine allgemeine Bewertung des Eingabevalidierungskonzepts (Design und tatsächliche Implementierung), SQL-Injection, Cross-Site-Scripting (XSS), LDAP-Injection, OS Command Injection, File Inclusion, Path Traversal oder Template Injection. Dies hängt stark von der spezifischen Anwendung, ihrer Technologie und ihrer Komplexität ab.

7.5.7 Logikfehler

Logische Fehler innerhalb einer Web-Anwendung resultieren aus vorgegebenen Abläufen, die von den Entwicklern implementiert wurden. Während der Prüfung werden diese Abläufe modifiziert und das Verhalten der Anwendung wird überprüft. Typische Tests umfassen:

- Manipulation von HTTP-Headern
- Löschung von Parametern
- Prüfung von mehrstufigen Funktionen durch z. B. Ändern der Reihenfolge
- Absichtliches Verursachen von Fehlern
- Bewertung der Upload- und Download-Funktionalität
- Bewertung der Update- und Konfigurationsexport- oder -importfunktionalität.

7.5.8 Preisgabe von Informationen

Während der umfangreichen Prüfung wird die Ausgabe von Informationen aus der Web-Anwendung überwacht, die eigentlich nicht verfügbar sein sollten, wie z. B. Versionsinformationen, interne Hostnamen,

IP-Adressen, Standard-Dateien/Ordner/Inhalte und Quellcode. Solche Informationen können von einem Angreifer verwendet werden, um weitere Angriffe vorzubereiten.

7.5.9 Untersuchung von Applikationsservern

Zu den Tests, die für den Web-/Anwendungsserver durchgeführt werden, gehören unter anderem auch Tests auf bereits bekannte Schwachstellen, Identifizierung von Standardinhalten, Black-Box-Test für unsichere Konfigurationen und die Prüfung auf eine unsichere SSL/TLS-Konfiguration.

7.6 Methodologie: Infrastruktur, Netzwerk & Server

Alle Netzwerkinfrastruktur- und Serversysteme werden sowohl auf System-, als auch auf Protokollebene auf Konfigurationsfehler und bekannte Schwachstellen überprüft. Anfangs werden automatisierte Werkzeuge eingesetzt. Die Ergebnisse ermöglichen eine vertiefte Analyse der entdeckten Systeme, die auf der Grundlage der Erfahrungen der Prüfer und spezialisierter oder speziell entwickelter Werkzeuge durchgeführt wird.

Die Prüfung umfasst das Betriebssystem, Authentifizierungsprüfungen, Prüfungen auf Standardkonten, Aufzählung und Test laufender Dienste, Konfigurationsfehler, Verwendung unsicherer Administrationsmethoden, wie z. B. Telnet, über nicht vertrauenswürdige Netzwerke oder Protokoll-Fehlkonfigurationen sowie Schwachstellen auf der Netzwerkebene.

8 Anhang

In diesem Teil werden zusätzliche Informationen, weitere Referenzen oder ergänzendes Material zur Verfügung gestellt.

8.1 Liste von Sicherheitsmeldungen und weiteren Ressourcen

In den folgenden Abschnitten sind die im Rahmen des ManiMed-Projekts entstandenen Sicherheitshinweise und Sicherheitsmeldungen (siehe Abschnitt 8.1.1), Publikationen, Blog-Einträge und Artikel (siehe Abschnitt 8.1.2) sowie Vorträge, Präsentationen und Interviews (siehe Abschnitt 8.1.3) aufgeführt.

Alle Schwachstellen wurden durch Julian Suleder, Birk Kauer, Nils Emmerich, Raphael Pavlidis, Linda Huischen, Jens Beyermann, Florian Bausch, Gregor Debus, Dennis Kniel, Dr. Andreas Dewald der ERNW Research GmbH sowie Dr. Oliver Matula und Dennis Mantz der ERNW Enno Rey Netzwerke GmbH identifiziert.

