Federal Office
for Information Security

Deutschland
Digital•Sicher•BSI•

Cyber Security Review of Network-Connected Medical Devices

BSI-Project 392: Manipulation of Medical Devices (ManiMed)

Change history

Version	*Date*	*Name*	*Description*
1.0	December 11, 2020	Dr. Dina Truxius, BSI Emanuel Müller, BSI Dr. Nikolai Krupp, BSI Julian Suleder, ERNW Dr. Oliver Matula, ERNW Dennis Kniel, ERNW	First version

Table 1: Change history

Federal Office for Information Security
Post Box 20 03 63
D-53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: referat-di24@bsi.bund.de
Internet: https://www.bsi.bund.de

Content

List of Figures

List of Abbreviations

Abbreviation	Definition
ACS	Alliance for Cyber Security
AD	Active Directory
ADT	Admit Discharge Transfer
AG	Aktiengesellschaft (Joint-stock company)
API	Application Programming Interface
ARM	Avanced RISC Machines
ASLR	Address Space Layout Randomization
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte (Federal Institute for Drugs and Medical Devices)
BLE	Bluetooth Low Energy
BIOS	Basic Input/Output System
BMG	Bundesministerium für Gesundheit (Federal Ministry of Health)
BMI	Bundesministerium des Inneren, Bau und Heimat (Federal Ministry the Interior, Building and Community)
BSI	Bundesministerium für Sicherheit in der Informationstechnik (Federal Office for Information Security)
BTS	Base Transceiver Station
CA	Certificate Authority
CERT	Computer Emergency Response Team
CISA	Cybersecurity and Infrastructure Security Agency
COVID	Coronavirus Disease
CS	Cyber-Sicherheitsanforderungen (Cybersecurity requirements)
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 (German Diabetes Association)
DEP	Data Execution Prevention
DICOM	Digital Imaging and Communications in Medicine
DIMDI	Deutsches Institut für Medizinische Dokumentation und Information (German Institute for Medical Documentation and Information)
DMEA	Digital Medical Expertise & Applications

Abbreviation	Definition
DNB	Deutsche Nationalbibliothek (German National Library)
DoS	Denial of Service
DSP	Digital Signal Processing
EC	European Counsil
ECG	Electrocardiogram
EEC	European Economic Community
EEG	Electroencephalography
EG	Europäische Gemeinschaft (European Community)
EMR	Electronic Medical Record
EU	European Union
EUDAMED	European Databank on Medical Devices
EWG	Europäische Wirtschaftsgemeinschaft (European Economic Community)
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

Abbreviation	Definition
IT	Information Technology
JTAG	Joint Test Action Group
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

Abbreviation	Definition
SD	Secure Digital
SDL	Software Development Lifecycle
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

Table 1: List of Abbreviations

1 Introduction

Vulnerabilities in IT systems can exist at any given time. Even medical devices are no exception. Discovered IT-security vulnerabilities in networked medical devices are usually of great concern as their exploitation could have an impact on patient safety or on their environment, e.g. hospital network. This document presents the results of the *BSI project 392: Manipulation of Medical Devices (ManiMed)*, which casts light on the IT security of certain devices. This project's objective is to assess the current state of the IT security posture for network-connected medical devices that have recently been approved for the German market and IT security-related processes.

Since the German market of connected medical devices has grown significantly over the last years (BSI, 2018), a market analysis was performed to identify relevant medical devices for the assessment since not all existing devices in Germany could be assessed as part of this project. The results of the market analysis were used to select ten devices from five different categories (two devices per category). The five categories addressed within this project are:

- implantable pacemakers and equipment
- insulin pumps
- ventilators
- infusion pumps
- patient monitors.

The selected devices (including infrastructure components required for their operation) were evaluated in an IT security assessment. The vulnerabilities that were identified as part of the assessment were responsibly disclosed. The project partners worked closely together with the manufacturers to ensure a timely fix of the vulnerabilities. In total, more than 150 vulnerabilities have been identified in scope of project ManiMed.

Apart from the current IT-security state of selected medical devices, project ManiMed demonstrates strategies how subsequent remediation and disclosure processes can be handled and coordinated. The results may allow for a critical review of internal processes, IT-security maturity, and future decisions. The overall goal is to keep IT-security in medical device on a high level and encouraging for constant improvement.

1.1 Motivation

Digital networking is already widespread in many areas of life. In the healthcare industry, a clear trend towards networked medical devices is noticeable so that the number of connected high-tech devices in, e.g., hospitals, medical practices, and medical care centers is steadily increasing (BSI, 2018). These include infusion pumps, implants, and large medical equipment such as computer tomography and magnetic resonance imaging systems in clinical settings. Apart from the device's usual risk of failures due to extensive usage over a prolonged service life, their interconnectivity poses new risks that were previously not existent. If any device software or hardware or their accompanying infrastructure exhibits flaws, malicious actors may exploit these vulnerabilities, thereby threatening patient's safety. However, if a vulnerability does not directly affect a patient's safety, it may still allow obtaining and leaking sensitive patient data.

The German Federal Office for Information Security (BSI), in its role as the federal IT security authority in Germany, aims to sensitize manufacturers and the public regarding security risks of networked medical devices. In response to the often fatal security reports of networked medical devices (BSI, 2018), (BSI, 2019), (Suleder, Dewald, & Grunow), the BSI initiated the project *Manipulation of Medical Devices (ManiMed)*. In this project, a security analysis of selected products is carried out through security assessments to gain insights into the IT security posture of network-connected medical devices on the

German market. Further disclosure processes are coordinated with eleven manufacturers to raise the awareness towards processes to improve the overall IT-security in medical devices.

1.1.1 The State of IT Security in Germany

As stated in the last three versions of the document *The State of IT Security in Germany* published by the Federal Office for Information Security (BSI, 2020; BSI, 2019; BSI, 2018), there is a clear trend to allow doctors, medical staff, or patients themselves to access data of medical devices via mobile applications. In individual cases, the mobile application can even be used to control the medical device.

The collected data might be transmitted to a cloud backend, where it can either be processed further or made available to doctors or medical staff, who are no longer required to be physically present for analyzing this data.

However, as more of these smart medical devices are launched on the market every year, attacks with impacts on privacy and safety are likely to increase. As stated in the 2018 report, such attacks are possible due to missing or weak authentication mechanisms and weak or no encryption used to communicate and store data. In the 2020 report, more detailed information about the IT security of medical devices and current attack scenarios are elucidated.

1.1.2 BfArM – Vigilance and Risk Notifications

The Federal Institute for Drugs and Medical Devices (BfArM) publishes information on risks posed by medical devices. Figure 1 shows the number of risk notifications per year from 2008 until 2017.

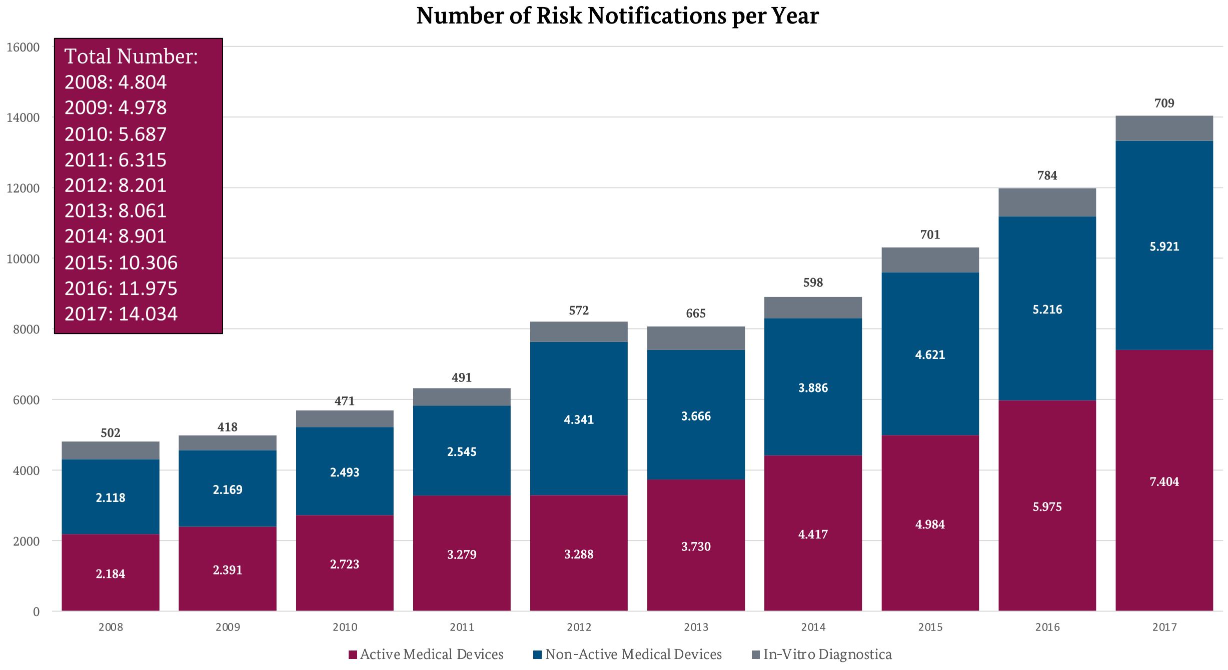


Figure 1: Number of Risk Notifications per Year taken from (BfArM, 2018)

As shown in Figure 1, the number of risk notifications has increased significantly from 2008 till 2017. However, the notifications predominantly inform about mechanical, electrical, and other types of errors or malfunctions (BfArM, 2017). IT security incidents have no dedicated category; hence, they are only included in the statistic if they exhibit potential safety impact.

The Federal Institute for Drugs and Medical Devices publishes a list of Field Safety Notices (FSN) related to IT security on a dedicated website (BfArM). Vendors send out such notices to information about safety risks in their products. At the time of writing, 21 such Field Safety Notices have been published on this web site. Compared to the number of risk notifications, this number is relatively small.