8.1.1 Security Advisories and Notifications

Die folgenden Sicherheitshinweise wurden von Herstellern oder dem ICS-CERT veröffentlicht:

- SOOIL Development Co. Ltd. Via Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM): **Dringende Sicherheitsinformation zu Insulinpumpe DANA Diabecare RS;mobilen Anwendung AnyDANA von SOOIL Development Co. Ltd.** May 08, 2020. Online: https://www.bfarm.de/SharedDocs/Kundeninfos/DE/07/2020/17203-19_kundeninfo_de.html
- ICS-CERT. **ICS Medical Advisory (ICSMA-20-254-01) Philips Patient Monitoring Devices**. September 10, 2020. Online: https://us-cert.cisa.gov/ics/advisories/icsma-20-254-01
- ICS-CERT. **ICS Medical Advisory (ICSMA-20-296-01) B. Braun OnlineSuite.** October 22, 2020. Online: https://us-cert.cisa.gov/ics/advisories/icsma-20-296-01
- ICS-CERT. **ICS Medical Advisory (ICSMA-20-296-02) B. Braun SpaceCom, Battery Pack SP with Wi-Fi, and Data module compactplus.** October 22, 2020. Online: https://us-cert.cisa.gov/ics/advisories/icsma-20-296-02
- B. Braun Melsungen AG. **B. Braun Vulnerability Disclosure Statement – Security Advisory.** Online: https://www.bbraun.com/en/products-and-therapies/services/b-braun-vulnerability-disclosure-policy/security-advisory.html

8.1.2 Publikationen

Die folgenden Publikationen wurden im Rahmen des Projekts ManiMed bereits veröffentlicht:

- Julian Suleder. **ERNW Whitepaper 69: Safety Impact of Vulnerabilities in Insulin Pumps**. September 12, 2020. Online: https://ernw-research.de/en/whitepapers/issue-69.html. Demo Video: https://www.youtube.com/watch?v=0GMe2poiYtE
- Julian Suleder. **Blog Post: Medical Device Security: HL7v2 Injections in Patient Monitors.** April 23, 2020. Online: https://insinuator.net/2020/04/hl7v2- injections-in-patient-monitors/.
- Julian Suleder, Dina Truxius. **Security Vulnerabilities in Medical Devices - Perspectives of IT Security Researchers.** PM QM 03/2020. In Press.
- Julian Suleder. **Kritische Schwachstellen in medizinischen Geräten – Erfahrungen eines IT-Sicherheitsforschers.** medizin://dokumentation/ informatik/ informationsmanagement/ (mdi).

Fachverband für Dokumentation und Informationsmanagement in der Medizin (DVMD) e.V. In Press.

8.1.3 Vorträge

Die folgenden Vorträge wurden im Zusammenhang mit dem Projekt ManiMed bisher gehalten:

- Julian Suleder, Dina Truxius. **Entdeckung und Veröffentlichung von Sicherheitslücken in einer Insulinpumpe.** IT-Tage 2020. December 10, 2020. Frankfurt, Germany (Online).
- Dina Truxius. **Cybersicherheit Medizintechnik und Ergebnisse aus dem BSI-Forschungsprojekt ManiMed.** Virtual MEDICA 2020. November 17, 2020. Düsseldorf, Germany (Online)
- Julian Suleder, Dina Truxius. **Hijacking an Insulin Pump: From Discovery to Disclosure.** INFOSEK 2020. September 30, 2020. Nova Gorica, Slovenia (Online).
- Julian Suleder, Dina Truxius. **A Million Boluses: Discovery and Disclosure of Vulnerabilities in an Insulin Pump.** HITCON 2020. September 11, 2020. Taipeh, Taiwan (Online). Online: https://www.youtube.com/watch?v=akdCGDuOSvA
- Julian Suleder, Dina Truxius**. Hijacking an Insulin Pump: From Discovery To Disclosure.** September 6, 2020. GMDS & CEN-IBS 2020: 65th Annual Meeting of the German Association for Medical Informatics, Biometry and Epidemiology (GMDS), Meeting of the Central European Network (CEN: German Region, Austro-Swiss Region and Polish Region) of the International Biometric Society (IBS) including the 66th Biometric Colloquium of the German Region. Berlin, Germany (Online).
- Dina Truxius, Julian Suleder, Mike Rushanan. **DIY Diabetics and a Million Boluses.** DEF CON Biohacking Village. August 8, 2020. Las Vegas, USA (Online). Online: https://www.youtube.com/watch?v=4a2Kmq74z5A
- GMDS SIG Consumer Health Informatics (CHI): **DIY Digital Health: 5 Fragen an Dina Truxius & Julian Suleder. Digital Panel DIY Digital Health - Helfen wir uns einfach selbst?!** Interview 3 - Risiken und Manipulation von vernetzter Medizintechnik. August 3, 2020. Heidelberg, Germany (Online). Online: https://www.gmds.de/aktivitaeten/medizinische-informatik/arbeitsgruppenseiten/consumer-health-informatics-chi/workshops-veranstaltungen/digital-panel-diy-digital-health/#c6915

8.2 Vorlage Anschreiben Krankenhäuser

Die folgende Vorlage wurde für die Briefe verwendet, die an ausgewählte Krankenhäuser in Deutschland geschickt wurden.

BSI-Projekt ManiMed: Sicherheitsanalyse vernetzter Medizinprodukte

Die digitale Vernetzung ist in vielen Lebensbereichen bereits weit verbreitet. Auch in der Gesundheitsbranche werden immer mehr medizinische Geräte vernetzt, sodass die Zahl der medizinischen High-Tech-Geräte in Krankenhäusern kontinuierlich steigt. Unsere Forschung zeigt, dass medizinische Geräte meist nur über grundlegende Sicherheitsmechanismen verfügen. Im klinischen Umfeld sind dies unter anderem Medikationspumpen, Implantate oder medizinische Großgeräte, wie z. B. CT und MRT. Gerade im klinischen Umfeld ist das hochkomplexe und kritische Einsatzgebiet sowie die lange Lebensdauer und intensive Nutzung der Geräte ein ernstzunehmendes Problem, da nicht selten grundlegende Sicherheitsmaßnahmen fehlen. Ein defektes oder manipuliertes Gerät kann eine massive Bedrohung für das Leben eines Patienten darstellen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) strebt in seiner Rolle als zentrale IT-Sicherheitsbehörde des Bundes eine Sensibilisierung von Herstellern und Bevölkerung bezüglich der IT-Sicherheitsrisiken von vernetzten Medizinprodukten an. Als eine Reaktion auf die häufig fatalen Sicherheitsmeldungen von vernetzten Medizinprodukten, initiierte das BSI die Ausschreibung des Projekts Manipulation von Medizinprodukten – ManiMed und wählte uns als Auftragnehmer aus. In diesem Projekt soll eine Analyse der IT-Sicherheit dieser Produkte durch stichprobenartige Security Assessments durchgeführt werden.

Für die Auswahl der Medizinprodukte möchten wir eine möglichst reale Abbildung der im klinischen Alltag genutzten Geräte erreichen, um mit dem Projekt den größten Mehrwert zu erzielen, da der gesellschaftliche Mehrwert der Identifikation von Sicherheitslücken in häufiger genutzten Geräten deutlich größer, als in weniger verbreiteten Geräten ist.

Sie können als Anwender von Medizinprodukten in Deutschland einen bedeutenden Mehrwert für die Gesellschaft schaffen. Wenn für die Untersuchungen Geräte ausgewählt werden können, die von Ihnen verwendet werden, profitieren Sie selbst davon, da beseitigte Schwachstellen in Geräten einen Sicherheitszugewinn auch für Sie/Ihre Patienten bedeutet.

Aus diesem Grund möchten wir Sie bitten uns mitzuteilen, welche vernetzten Medizingeräte Sie in den letzten fünf Jahren erworben haben oder planen in Zukunft zu erwerben. Auch bereits eine Auswahl an Geräten stellt eine große Hilfe dar. Wir können Ihnen versichern, dass wir mit den Informationen im höchsten Maße vertraulich umgehen werden.