Hence, the current work should raise awareness that IT security-related issues should be considered when discussing potential risks posed by medical devices. Therefore, the current work tries to assess if IT security-related issues should be examined separately when discussing potential risks posed by medical devices.

1.2 Related Work

There have been several publications related to medical device IT security in the past. For example, the talk *Understanding and Exploiting Implanted Medical Devices* (Black Hat USA, 2018) reported critical vulnerabilities found in implanted medical devices (Rios & Butts, 2018).

The ERNW White Paper 66 summarizes the state of medical device security based on publicly available information (Suleder, Dewald, & Grunow). Furthermore, research performed by ERNW on patient monitors, syringe pumps, electroencephalography systems, home monitoring devices, and a Magnetic Resonance Imaging system demonstrated that the analyzed devices were affected by several vulnerabilities (SZ, 2015), (Grunow, 2015).

Moreover, a list of notifications about IT security issues is published by the Federal Institute for Drugs and Medical Devices in Germany (BfArM). Internationally, a list of Cybersecurity Safety Communications is published by the U.S. Food & Drug Administration (FDA, 2020). The Cybersecurity and Infrastructure Security Agency (CISA, USA) regularly publishes ICSMA (ICS Medical Advisories) to communicate vulnerabilities in medical devices.

Currently, no systematic study exists to evaluate the extent to which vulnerabilities occur in medical devices. Therefore, little data is available about the effectiveness of regulatory measures to prevent such vulnerabilities.

ManiMed is the first project that assesses the general IT security posture of connected medical devices. The IT security posture is evaluated based on IT security assessments performed to select connected medical devices. As a government-funded project, the results of ManiMed should serve as an information basis for the public and future regulatory specifications.

1.3 Audience

First, this document is intended for several audiences and to provide the public with the project results. To facilitate easy comprehension, the authors provided the basic terminology used throughout this document in Section 2. To provide a better understanding of the methodology used during the security assessments, Section 7 contains a dedicated description.

Second, the document is intended to provide information to operators/users of medical facilities (incl. medical personnel) to gain an overview of the IT security posture of connected medical devices on the German market. This should support operators in understanding which additional risks might be incurred by integrating connected medical devices into their infrastructure. It should be noted, though, that this does not mean that these connected devices, in general, increase the overall risk for a patient's safety. There are often several advantages compared to non-connected devices, such as a quicker response in the case of an emergency (when medical data of a patient is used to monitor for such events). Nevertheless, connected medical devices may introduce additional risks that the operators of medical facilities should be aware of.

Third, the document is intended to provide information to medical device vendors to a) make them aware of types of vulnerabilities that can occur in connected medical devices and b) to support them in reducing or eliminating vulnerabilities in their devices by showing technical and process-related measures against such flaws.

Fourth, the document is also intended for decision-makers for medical device regulations. This document's results should allow them to evaluate IT security in the context of regulations concerning medical devices in the future. It should be noted that the regulatory landscape in the European Union and therefore Germany will change significantly when the Medical Device Regulation (see Section 2.2) becomes obligatory. However, this work's results have been obtained within the current regulatory body for medical devices in Germany. Hence, these results cannot provide an indication of the IT security posture of medical devices that obtain access to the German market under the Medical Device Regulation.

1.4 Acknowledgments

The authors would like to use this paragraph to express gratitude to all vendors and associated parties that participated in this project. All participants showed a massive interest in an independent assessment and exclusive knowledge on their IT security posture as part of the project and with the intention to improve the security of their products.

By participating in this project, the vendors demonstrated that their products' security and safety is of great concern to them and that they strive to improve their products in a transparent way. Overall, the issues identified during the security assessments should be seen in this context: vendors that would like to make their products better, safer, and more secure.

Furthermore, the authors would also like to thank the medical facilities that took their time to answer our inquiry and provided information on their equipment. The information was valuable to identify devices that should be analyzed within this project.

The authors would like to thank all national and international authorities involved, specifically BfArM and CISA.

Finally, the authors would like to thank all other involved parties that have not been named explicitly here.

1.5 Project Partners

This section introduces the parties involved in performing the project: the ERNW Research GmbH, the ERNW Enno Rey Netzwerke GmbH, and the Federal Office for Information Security.

1.5.1 ERNW Research GmbH & ERNW Enno Rey Netzwerke GmbH

ERNW Research GmbH is an independent IT Security service provider based in Heidelberg, Germany. Since its founding in 2015, the focus of the ERNW Research GmbH has been on performing research projects in all areas of IT security - publicly funded projects in cooperation with universities, customer projects, and internal research projects.

ERNW Enno Rey Netzwerke GmbH is a vendor-independent consulting and security assessment service provider with a dedicated scope on network and application security. The company was founded in 2001. Many of the employees dispose of more than ten years of experience designing, implementing, operating, and securing extensive corporate networks.

The employees of both, the ERNW Research GmbH and the ERNW Enno Rey Netzwerke GmbH, regularly share their knowledge on international security conferences (e.g., regular speaker on Black Hat since 2006) and published a high number of books, professional articles, and white papers. In close cooperation with different universities, many theses about current information security topics are created every year.

The mission statement of both companies is to “Make the World a Safer Place!”. This bold, yet simple, message is the moral compass that guides the companies. This statement applies to the methodologies and research on how ERNW develops its staff, conveys its integrity to its customers, and the way it conducts itself within the local and global community. Particular fields of attention are the areas of Incident Response, Forensic Computing, Malware Analysis, and Medical Device Security, as well as advanced security assessments.

Contact:

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

1.5.2 The Federal Office for Information Security

The German Federal Office for Information Security (BSI) was founded in 1991 by law and is located in Bonn, Germany. The BSI is a non-profit organization under the authority of the Ministry of the Interior, Building and Community (BMI) and has eight departments, one central and seven specialized departments. Each department consists of one to three divisions, each of which in turn comprises a number of sections. In its role as the Federal Cyber Security Authority, the BSI shapes information security in digitization through prevention, detection and reaction for government, business and society. The overall goal is to promote IT security in Germany. Since its foundation the BSI continuously expanded in terms of resources and areas of competence.

The more dependent people become on information technology, the more relevant the issue of IT security becomes. The threat to our society in terms of the havoc that computer failure, misuse or sabotage could cause is greater than ever before. Due to the complexity of IT problems, the spectrum of tasks facing the BSI is extremely wide-ranging. In general, the BSI is first and foremost the central IT security service provider for the federal government in Germany. However, services to IT manufacturers as well as private and commercial users and providers of information technology are offered because effective security is only possible when all parties involved contribute. For this reason, the BSI wants to work in even closer co-operation with all those working in the IT and Internet industry in the field of IT security.

The BSI investigates security risks associated with IT, defines state of the art technology, publishes information on risks and threats (BSI, 2020) and seeks out appropriate solutions. All IT systems, even technically secure information and telecommunications systems potentially exhibit exploitable vulnerabilities at any given time. Consequently, any imaginable risk and damage have to be considered. In order to diminish or even avoid these risks, the BSI's services are intended for a variety of target groups: advising manufacturers, distributors and users of information technology and analyses current trends in the field of information technology.

Contact:

ManiMed Project Team
referat-di24@bsi.bund.de
Federal Office for Information Security

Cyber Security in the Public Health and Financial Services Sectors
Godesberger Allee 185-189
53175 Bonn
Germany
www.bsi.bund.de

1.6 About the Document

The following document is written by the BSI and security researchers based on experience gained from IT security-related projects, for example, penetration tests, concept reviews, audits of system environments, and development of security concepts. However, neither the ERNW Research GmbH nor the ERNW Enno Rey Netzwerke GmbH are manufacturers of digital health applications, medical devices, or auditors of a Notified Body or other certifiers, users or operators of medical devices or possess similar roles that could have a different view on the products. In addition to relevant expert knowledge for identifying security vulnerabilities in medical devices, systems, and extensive enterprise environments, as well as the ethical handling of vulnerabilities in coordinated disclosure processes, the authors have basic knowledge about the approval of medical devices and the corresponding legal requirements.

2 Terminology

In this section, the basic terminology used throughout this document is introduced. This includes, for example, common medical terms, as well as technical terms that are used to describe security issues. Moreover, the entities involved in publishing information on medical devices, approving medical devices for the German market, and responding to security issues in medical devices are discussed.

2.1 Medical Device

A medical device is defined in Article 2 (1) Medical Device Regulation (European Parliament and the Council of the European Union, 2017) as:

any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:

- *diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,*
- *diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,*
- *investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,*
- *providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations,*

and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.

The following products shall also be deemed to be medical devices:

- *devices for the control or support of conception;*
- *products specifically intended for the cleaning, disinfection or sterilisation of devices as referred to in Article 1(4) [of the Medical Device Regulation] and of those referred to in the first paragraph of this point.*

2.2 Regulations for Market Access of Medical Devices in Germany

Medical devices are approved for market access in Germany if they possess a CE marking. The CE marking provides a declaration by the vendor that the product complies with legal requirements. A so-called conformity assessment is performed to evaluate which legal requirements need to be considered.

Requirements are specified in Annex I of the Council Directive 90/385/EEC for active implantable medical devices (European Parliament and the Council of the European Union, 1990), Council Directive 98/79/EC for *in vitro* diagnostic medical devices (European Parliament and the Council of the European Union, 1998), and Council Directive 93/42/EEC for other medical devices (European Parliament and the Council of the European Union, 1993).

How the conformity assessment is to be performed depends on the potential risk associated with a medical device. Based on the risk assessment specified in the corresponding directive, the devices are categorized into product classes (except for active implantable devices, which are not further categorized based on risk criteria). These product classes determine the conformity assessment process and govern if a so-called *Notified Body* is required to be involved within this process.

The Council Directive 93/42/EEC for other medical devices specifies four categories in its Annex IX: I, IIa, IIb, and III.

It is noted that the directives mentioned above need to be translated to national law. For Germany, this is implemented via the Act on Medical Devices (Bundesgesetzblatt, 1994).

The presented Council Directives will be replaced by the Medical Device Regulation (see Section 2.3).