Sehr gerne stehe ich zusammen mit dem BSI für Rückfragen zur Verfügung und freue mich auf Ihre Rückmeldung!

Freundliche Grüße,

_____

8.3 Fragebogen

Es gibt zwei Versionen des Fragebogens: eine lange und eine kurze Version. Die Langfassung des Fragebogens wurde an Anbieter bestimmter Gerätekategorien verschickt, bei denen die Internetrecherche und die Recherche über die MPA-Datenbank nicht die erforderlichen Informationen lieferten. Als Alternative wurde eine Kurzversion erstellt, falls die Hersteller nicht auf die Langfassung antworten wollten.

Die folgenden Fragen waren Teil der Langfassung des Fragebogens (die Fragen wurden in deutscher Sprache an die Anbieter versandt.

1. Hardware

1.1 Besitzt das Produkt Ethernet-Schnittstellen? Falls ja, bitte Spezifikationen bereitstellen.

1.2 Besitzt das Produkt WLAN-Schnittstellen? Falls ja, bitte Spezifikationen bereitstellen.

1.3 Besitzt das Produkt Bluetooth-Schnittstellen? Falls ja, bitte Spezifikationen bereitstellen.

1.4 Besitzt das Produkt RFID bzw. NFC-Schnittstellen? Falls ja, bitte Spezifikationen bereitstellen.

1.5 Besitzt das Produkt Mobilfunkmodule (z. B. 2G, 3G, 4G)? Falls ja, bitte Spezifikationen bereitstellen.

1.6 Besitzt das Produkt USB-Schnittstellen? Falls ja, bitte Spezifikationen bereitstellen.

1.7 Besitzt das Produkt Thunderbolt-Schnittstellen? Falls ja, bitte Spezifikationen bereitstellen.

1.8 Besitzt das Produkt serielle Schnittstellen? Falls ja, bitte Spezifikationen bereitstellen.

1.9 Besitzt das Produkt Display-Schnittstellen (z. B. VGA, HDMI, Display Port)? Falls ja, bitte Spezifikationen bereitstellen.

1.10 Besitzt das Produkt weitere Hardware-Schnittstellen (inkl. funkfähiger Schnittstellen)?

1.11 Besitzen die Prozessoren des Produkts Debugging-Schnittstellen (z. B. UART, JTAG, SPI)?

1.12 Ist ein Trusted Platform Module (TPM) im Produkt verbaut?

1.13 Können externe Datenspeicher an das Produkt angeschlossen und genutzt werden (z. B. externe SD-Karte, externer USB-Speicher)?

1.14 Wird BIOS oder UEFI-Firmware innerhalb des Produkts genutzt?

1.15 Kann das Produkt von externen Datenspeichern booten?

1.16 Kann das Basisprodukt durch zusätzliche Komponenten erweitert werden?

1.17 Welche Prozessoren mit welcher Prozessorarchitektur (z. B. x86-64, ARM7, MIPS) werden verwendet? Bitte Spezifikationen für die Prozessoren bereitstellen.

2. Software

2.1 Welches Betriebssystem (inkl. Versionsnummer) wird auf dem Produkt verwendet (z. B. Windows Server 2016, Ubuntu Server 18.04.2 LTS)?

2.2 Besitzt das Produkt einen Web Server, auf den per Browser über eine der unter Abschnitt 1 genannten Schnittstellen zugegriffen werden kann?

2.3 Besitzt das Produkt einen Fernzugriffsdienst (z. B. Telnet, SSH, RDP), auf den mit einem geeigneten Programm über eine der unter Abschnitt 1 genannten Schnittstellen zugegriffen werden kann?

2.4 Gibt es externe Applikationen (z. B. in der Form von Mobile Apps), über die mit dem Produkt kommuniziert werden kann oder über die das Produkt konfiguriert werden kann?

2.5 Welche Programmiersprachen werden zur Entwicklung der Software-Dienste des Produkts verwendet (z. B. C/C++, Java, Python)?