2.3 Medical Device Regulation (MDR)

The Medical Device Regulation (MDR) governs the main formalities concerning medical devices within the European Union (European Parliament and the Council of the European Union, 2017). It came into effect on May 25, 2017 and becomes obligatory on May 26, 2021 (the date has been postponed by one year due to the COVID-19 pandemic). Among other things, the MDR replaces the Medical Device Directive (MDD; Directive 93/42/EEC).

2.4 Federal Institute for Drugs and Medical Devices (BfArM)

The Federal Institute for Drugs and Medical Devices (German: Bundesinstitut für Arzneimittel und Medizinprodukte – BfArM) is the regulatory authority for drugs and medical devices in Germany. It is under the authority of the Federal Ministry of Health (German: Bundesministerium für Gesundheit – BMG). The main tasks of the BfArM in the field of medical devices are (BfArM):

- Central registration, evaluation, and assessment of occurring risks regarding the use of medical devices and coordination of measures to be taken
- Special approval of medical devices
- Counselling of responsible agencies, Notified Bodies, and vendors regarding questions concerning the classification of medical devices and their boundary to other devices as well as the decision thereof
- Counselling of responsible agencies and Notified Bodies regarding technical and medical requirements and regarding questions concerning the safety of medical devices
- Collaboration in nation-state/federal-state committees, working groups of the European Commission as well as national, European, and international standardization committees
- Execution of consultation procedure for medical devices with pharmaceutical parts on request of Notified Bodies
- Evaluation and assessment of clinical trials of medical devices and performance evaluation tests of *in-vitro* diagnostics

2.5 German Institute for Medical Documentation and Information (DIMDI)

The German Institute for Medical Documentation and Information (DIMDI) was a government agency within Germany. The area of responsibility has been assigned to BfArM on May 26, 2020.

One of its primary tasks is the operation of the database for medical devices mandated by the Act on Medical Devices. With its query functionality, the information system was used as part of the market analysis (see Section 3.1.1 to identify medical devices that fulfill the requirements mentioned in Section 3. Further information on the system can be found on the website of the Federal Institute for Drugs and Medical Devices (BfArM).

2.6 European Databank on Medical Devices (EUDAMED)

The European Databank on Medical Devices (EUDAMED) should allow authorities to quickly access relevant data about medical device vendors and the devices to improve the monitoring of the European market of medical devices.

The MDR states that vendors or corresponding distributors of medical devices have to register in EUDAMED and provide information about themselves prior to the distribution of medical devices on the European market. Moreover, before any medical device can get approval for the European market, the vendor must provide certain information about the device and enter it into the database.

It should be noted that at the time of writing, the development of the database and its interfaces is still ongoing.

2.7 Operation Modes for Medical Devices

The Federal Office for Information Security published a best practice guide for manufactures of network-connected medical devices (BSI, 2018).

The document has been published with the following intentions. First, it should serve as an accompanying guideline for the implementation of regulatory requirements. Second, it should support the development and maintenance of medical devices with a focus on security. Third, it should help how to reduce security issues from the risk analysis performed as part of the conformity assessment.

The document differentiates between several modes of operation that are supported by most devices. The following modes are introduced:

- Medical Operation Mode – The device is used for its intended medical use.
- Device Configuration Mode – The device is being configured for its medical purpose (including patient-specific parameters).
- Technical Maintenance Mode – Installation of updates from the manufacturer or third-party providers as well as basic calibration or adjustments of the device.

As stated in the document, the different modes may affect one another. For example, if malware is installed during the technical maintenance mode, this can also affect the medical operation mode. Nevertheless, the distinction between these different modes is essential to evaluate the patient risk associated with a specific vulnerability. If a vulnerability can only occur during the technical maintenance mode, an attacker would first need to identify a mechanism to set the device into this mode.

2.8 Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (CVSS) is a framework to rate the criticality of individual vulnerabilities. It was developed by the Forum of Incident Response and Security Teams (FIRST, 2019).

2.8.1 Basics of CVSS

CVSS defines a metric for calculating three different scores, each of them with their distinct statement. The scores are called *Base Metrics*, *Temporal Metrics,* and *Environmental Metrics*. The Base Metrics determine the general severity of the vulnerability and, once it is assigned, do not change anymore. The Temporal Metrics characterizes how complex it is for an attacker to exploit the vulnerability and may change over time. This can change, for example, if exploit code for a vulnerability is made publicly available. Finally, the Environmental Metrics considers the impact of the vulnerability in a specific environment and, hence, may change for different environments. Overall, the three metrics are combined to obtain a CVSS score. This CVSS score reflects the severity of a vulnerability at a specific point of time in a particular environment.

Further information on the CVSS score calculation can be found in the publicly available documents (FIRST, 2019).

It is noted that the CVSS scoring system has been developed to rate the severity of vulnerabilities for enterprise information technology systems. Hence, it does not adequately reflect the severity of medical devices' vulnerabilities as the patient safety impact of a vulnerability is not well incorporated into the scoring system. That is why the MITRE Corporation has made efforts under contract to the Food and Drug Administration of the United States to adapt the CVSS scoring system for medical devices (Chase & Coley, 2019). This adaptation does not modify the calculation of the CVSS score but introduces a questionnaire, based on which individual parameters of the metrics should be determined. However, it should be noted that this document is classified as an early draft at the time of writing.

2.8.2 Use of CVSS

Within the project, the CVSS scoring system (version 3) together, with the presented extension, was used to rate all identified vulnerabilities. These were then communicated to each corresponding vendor during the disclosure process. However, the CVSS scoring system is not included in this document for the following reasons:

- As the disclosure process is still ongoing at the time of writing, several security advisories containing CVSS scores have not been published yet. It has to be considered that the vulnerabilities are discussed during this disclosure process with vendors, and additional information may be provided that potentially affects the rating of the CVSS score. Consequently, if a CVSS rating would be included in this document, it might differ from the final one provided along with the security advisory. As this document should not contain conflicting information regarding these security advisories, no CVSS scores will be provided here.
- The CVSS scoring system uses a *quantitative* approach to determine the severity of a vulnerability. Values are assigned to the parameters of the different CVSS metrics to obtain an overall CVSS score. This allows a simple comparison of the severity of various vulnerabilities but is typically more challenging to understand than a *qualitative* approach where descriptive terms are used to define the vulnerability's severity.

2.9 Security vs. Safety

The German language uses the same word “Sicherheit” as a translation for the English terms “security” and “safety”. Security and safety have different meanings that cannot be appropriately described only with the single word “Sicherheit” (such that other words have to be used to describe the exact context). Therefore, we will explain the terms security and safety as they are used within this document and highlight their differences.

The term security denotes the protection of an entity against external threats. Hence, if some vulnerability exists (e.g., a medical device within the context of this document), this reduces the device's security since it is not protected accurately against threats enabled by the vulnerability. It should be noted here that, except for very simple systems, it is impossible to prove that a device is secure, i.e., no method or algorithm exists to determine if an entity is accurately protected against all external threats.

Nevertheless, sometimes the statement can be made that a device is secure or that it shows a high level of security. This does not mean that the device is secure in general but that the time and effort spent to analyze an entity for vulnerabilities via a certain assessment methodology did not result in any meaningful findings. Hence, if more time is spent to analyze any system for vulnerabilities, it becomes more likely that they are found. Therefore, it is important to recognize how much time was spent on this assessment to judge the results of a security assessment.

Often the abbreviation IT (Information Technology) or the term cyber will be prepended to the term security, i.e., IT-security or cyber security, to denote only the security of an entity affected by IT-related threats (such as an attack on the communication protocols of an electronic device).

The term safety denotes the protection of a system against internal and external threats that negatively affect a patient’s wellbeing. First, it should be noted that, in contrast to the term security, the term safety also includes internal threats. For example, a malfunction of a medical device (not caused by external influence) can harm a patient's wellbeing if it affects a critical part of the device. Therefore, such internal threats must be included.

Second, the definition only includes those threats that affect the wellbeing of the entity. Hence, regarding external threats, safety-related issues form a sub-category of security-related issues. That is, a security-related issue may have a safety impact. For example, suppose a medical device is rendered unusable when an external attacker exploits a vulnerability. The medical device performs a function that is critical to the wellbeing of the patient. In that case, this security issue has an impact on safety. However, if an external attack can only use the vulnerability to read configuration data of the device, which does not have an impact on the wellbeing of the patient, then the issue only has a security impact, but no safety impact.

As part of the Coordinated Vulnerability Disclosure process (see Section 2.11), where a vulnerability is reported to a vendor, an important step is to clarify if a security issue has safety impact. This usually requires additional information to allow for an appropriate rating of the reported issue. Hence, vendors need to provide a statement, clarifying if the reported issue is a valid finding and if it has safety impact.

2.10 Confidentiality, Integrity, and Availability

Information security standards, such as the ISO/IEC 27001 (ISO/IEC, 2013) often use a special set of categories to classify a vulnerability's impact better. This set usually includes the categories of confidentiality, integrity, and availability. This document will also use these categories as defined by the ISO/IEC standards when describing the risk of the identified vulnerabilities.

The ISO/IEC standards (ISO/IEC, 2018) define confidentiality as the “property that information is not made available or disclosed to unauthorized individuals, entities, or processes”. For example, suppose a vulnerability allows an attacker to get unauthorized access to data on a system. In this case, the vulnerability affects the confidentiality of the data of this system.

The ISO/IEC standards define the term integrity as “property of accuracy and completeness”. In other words, this means that unauthorized individuals cannot tamper with information. This includes both information that is stored (at rest) and information that is in transit. For example, if a device has an update mechanism where a firmware image can be provided, an attacker may modify the firmware image and deploy his own. If the firmware image is not protected by additional measures such as a cryptographic signature and a corresponding signature check, the device cannot ensure the firmware's integrity as the firmware image may be tampered with.

Finally, the ISO/IEC standards define availability as “property of being accessible and usable on demand by an authorized entity”. For a medical device, availabilitycplays an important role. If the device is not available or usable anymore, for example, due to an attack, this may have a direct safety impact.

2.11 Coordinated Vulnerability Disclosure

A Coordinated Vulnerability Disclosure (CVD) is defined as “the process of gathering information from vulnerability finders, coordinating the sharing of that information between relevant stakeholders, and disclosing the existence of software vulnerabilities and their mitigations to various stakeholders, including the public“ (Carnegie Mellon University, 2017).

Even in a supposedly secure system, nobody can ever wholly rule out vulnerabilities. Therefore, the professional handling of vulnerabilities is an integral part of the manufacturer's product lifecycle activities. In most enterprises, when external parties report vulnerabilities, Coordinated Vulnerability Disclosures are carried out.

In the IT security industry, disclosure periods of up to 90 days are established from notification to the vulnerabilities' publication. A manufacturer can only successfully (means repeatable and reliable) carry out a CVD if a well-defined response process is established. These processes must be established in a comprehensible and transparent manner before vulnerabilities are reported so that they can be remedied promptly.

Multiple entities such as vulnerability finders, vulnerability reporters, vendors, deployers, and coordinators are involved in a CVD process. CVD means a high level of communication among all those involved. The process should be designed in a trustful mutual exchange and continuous cooperation. All entities agree on keeping vulnerability information confidential until the disclosure process ends.

A coordinated vulnerability disclosure can be divided into different phases. First, a finder discovers one or more vulnerabilities in a product. Afterward, the finder submits a vulnerability report to the product vendor or a third-party coordinator. In the third phase, a vendor first performs a validation and then a triage of the vulnerabilities. Afterward, a remediation plan or timeline for a software patch or mitigating controls is developed. After that, the vulnerability and its remediation plan are disclosed to the public.

It is a cross-industry best practice that the vulnerability reporters pose a disclosure date of 90 days from notifying the vendor to disclosing vulnerability information. Necessary extensions may be granted at the discretion of the reporters when the vendor can justify the expansion. (Carnegie Mellon University, 2017) In the US, the FDA recommends a 60-day disclosure in case of vulnerabilities that can affect patient safety (FDA, 2016). The mode of the vulnerability disclosure is at the finder’s discretion. Often blog posts or white papers are published to inform the public about their discoveries. These blog posts typically contain in-depth technical explanations for identifying the vulnerabilities. Further, the proposed fixes and measures taken by the vendor are presented. Besides, it is another industry best practice to assign so-called Common Vulnerabilities and Exposures (CVE) for fixed vulnerabilities. These CVEs contain information about the identified vulnerability and affected product in a straightforward and structured manner. A unique ID number is assigned to each CVE, and all CVEs are listed in the MITRE database.

2.12 ManiMed Disclosure Framework

In contrast to other disclosure processes, as described above, ManiMed only assessed medical products. This might pose a risk to patients if a disclosure process is not thoroughly planned and executed. Therefore, a responsible approach was always adhered to, keeping technical details and points of time for publishing information in mind at all times. A security and a safety risk assessment were requested, as the manufacturer is obliged to assess his own products for both – security and safety. For vulnerabilities that could affect the physical health of a patient, consulting BfArM was a major part of the process.

In the following, all standard steps taken during each CVD process are explained. Every manufacturer was treated equally, to prevent market distortion.

After the security assessment of the particular medical device, the project team reached out to the manufacturer's point of contact. This contact was predefined, as the manufacturer, in most cases, provided the devices and/or a testing lab.

As a first step, the manufacturer was informed about all findings. For this purpose, each manufacturer was provided with a complete and detailed security assessment report for their device or system. All reports were written in English to ease communication within most manufacturers' multi-national structures. To enable fast and effective remediation, each report included:

- a detailed explanation of all assessed systems
- descriptions of all vulnerabilities
- full proof-of-concept code
- developed exploits
- exemplary videos that were taken of, e.g., crashes.

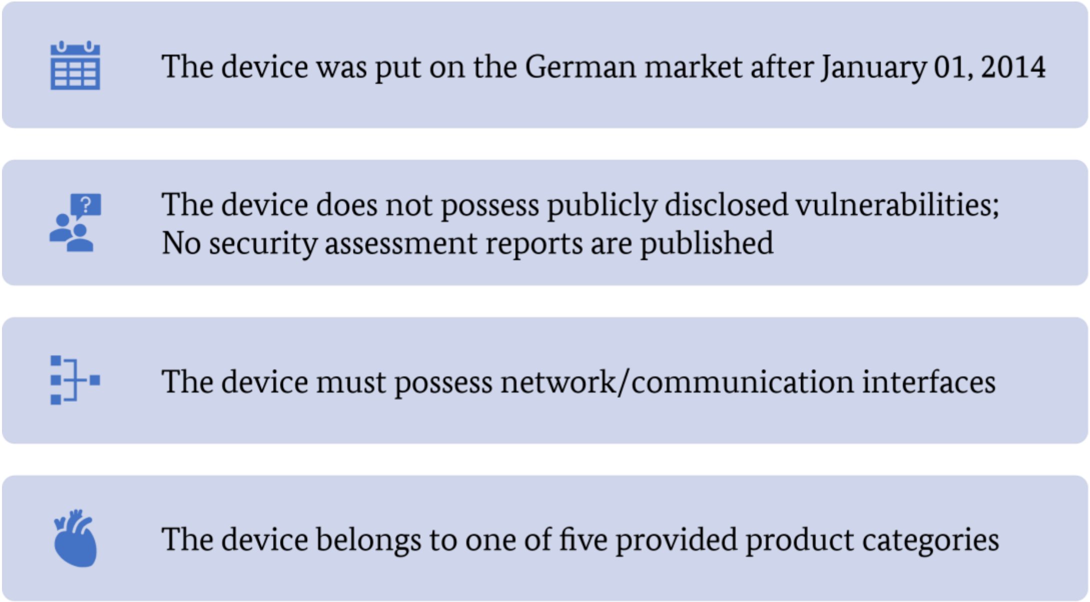
In a second step, each report and its findings were presented and discussed with the responsible teams. Mitigations and patch timelines were appointed, and a disclosure date fixed.

The third step encompassed to establish contact with the Cybersecurity and Infrastructure Security Agency (CISA), a United States agency with the role to improve cybersecurity. Together, CVEs and security advisories were assigned to fixed/remediated vulnerabilities and published to increase transparency. A publication of vulnerabilities demonstrates that a manufacturer is aware of potential defects and possible enhancements for their devices and continuously improves them. In contrast to CVEs, security advisories enable manufacturers to state their risk analysis and mitigations, as well as fixes implemented. Further, CVEs allow a public referencing of security vulnerabilities in reports, discussions, and security recommendations. Most manufacturers appreciated the publication of the vulnerabilities because it adds another driving force to promote and deploy patches in the field. Prior to publication, every publication, advisory and CVE description was consolidated with the respective manufacturer.

Manufacturers were free to release advisories prior to this document. Each manufacturer decided whether they want to be named with their product’s name or prefer to remain anonymous in this document. A final letter from the BSI addressing the manufacturer marked the end of the disclosure. It allowed manufacturers to advertise their participation in project ManiMed without promoting their examined products as "tested by BSI" or "with BSI certification". After the CVD process, the vulnerabilities can be publicly discussed at IT security conferences. Published vulnerabilities can be used for publications related to the ManiMed project. With respect to best IT-security practices, CVEs and security advisories are publicly available to increase transparency and awareness. The list of advisories and CVEs linked to project ManiMed can be reviewed in Section 8.1.

3 Market Analysis

This chapter provides the market analysis for medical devices examined in an IT security assessment within the scope of the project ManiMed. To select appropriate devices for such assessments, the following requirements have been established:



The device was put on the German market after January 01, 2014

The device does not possess publicly disclosed vulnerabilities; No security assessment reports are published

The device must possess network/communication interfaces

The device belongs to one of five provided product categories

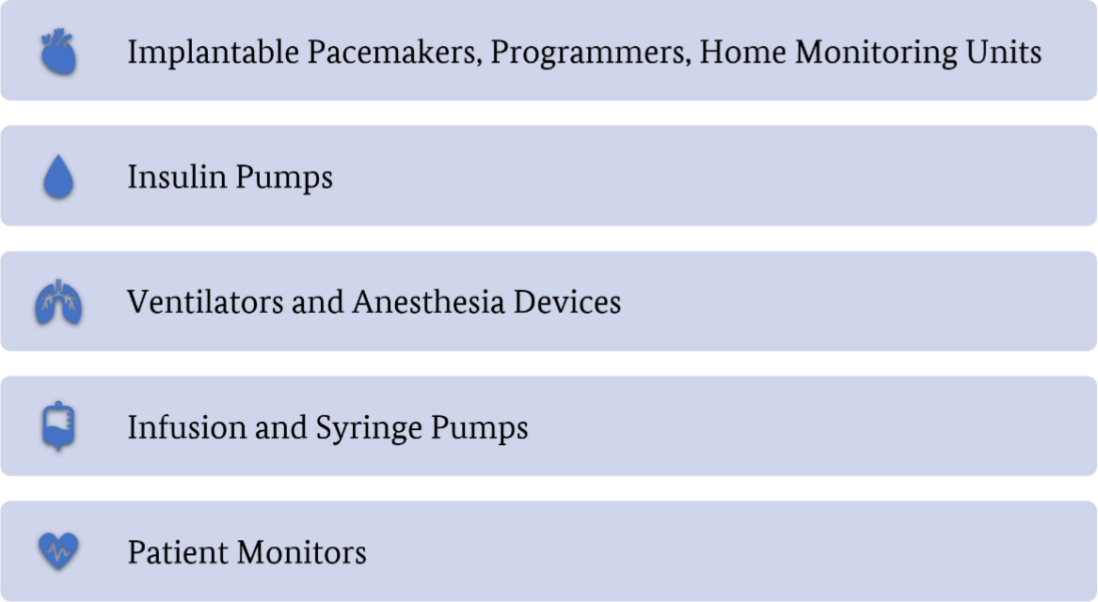
Figure 2: Requirements for medical devices within the market analysis

These four constraints/requirements have to be met for devices subjected to IT security assessments apart from the fact that the selected device categories are dependent on high security postures due to their impact on patient safety.