2.6 Gibt es einen Update-Mechanismus der Software/Firmware des Produktes? Falls ja, bitte Details zum Mechanismus angeben.

2.7 Kann Software auf dem Produkt installiert werden, welche nicht durch den Hersteller autorisiert wurde?

English 2.7: Can software be installed on the product that is not authorized by the vendor?

3. Kommunikationskanäle (Communication Channels)

3.1 Kommuniziert das Produkt mit Systemen in einer privaten/öffentlichen Cloud?

3.2 Gibt es externe Software-Lösungen, die für den Betrieb des Produkts aufgesetzt werden müssen und mit denen das Produkt über eine der in Abschnitt 1 genannten Schnittstellen kommuniziert (z. B. eine externe Web Server-Komponente)?

3.3 Nutzt das Produkt unverschlüsselte Kommunikationskanäle?

3.4 Für verschlüsselte Kommunikationskanäle, welche kryptographischen Verfahren werden hier eingesetzt?

4. Sonstiges (Miscellaneous)

4.1 Welche Sicherheitsstandards (z. B. Common Criteria, Protection Profiles, Normen) erfüllt das Produkt?

4.2 Welche der folgenden Datentypen werden auf dem Produkt verarbeitet:

4.2a Demographische Daten (z. B. Name, Adresse, Anschrift)

4.2b Medizinische Daten (z. B. Anamnese, Befund, Bildgebung)

4.2c Sonstige vom Benutzer eingegebene Daten

4.3 Besitzt das Produkt eine Notfallfunktion ("break-glass"), um an die unter Punkt 4.2 beschriebenen Daten zu gelangen?

4.4 Hat das Produkt in der Vergangenheit Sicherheitslücken besessen, über die in der Presse öffentlich berichtet wurde?

4.5 Wurden für das Produkt IT-Sicherheitsüberprüfungen (z. B. in der Form von Penetrationstests) durchgeführt, über die in der Presse öffentlich berichtet wurde?

Die folgenden Fragen waren Teil der Kurzfassung des Fragebogens (die Fragen wurden in deutscher Sprache an die Anbieter geschickt; für jede Frage ist hier eine englische Übersetzung angegeben).

1. Hardware

1.1 Besitzt das Produkt Ethernet-Schnittstellen?

1.2 Besitzt das Produkt WLAN-Schnittstellen?

1.3 Besitzt das Produkt Bluetooth-Schnittstellen?

1.4 Besitzt das Produkt RFID bzw. NFC-Schnittstellen?

1.5 Besitzt das Produkt Mobilfunkmodule (z. B. 2G, 3G, 4G)?

1.6 Besitzt das Produkt USB-Schnittstellen?

1.7 Besitzt das Produkt Thunderbolt-Schnittstellen?

1.8 Besitzt das Produkt serielle Schnittstellen?

1.9 Besitzt das Produkt Display-Schnittstellen (z. B. VGA, HDMI, Display Port)?

1.10 Können externe Datenspeicher an das Produkt angeschlossen und genutzt werden (z. B. externe SD-Karte, externer USB-Speicher)?

1.11 Kann das Basisprodukt durch zusätzliche Komponenten erweitert werden?

2. Software

2.1 Welches Betriebssystem (inkl. Versionsnummer) wird auf dem Produkt verwendet (z. B. Windows Server 2016, Ubuntu Server 18.04.2 LTS)?

2.2 Besitzt das Produkt einen Web Server, auf den per Browser über eine der unter Abschnitt 1 genannten Schnittstellen zugegriffen werden kann?

2.3 Besitzt das Produkt einen Fernzugriffsdienst (z. B. Telnet, SSH, RDP), auf den mit einem geeigneten Programm über eine der unter Abschnitt 1 genannten Schnittstellen zugegriffen werden kann?

2.4 Gibt es externe Applikationen (z. B. in der Form von Mobile Apps), über die mit dem Produkt kommuniziert werden kann oder über die das Produkt konfiguriert werden kann?