However, these selection criteria may also introduce certain biases to the results of the security assessment for the following reasons:

- The date, January 1, 2014, is deemed reasonable to include only devices with novel communication interfaces that might be affected by vulnerabilities. Devices placed on the German market before this date might also possess such interfaces, but these devices are excluded from the analysis.
- Excluding devices on which vulnerabilities were already disclosed in the past or which were part of a published security assessment might also incur a bias for this assessment. Primarily because these devices might yield additional security vulnerabilities apart from what was already published, therefore reducing possible findings within this project. However, these devices might still have additional security vulnerabilities apart from the already published ones or the ones discovered via the security assessment. On the other hand, if no security vulnerabilities have been published so far, this could mean that either the vendor himself is performing intensive security assessments before the market release or that nobody has analyzed the device yet. The market analysis does not consider these points.

The following categories (listed in Figure 3) were chosen prior to the start of this project:



Implantable Pacemakers, Programmers, Home Monitoring Units

Insulin Pumps

Ventilators and Anesthesia Devices

Infusion and Syringe Pumps

Patient Monitors

Figure 3: Medical device categories for market analysis

All selected categories correspond to devices that might have a critical impact on patient safety in case of security issues.

To search for devices that fulfill the requirements listed in Figure 2 and belong to one of the categories listed in Figure 3, several sources were utilized that are presented in Section 3.1. For each device category, the results of this search are illustrated as flow charts in Section 3.2. Further information on the selection criteria used in the different iterations of the search is provided there. Detailed information about the devices assessed and the results of the assessments are given in Section 4.

3.1 Sources

The following sources were used to perform the market analysis:

- Medical Devices Notifications Database
- Inquiry to Medical Facilities
- Public Information from Medical Device Vendors
- Internet Research
- Questionnaire to Vendors

The different sources are further described below.

3.1.1 Medical Devices Notifications Database

The DIMDI operates an information system on medical devices used, for example, for notifying competent authorities according to § 33 of the Act on Medical Devices (Bundesgesetzblatt, 1994). The public part of this information system contains the Medical Devices Notifications (MPA) database. At the time of this investigation (June 04, 2019), the database comprised 105,730 medical devices since the beginning of data acquisition in 2002. This count constantly changes, as the database receives daily updates.

Requests to the database are sent via the DIMDI SmartSearch interface. This interface allows defining individual fields of the database and combining search queries. Certain fields feature a fixed range of possible values, which can be queried via an index. Furthermore, searches with wildcards for free text fields are possible. The results of a query can be exported via a watchlist in XML format. The MPA database can be accessed using the Medical Device Information System box provided by the BfArM (BfArM).

Not all medical devices approved for the German market are included within the database. It stands to reason that an incomplete synchronization causes this discrepancy with other medical device databases in the European Union. For example, if the first placing of a medical device occurred in another state of the EU, it is likely to be registered with the corresponding national database only. Furthermore, some manufacturers do not register complete devices in these databases but file different components and modules separately. This makes it very difficult for others to reconstruct all necessary parts of a device. Therefore, additional sources to identify medical devices approved for the German market were used as described below.

3.1.2 Inquiry to Medical Facilities

To estimate which medical devices facilities in Germany use, inquiries were sent to selected facilities with an appeal to provide information on their inventory of medical devices. The template for the letters can be found in Section 8.2.

3.1.3 Public Information of Medical Device Vendors

As a third source, information that has been published by the medical device vendors was used to identify additional medical devices. Online search engines, the MPA data, and the inquiry to the medical facilities were utilized to identify vendors for medical devices within the different categories. Afterward, the vendor’s device portfolio was analyzed for suitable devices. Specifications for the devices were used to investigate if the device features any networking functionality or other promising interfaces.

3.1.4 Internet Research

Apart from the information published by medical device vendors, lists of exhibitors of relevant medical informatics and medical product fairs were used to maximize the number of vendors for the market analysis. This search was predominantly conducted online. It includes the Digital Medical Expertise & Applications (DMEA) and the MEDICA. Both fairs are internationally recognized and the largest in their respective branches, which has the advantage that exhibitors on these fairs represent a significant percentage of the global medical device market.

Moreover, recent technical advances in the medical field were incorporated via an investigation of scientific publications and case studies as well as practical evaluations of national and international pilot projects. For example, PubMed (NCBI) was used as one of the sources for this investigation. PubMed is an English, text-based Meta database containing medical and scientific articles. The database is developed and operated by the National Center for Biotechnology Information (NCBI) within the National Library of Medicine (NLM) by the National Institute of Health (NIH) of the USA.

A further source is the German National Library (German: Deutsche Nationalbibliothek, DNB), which is the central archive library for all media work published in German (DNB).

No further devices could be identified via this method, i.e. all devices were already identified via other sources.

3.1.5 Questionnaire to Vendors

In individual cases, where only limited information was available, a questionnaire was sent to the medical device vendors to gain further information. The content of the questionnaire is provided in Section 8.3.

3.2 Results

The following sections contain the results of the market analysis for each device category. The selection of the devices for each category is based on the source presented in the previous chapter. The overall selection process follows the steps laid out in Figure 4.

The figure shows the basic selection of medical devices containing all devices that have been identified via the Internet research, the DIMDI database research, and the responses to the inquiries sent to health delivery organizations. Afterward, the devices were evaluated for their communication interfaces and devices were sorted out that do not possess relevant communication interfaces. For the remaining devices, it was evaluated if vulnerabilities or reports about security assessments have already been published. If not, these devices were included in the preselection. In a final step, if there were more than five devices left, vendors were queried for more details on the devices. The details were used to generate a prioritized list of devices for the assessment. It is noted that selected devices are further described from a technical perspective in Section 4.

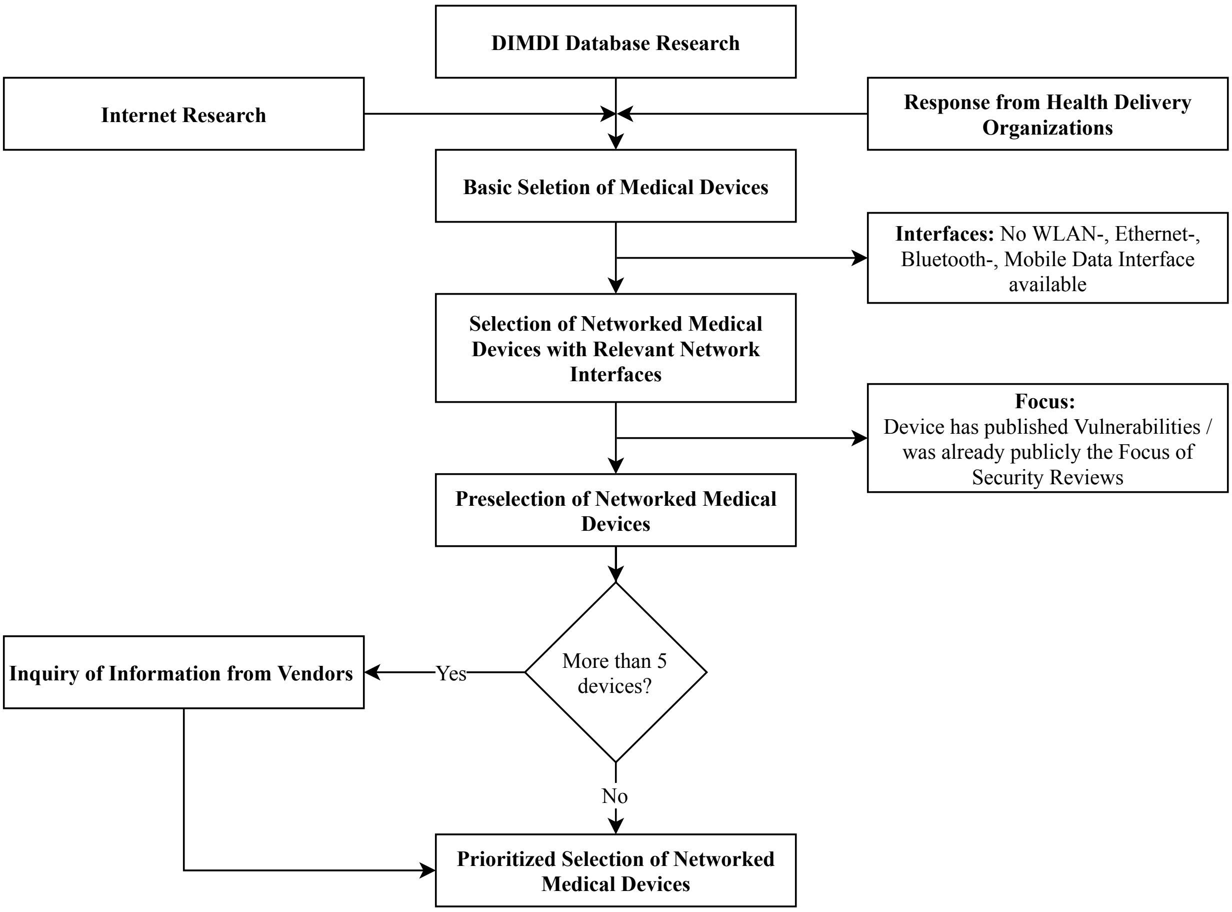

DIMDI Database Research
Internet Research
Response from Health Delivery Organizations
Basic Seletion of Medical Devices
Interfaces: No WLAN-, Ethernet-, Bluetooth-, Mobile Data Interface available
Selection of Networked Medical Devices with Relevant Network Interfaces
Focus: Device has published Vulnerabilities / was already publicly the Focus of Security Reviews
Preselection of Networked Medical Devices
More than 5 devices?
Yes
Inquiry of Information from Vendors
No
Prioritized Selection of Networked Medical Devices

Figure 4: The overall selection process performed during the market analysis.