2.5 Welche Programmiersprachen werden zur Entwicklung der Software-Dienste des Produkts verwendet (z. B. C/C++, Java, Python)?

2.6 Gibt es einen Update-Mechanismus der Software/Firmware des Produktes?

3. Kommunikationskanäle (Communication Channels)

3.1 Kommuniziert das Produkt mit Systemen in einer privaten/öffentlichen Cloud?

3.2 Gibt es externe Software-Lösungen, die für den Betrieb des Produkts aufgesetzt werden müssen und mit denen das Produkt über eine der in Abschnitt 1 genannten Schnittstellen kommuniziert (z. B. eine externe Web Server-Komponente)?

4. Sonstiges (Miscellaneous)

4.1 Welche Sicherheitsstandards (z. B. Common Criteria, Protection Profiles, Normen) erfüllt das Produkt?

4.2 Welche der folgenden Datentypen werden auf dem Produkt verarbeitet:

4.2a Demographische Daten (z. B. Name, Adresse, Anschrift)

4.2b Medizinische Daten (z. B. Anamnese, Befund, Bildgebung)

4.2c Sonstige vom Benutzer eingegebene Daten

4.3 Besitzt das Produkt eine Notfallfunktion ("break-glass"), um an die unter Punkt 4.2 beschriebenen Daten zu gelangen?

4.4 Hat das Produkt in der Vergangenheit Sicherheitslücken besessen, über die in der Presse öffentlich berichtet wurde?

4.5 Wurden für das Produkt IT-Sicherheitsüberprüfungen (z. B. in der Form von Penetrationstests) durchgeführt, über die in der Presse öffentlich berichtet wurde?

Literaturverzeichnis

ACS. (5. November 2019). *Sicherheit von Medizinprodukten*. Abgerufen am 07. August 2020 von Allianz für Cybersicherheit (ACS): https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/Expertenkreis_CyberMed_MDS2.pdf

BfArM. (4. August 2017). *Fehlerarten*. Abgerufen am 07. August 2020 von Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM): https://www.bfarm.de/DE/Service/Statistiken/MP_statistik/Problemanalyse/Fehlerarten/_node.html

BfArM. (3. April 2018). *Anzahl des Risikomeldungen in den letzten 10 Jahren*. Abgerufen am 07. August 2020 von Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM): https://www.bfarm.de/SharedDocs/Downloads/DE/Service/Statistik/MP-Statistik/statist-Auswert_Anzahl-Risikomel.jpg?__blob=poster&v=11

BfArM. (kein Datum). *Cybersicherheit von Medizinprodukten*. Abgerufen am 07. August 2020 von Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM): https://www.bfarm.de/DE/Medizinprodukte/RisikoerfassungUndBewertung/Cybersicherheit/kundeninfos_cybersicherheit_node.html

BfArM. (kein Datum). *Medical Devices*. Von https://www.dimdi.de/dynamic/en/medical-devices/ abgerufen

BfArM. (n.d.). *Medizinproduke-Informationssystem*. Retrieved August 07, 2020, from Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM): https://www.dimdi.de/dynamic/de/medizinprodukte/informationssystem/

BfArM. (kein Datum). *Medizinprodukte: Aufgaben des BfArM*. Abgerufen am 07. August 2020 von Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM): https://www.bfarm.de/DE/Medizinprodukte/RechtlicherRahmen/aufgaben/_node.html

Boehm, B. (1984, January). Software Engineering Economics. *IEEE Transactions on Software Engineering, SE-10*(1).