3.2.1 Implantable Pacemakers, Programmers, Home Monitoring Units

For the market analysis of medical devices, the Medical Device Notifications (MPA) database described in Section 3.1.1 was used as a basis. Here, the exemplary analysis focuses on pacemakers approved in Germany that were granted access to the market in the past five years. Figure 5 shows the selection process for pacemakers along with the associated selection criteria in a flow chart. The criteria *modification date, type of report*, and *category* are strict exclusion criteria of this database search.

As shown in Figure 5, the search with the MPA database resulted in 19 potential devices. However, after a manual review of these devices, it was asserted that the devices did not contain any interfaces worth investigating in an IT security assessment. Moreover, in this category, every single part of the pacemaker system is listed separately. The final implanted product is more like a construction system to enable flexibility, compatibility between multiple products of the same product family, and ease certification.

Moreover, the inquiries sent to medical facilities yielded no further device information.

Finally, the 2016 annual report of the German Pacemaker and Defibrillator Registry (IQTIG, 2016) was consulted as it contains a list quantifying the number of implanted pacemakers per vendor in 2014, 2015, and 2016. Such a list was not included in the 2017 report, so the 2017 report could not be used to obtain this data.

3.2.1.1 Results

Based on the information in the report (in particular the market distribution of vendors), the following pacemaker infrastructures were selected for the assessment:

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

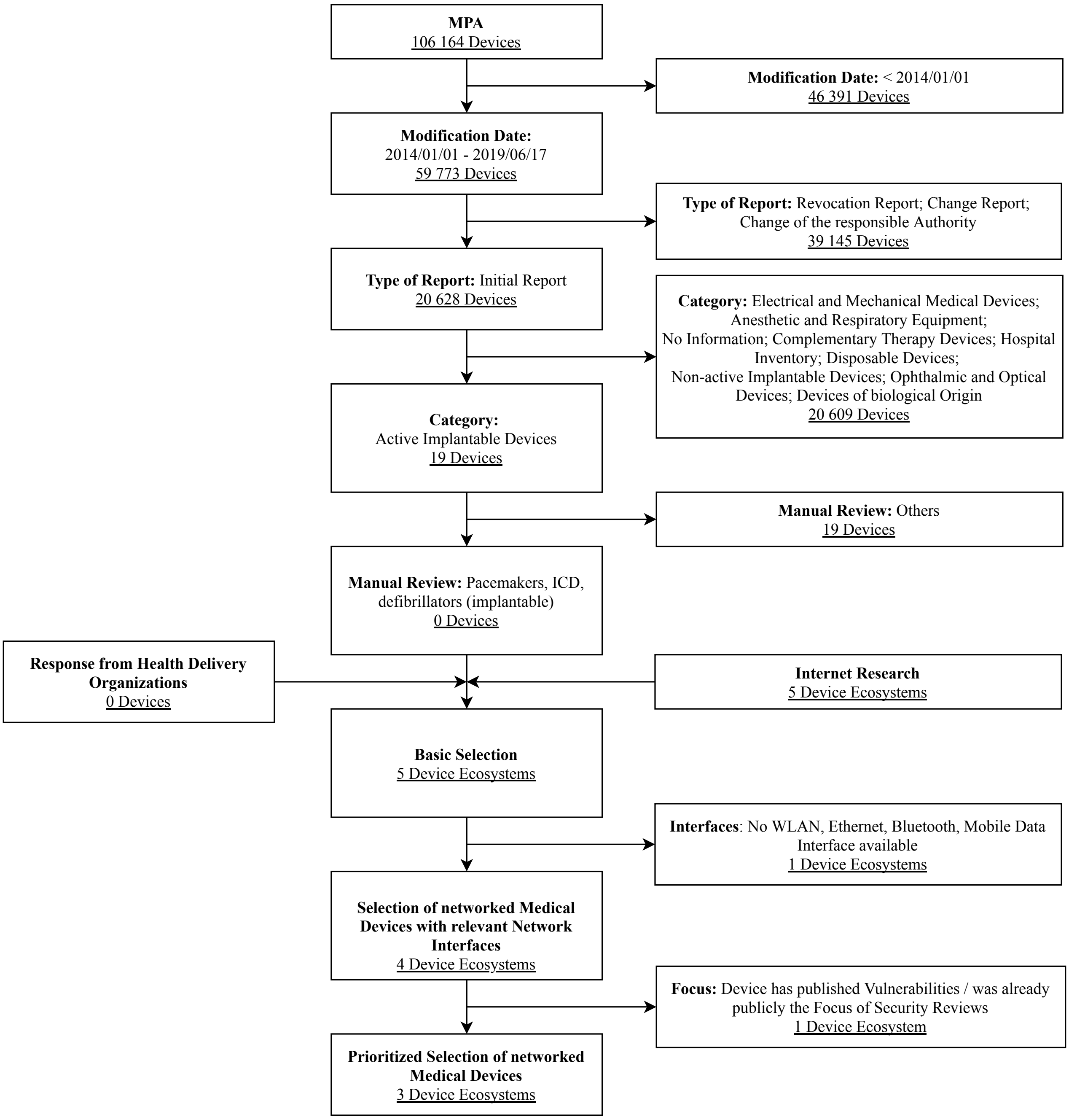

MPA
106 164 Devices
Modification Date: < 2014/01/01
46 391 Devices
Modification Date:
2014/01/01 - 2019/06/17
59 773 Devices
Type of Report: Revocation Report; Change Report; Change of the responsible Authority
39 145 Devices
Type of Report: Initial Report
20 628 Devices
Category: Electrical and Mechanical Medical Devices; Anesthetic and Respiratory Equipment; No Information; Complementary Therapy Devices; Hospital Inventory; Disposable Devices; Non-active Implantable Devices; Ophthalmic and Optical Devices; Devices of biological Origin
20 609 Devices
Category:
Active Implantable Devices
19 Devices
Manual Review: Others
19 Devices
Manual Review: Pacemakers, ICD, defibrillators (implantable)
0 Devices
Response from Health Delivery Organizations
0 Devices
Internet Research
5 Device Ecosystems
Basic Selection
5 Device Ecosystems
Interfaces: No WLAN, Ethernet, Bluetooth, Mobile Data Interface available
1 Device Ecosystems
Selection of networked Medical Devices with relevant Network Interfaces
4 Device Ecosystems
Focus: Device has published Vulnerabilities / was already publicly the Focus of Security Reviews
1 Device Ecosystem
Prioritized Selection of networked Medical Devices
3 Device Ecosystems

Figure 5: Flow chart illustrating the MPA search process for implantable pacemakers.

3.2.2 Insulin Pumps

The research focuses on outpatient insulin pumps licensed in Germany. Clinical insulin infusion pumps are not considered in this category. Figure 6 shows the selection process used for insulin pumps along with associated selection criteria in a flow chart. The criteria *modification date*, *type of report*, *category,* and *nomenclature term* were strict exclusion criteria for this database search. These results were expanded after a manual review by the Internet research results and feedback on health delivery organizations' devices. They were also filtered by the exclusion criteria *interfaces* and *focus* to obtain a prioritized list of the devices.

As shown in Figure 6, eight devices fulfilling the requirements were identified after applying the exclusion criteria to the database search. Moreover, the inquiries sent to medical facilities resulted in no further devices.

For the Internet research, patient portals, Internet forums, and information websites were systematically searched for device lists and device reviews. Four insulin pumps were identified, which gained approval for the German market after January 1, 2014, and are not listed in the DIMDI MPA database.

In sum, twelve devices could be identified after all three sources were evaluated. These devices were further examined for their attack surface, i.e., if these devices have any communication interfaces implemented. This yielded six devices. Furthermore, devices for which vulnerabilities were published had to be excluded such that a total number of four devices remained.

3.2.2.1 Results

To select the devices to be further analyzed within an IT security assessment, priority was assigned to pumps where a mobile app can control the pump in comparison where it can only read historical data. Overall, the following insulin pump systems were selected for the IT security assessment:

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

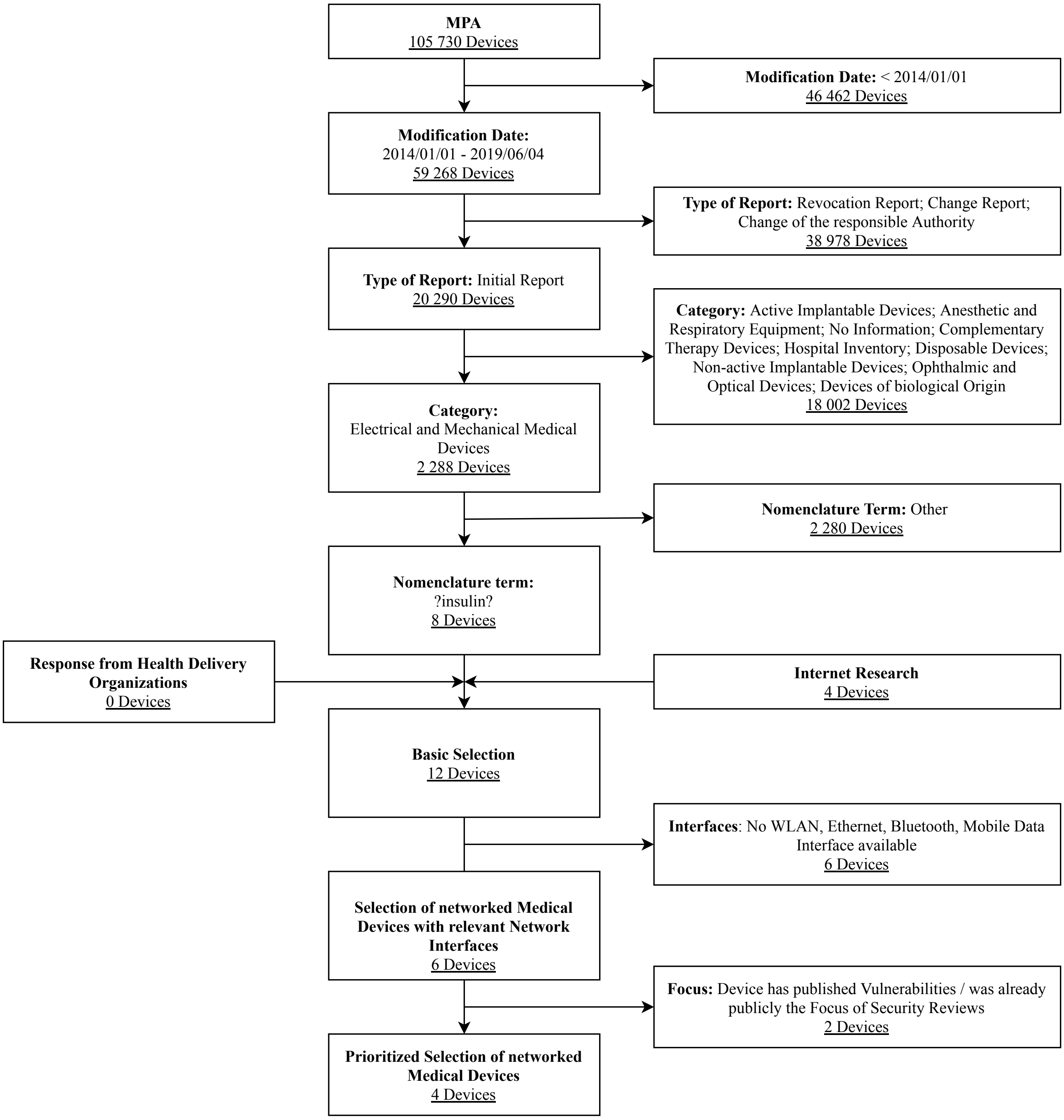

MPA
105 730 Devices
Modification Date: < 2014/01/01
46 462 Devices
Modification Date:
2014/01/01 - 2019/06/04
59 268 Devices
Type of Report: Revocation Report; Change Report; Change of the responsible Authority
38 978 Devices
Type of Report: Initial Report
20 290 Devices
Category: Active Implantable Devices; Anesthetic and Respiratory Equipment; No Information; Complementary Therapy Devices; Hospital Inventory; Disposable Devices; Non-active Implantable Devices; Ophthalmic and Optical Devices; Devices of biological Origin
18 002 Devices
Category:
Electrical and Mechanical Medical Devices
2 288 Devices
Nomenclature Term: Other
2 280 Devices
Nomenclature term:
?insulin?
8 Devices
Response from Health Delivery Organizations
0 Devices
Internet Research
4 Devices
Basic Selection
12 Devices
Interfaces: No WLAN, Ethernet, Bluetooth, Mobile Data Interface available
6 Devices
Selection of networked Medical Devices with relevant Network Interfaces
6 Devices
Focus: Device has published Vulnerabilities / was already publicly the Focus of Security Reviews
2 Devices
Prioritized Selection of networked Medical Devices
4 Devices

Figure 6: Flow chart illustrating the selection process for insulin pumps.

3.2.3 Ventilators

The analysis focuses on ventilators and anesthesia devices approved for Germany. Humidifiers, heaters, and distributors of gases remain out of consideration. Figure 7 shows the selection process used for ventilators along with associated selection criteria in a flow chart. The criteria *modification date*, *type of report*, *type of product*, *category,* and *medical device class* were strict exclusion criteria for the database search. These results were expanded after a manual review by the Internet research results and the feedback on devices by health delivery organizations. Two exclusion criteria further filtered them: *interfaces* and *focus.* After obtaining further information utilizing questionnaires sent to vendors, a prioritized list of these devices was created.

As shown in Figure 7, after applying the exclusion criteria to the database search, 56 devices fulfilling the requirements were identified.

Moreover, three clinical ventilators were reported in response to the inquiry sent to clinical facilities, of which two were eligible regarding their appearance on the German market. However, both devices were already identified by searching the MPA database.

For the Internet research, ventilators were searched on websites of, for example, medical technology fairs such as MEDICA (MEDICA, 2019) for devices not yet included in the result set. In the process, 20 devices were identified, which were possible candidates but not listed in the MPA database. It should be mentioned that devices were also included if no specific date of approval for the German market could be identified.

Therefore, 78 devices were identified after making use of all three sources. These devices were further examined for their attack surface, i.e., if these devices have any communication interfaces implemented. This resulted in a total number of 31 devices. Furthermore, none of the devices had publicly known vulnerabilities and, hence, none of the devices were excluded.

3.2.3.1 Results

To select devices for the IT security assessment, the degree of device networking functionalities advertised by the vendor, and the health delivery organizations' feedback were considered. Overall, the Hamilton Medical AG HAMILTON-T1 ventilator was selected for the IT security assessment.

It was planned to assess two ventilators during the ManiMed project. As a response to the situation and circumstances coming along with the Covid-19 pandemic, the second ventilator was not tested within the project timeframe.

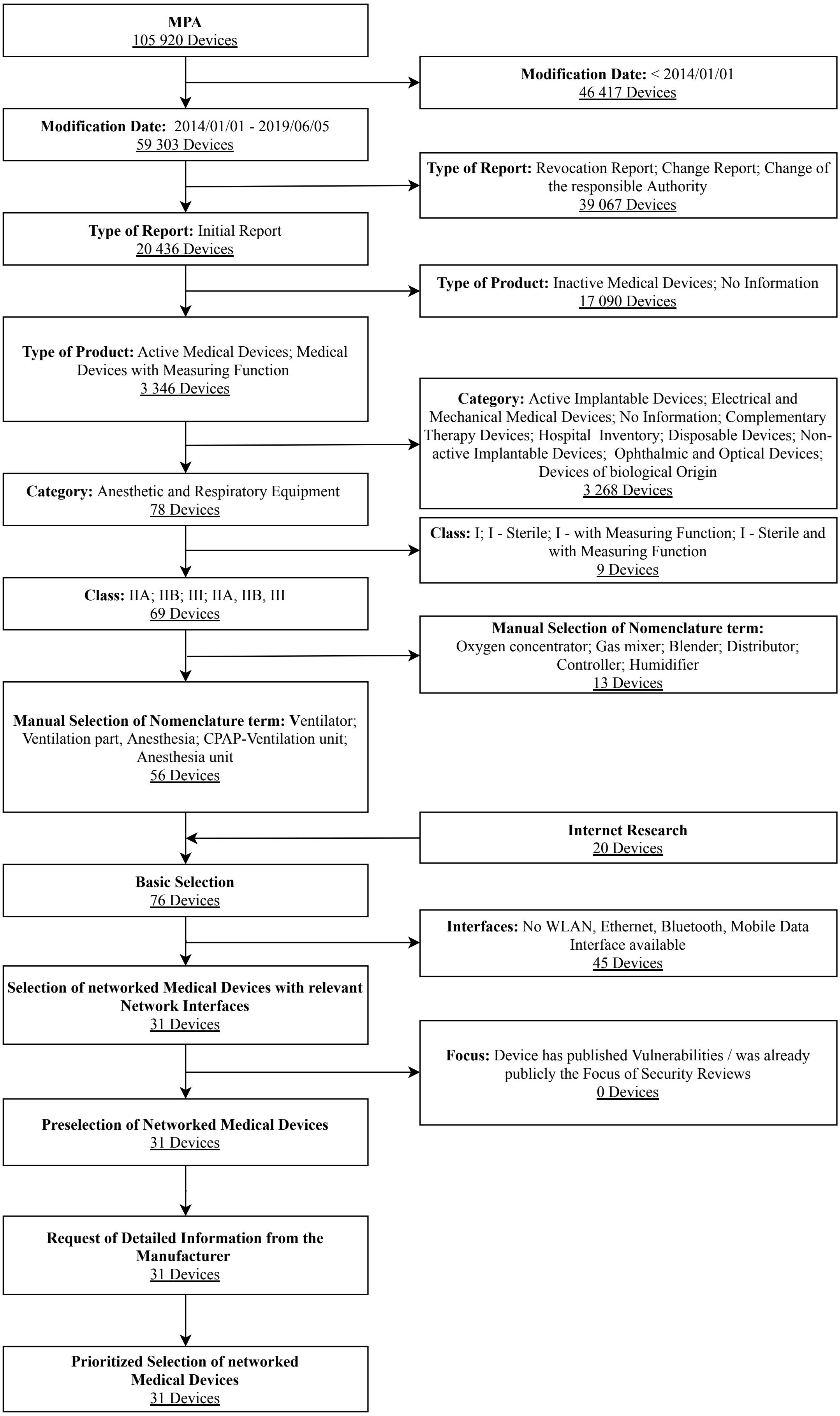

MPA
105 920 Devices
Modification Date: < 2014/01/01
46 417 Devices
Modification Date: 2014/01/01 - 2019/06/05
59 303 Devices
Type of Report: Revocation Report; Change Report; Change of the responsible Authority
39 067 Devices
Type of Report: Initial Report
20 436 Devices
Type of Product: Inactive Medical Devices; No Information
17 090 Devices
Type of Product: Active Medical Devices; Medical Devices with Measuring Function
3 346 Devices
Category: Active Implantable Devices; Electrical and Mechanical Medical Devices; No Information; Complementary Therapy Devices; Hospital Inventory; Disposable Devices; Non-active Implantable Devices; Ophthalmic and Optical Devices; Devices of biological Origin
3 268 Devices
Category: Anesthetic and Respiratory Equipment
78 Devices
Class: I; I - Sterile; I - with Measuring Function; I - Sterile and with Measuring Function
9 Devices
Class: IIA; IIB; III; IIA, IIB, III
69 Devices
Manual Selection of Nomenclature term: Oxygen concentrator; Gas mixer; Blender; Distributor; Controller; Humidifier
13 Devices
Manual Selection of Nomenclature term: Ventilator; Ventilation part, Anesthesia; CPAP-Ventilation unit; Anesthesia unit
56 Devices
Internet Research
20 Devices
Basic Selection
76 Devices
Interfaces: No WLAN, Ethernet, Bluetooth, Mobile Data Interface available
45 Devices
Selection of networked Medical Devices with relevant Network Interfaces
31 Devices
Focus: Device has published Vulnerabilities / was already publicly the Focus of Security Reviews
0 Devices
Preselection of Networked Medical Devices
31 Devices
Request of Detailed Information from the Manufacturer
31 Devices
Prioritized Selection of networked Medical Devices
31 Devices

Figure 7: Flow chart illustrating the selection process for ventilators.