BSI. (2018, November 13). *Cyber Security Requirements for Network-Connected Medical Devices*. Retrieved August 07, 2020, from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/ICS/Medical_Devices_CS-E_132.pdf

BSI. (2018). *The State of IT Security in Germany 2018*. Retrieved August 07, 2020, from Federal Office for Information Security (BSI): https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2018.pdf;jsessionid=E4E6FB4442E4E9B535017DBA246282E2.1_cid502?__blob=publicationFile&v=3

BSI. (2019). *The State of IT Security in Germany 2019*. Retrieved August 07, 2020, from Federal Office for Information Security (BSI): https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2019.pdf

BSI. (2020). *The State of IT Security in Germany 2020*. Von Federal Office for Information Security (BSI): https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html abgerufen

Bundesgesetzblatt. (2. August 1994). *Gesetz über Medizinprodukte*. Abgerufen am 07. August 2020 von https://www.gesetze-im-internet.de/mpg/

Carnegie Mellon University. (2017, August). *Software Engineering Institute.* Retrieved August 07, 2020, from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330

Chase, M. P., & Coley, S. M. (2019, September). *Rubric for Applying CVSS to Medical Devices*. Retrieved August 07, 2020, from https://www.mitre.org/publications/technical-papers/rubric-for-applying-cvss-to-medical-devices

DDG. (14. November 2019). *Deutscher Gesundheitsbericht - Diabetes 2020: Die Bestandsaufnahme.* Abgerufen am 07. August 2020 von Deutsche Diabetes Gesellschaft (DDG) und diabetesDE – Deutsche Diabetes-Hilfe: https://www.deutsche-diabetes-gesellschaft.de/fileadmin/user_upload/06_Gesundheitspolitik/03_Veroeffentlichungen/05_Gesundheitsbericht/2020_Gesundheitsbericht_2020.pdf

DNB. (kein Datum). *Deutsche Nationalbibliothek*. Abgerufen am 31. 07 2020 von Deutsche Nationalbibliothek (DNB): https://www.dnb.de

ERNW Research GmbH. (17. September 2020). *Demo: Hijacking the DANA Diabecare RS Insulin Pump.* Von TROOPERScon - YouTube: https://www.youtube.com/watch?v=0GMe2poiYtE abgerufen

EUDAMED. (kein Datum). *Medical Devices - EUDAMED* . Abgerufen am 17. 09 2020 von https://ec.europa.eu/health/md_eudamed/overview_de

European Parliament and the Council of the European Union. (20. Juni 1990). *Richtlinie 90/385/EWG des Rates vom 20. Juni 1990 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über aktive implantierbare medizinische Geräte*. Abgerufen am 07. August 2020 von Official Journal of the European Union: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A31990L0385

European Parliament and the Council of the European Union. (14. Juni 1993). *Richtlinie 93/42/EWG des Rates vom 14. Juni 1993 über Medizinprodukte*. Abgerufen am 07. August 2020 von Official Journal of the European Union: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A31993L0042

European Parliament and the Council of the European Union. (27. Oktober 1998). *Richtlinie 98/79/EG des Europäischen Parlaments und des Rates vom 27. Oktober 1998 über In-vitro-Diagnostika*. Abgerufen am 07. August 2020 von Official Journal of the European Union: Richtlinie 98/79/EG des Europäischen Parlaments und des Rates vom 27. Oktober 1998 über In-vitro-Diagnostika

European Parliament and the Council of the European Union. (2017, April 5). *Regulation (EU) 2017/745 of the European Parliament and of the Council*. Retrieved August 07, 2020, from Official Journal of the European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745

European Parliament and the Council of the European Union. (2017, May 5). *Regulation (EU) 2017/746 of the European Parliament and of the Council on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU*. Retrieved August 07, 2020, from Official Journal of the European Union: https://eur-lex.europa.eu/eli/reg/2017/746/oj

FDA. (2016, December). *Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff.* Retrieved August 07, 2020, from Food and Drug Administration (FDA): https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices

FDA. (2020, March 3). *Cybersecurity*. Retrieved August 07, 2020, from Food and Drug Administration (FDA): https://www.fda.gov/medical-devices/digital-health/cybersecurity

FIRST. (2019, June). *Common Vulnerability Scoring System version 3.1: Specification Document*. Retrieved August 07, 2020, from Forum of Incident Response and Security Teams (FIRST): https://www.first.org/cvss/specification-document

Grunow, F. (2015, July 1). *The patient's last words: I am not a target!* Retrieved August 07, 2020, from Insinuator: https://insinuator.net/2015/07/the-patients-last-words-i-am-not-a-target/

IQTIG. (2016). *Jahresbericht 2016 des Deutschen Herzschrittmacher- und Defibrillatorregister - Teil 1 Herzschrittmacher*. Abgerufen am 07. August 2020 von Institut für Qualitätssicherung und Transparenz im Gesundheitswesen (IQTIG): https://pacemaker-register.de/wp-content/uploads/Jahresbericht-2016-des-Deutschen-Herzschrittmacher-und-Defibrillatorregister-Teil-1-Herzschrittmacher.pdf

ISO/IEC. (1994, November 15). *ISO/IEC 7498-1:1994 - Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*. Retrieved August 07, 2020, from https://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip

ISO/IEC. (2013). *ISO/IEC 27001, Second Edition*. Retrieved 09 25, 2020

ISO/IEC. (2018, September 25). *ISO/IEC 27000, Fifth Edition*. Retrieved 2020, from https://www.iso.org/standard/73906.html

ISO/IEC. (2018). *ISO/IEC 27005, Third Edition*. Retrieved August 07, 2020, from https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en:sec:2

MDCG. (2019, December). *Guidance on Cybersecurity or medical devices*. Retrieved August 07, 2020, from Medical Device Coordination Group (MDCG): https://ec.europa.eu/docsroom/documents/41863

MEDICA. (2019). *Produktkategorien*. Abgerufen am 07. August 2020 von https://www.medica.de/de/Firmen_Produkte/Produkte/Produktkategorien

NCBI. (n.d.). *National Library of Medicine*. Retrieved August 07, 2020, from National Center for Biotechnology Information (NCBI): https://pubmed.ncbi.nlm.nih.gov/

NEMA. (2019, October 8). *Manufacturer Disclosure Statement for Medical Device Security*. Retrieved August 07, 2020, from National Electrical Manufacturers Association (NEMA): https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx

Rios, B., & Butts, J. (2018, August 9). *Understanding and Exploiting Implanted Medical Devices*. Retrieved August 07, 2020, from https://www.blackhat.com/us-18/briefings/schedule/index.html#understanding-and-exploiting-implanted-medical-devices-11733

Shannon, C. (1949, October 4). Communication Theory of Secrecy Systems. *Bell System Technical Journal, 28*.

SOOIL Development Co. Ltd. (8. May 2020). *Dringende Sicherheitsinformation zu Insulinpumpe DANA Diabecare RS;mobilen Anwendung AnyDANA von SOOIL Development Co. Ltd.* Abgerufen am 07. August 2020 von Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM): https://www.bfarm.de/SharedDocs/Kundeninfos/DE/07/2020/17203-19_kundeninfo_de.html

Suleder, J. (2020, September 11). *ERNW Whitepaper 69: Safety Impact of Vulnerabilities in Insulin Pumps.* Retrieved August 07, 2020, from https://ernw-research.de/en/whitepapers/issue-69.html

Suleder, J. (2020, April 23). *Medical Device Security: HL7v2 Injections in Patient Monitors.* Retrieved August 07, 2020, from Insinuator Blog: https://insinuator.net/2020/04/hl7v2-injections-in-patient-monitors/

Suleder, J., Dewald, A., & Grunow, F. (2018, April 25). *ERNW Whitepaper 66: Medical Device Security - A Survey of the current State*. Retrieved August 07, 2020, from ERNW Enno Rey Netzwerke GmbH: https://static.ernw.de/whitepaper/ERNW_Whitepaper66_Medical_Device_Security_signed.pdf

SZ. (23. Juni 2015). *Nächtliches Desaster*. Abgerufen am 07. August 2020 von Süddeutsche Zeitung (SZ): https://www.sueddeutsche.de/wirtschaft/medizintechnik-naechtliches-desaster-1.2534424

WHO. (2011). *Ventilator, Intensive Care.* Retrieved August 07, 2020, from World Health Organization (WHO): https://www.who.int/medical_devices/innovation/ventilator_intensive_care.pdf