3.2.4 Infusion and Syringe Pumps

The research focuses on syringe and infusion pumps. Figure 8 shows the selection process used for syringe and infusion pumps along with associated selection criteria in a flow chart. The criteria *modification date*, *type of notification* and, *UMDNS code* were strict exclusion criteria for this database search. These results were expanded after a manual review by the Internet research results and feedback on health delivery organizations' devices. They are also filtered by the exclusion criteria *interfaces* and *focus.* After obtaining further information utilizing questionnaires sent to vendors, a prioritized list of devices in the result set was generated.

As shown in Figure 8, no device listed in the database fulfilled all requirements, and the selected table was returned empty.

The questionnaires sent to medical facilities resulted in seven devices of clinical infusion and syringe pumps. Additionally, different websites, e.g., medical technology trade fairs such as MEDICA (MEDICA, 2019), were evaluated for viable infusion and syringe pumps during the Internet research. Furthermore, at the beginning of the search, feedback from health delivery organizations was already available, so that the devices reported therein could be utilized as a starting point. 34 devices were identified that are not listed in the MPA database of DIMDI. It should be noted that devices are also included for which no specific date of approval for the German market could be identified. Furthermore, most infusion systems were put on the market before 2014 and are regularly expanded by new pumps. Therefore, the market access criterion was not used as a strict exclusion criterion; otherwise, no devices would be available for subsequent security analysis.

Infusion and syringe pumps are rarely used alone in a clinical context, as multiple drugs and infusions are often administered in parallel with different pumps. For this reason, they have no additional networking interfaces except for infrared and serial interfaces. Instead, they are aggregated into docking stations, which then provide a shared networking interface for all pumps. For this reason, networked infusion and syringe pumps in this project were analyzed in combination with their device series, as they usually have a networked docking station. For the device series to remain in the result set, they needed at least one network interface, e.g. WLAN, Ethernet, RFID / NFC or Bluetooth for connection to a Patient Data Management Systems (PDMS). To filter these interfaces, technical device datasheets, flyers, and manuals were used. Overall, this resulted in seven device ecosystems. Two of these ecosystems already had published vulnerabilities leaving five of them as eligible candidates for this assessment.

3.2.4.1 Results

To select the devices for further analysis within an IT security assessment, priority was given to infusion and syringe pumps based on feedback from health delivery organizations and existing interfaces. Network interfaces such as Ethernet and WLAN were prioritized first, followed by USB and serial interfaces. To choose between devices with similar interfaces, the number of devices purchased by participating health delivery organizations was considered.

As stated in chapter 3.2.3.1 the second ventilator was not tested. Instead, a third infusion system was selected for the IT security assessment:

- **B. Braun Melsungen AG:** Space System
- **Anonymous:** Infusion System #1
  Anonymous: Infusion System #2

Moreover, a pump management system for syringe and infusion pumps was tested:

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

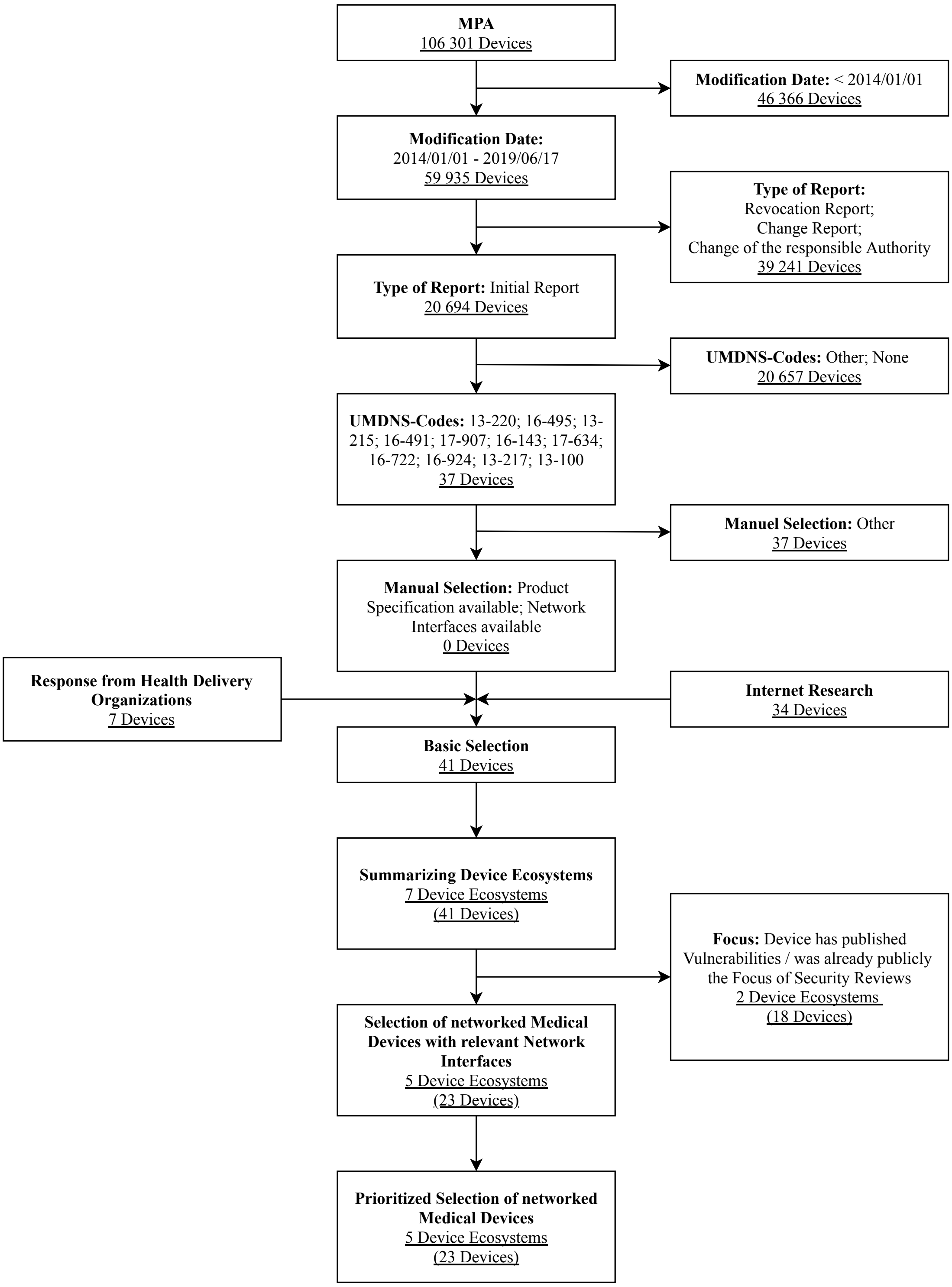

MPA
106 301 Devices
Modification Date: < 2014/01/01
46 366 Devices
Modification Date:
2014/01/01 - 2019/06/17
59 935 Devices
Type of Report:
Revocation Report;
Change Report;
Change of the responsible Authority
39 241 Devices
Type of Report: Initial Report
20 694 Devices
UMDNS-Codes: Other; None
20 657 Devices
UMDNS-Codes: 13-220; 16-495; 13-215; 16-491; 17-907; 16-143; 17-634; 16-722; 16-924; 13-217; 13-100
37 Devices
Manuel Selection: Other
37 Devices
Manual Selection: Product Specification available; Network Interfaces available
0 Devices
Response from Health Delivery Organizations
7 Devices
Internet Research
34 Devices
Basic Selection
41 Devices
Summarizing Device Ecosystems
7 Device Ecosystems
(41 Devices)
Focus: Device has published Vulnerabilities / was already publicly the Focus of Security Reviews
2 Device Ecosystems
(18 Devices)
Selection of networked Medical Devices with relevant Network Interfaces
5 Device Ecosystems
(23 Devices)
Prioritized Selection of networked Medical Devices
5 Device Ecosystems
(23 Devices)

Figure 8: Flow chart illustrating the selection process, for infusion and syringe pumps.

3.2.5 Patient Monitors

The research focuses on patient monitors approved in Germany. Here, ECG and EEG devices are out of consideration. The diagram in Figure 9 shows the selection process used for the patient monitors along with associated selection criteria in a flow chart. The criteria *modification date*, *type of notification*, and *UMDNS code* were strict exclusion criteria for this database search. These results were expanded after a manual review by the Internet research results and feedback on health delivery organizations' devices. They are also filtered by the exclusion criteria *interfaces* and *focus.* After obtaining further information utilizing questionnaires sent to vendors, a prioritized list of devices in the result set was created.

As shown in Figure 9, after every exclusion criterion was applied and the devices were manually reviewed for their attack surface, eight devices were left. Moreover, at the time of writing, five clinical patient monitor devices were reported by health deliver organizations, but four were launched before 2014 and, therefore, not eligible for testing. As a result, only one additional device was obtained from the response from health delivery organizations.

For the Internet research, patient monitors were searched on medical technology fairs' websites, such as MEDICA, for devices not yet included in the result set. 18 devices could be identified that were approved for the German market after January 1, 2014 and were not listed in the MPA database of DIMDI.

Overall, the three sources resulted in 27 feasible devices. However, four devices had already published vulnerabilities, and eight devices possessed no relevant network interfaces such that the search resulted in a total number of 15 devices.

3.2.5.1 Results

A prioritizing factor was the date of market access, so newer devices were preferred over older ones. Also, devices with a central management software were favored over devices without such a solution. Furthermore, extended network functionality such as centralized user management via, e.g., LDAP or standardized communication interfaces such as HL7 standards or ADT, had a higher priority. Specialized devices for use in limited applications, such as devices that can be used within magnetic resonance tomography, were given less priority because they usually exhibit fewer interfaces due to the environmental conditions.

Overall, the following patient monitors were selected for the IT security assessment:

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

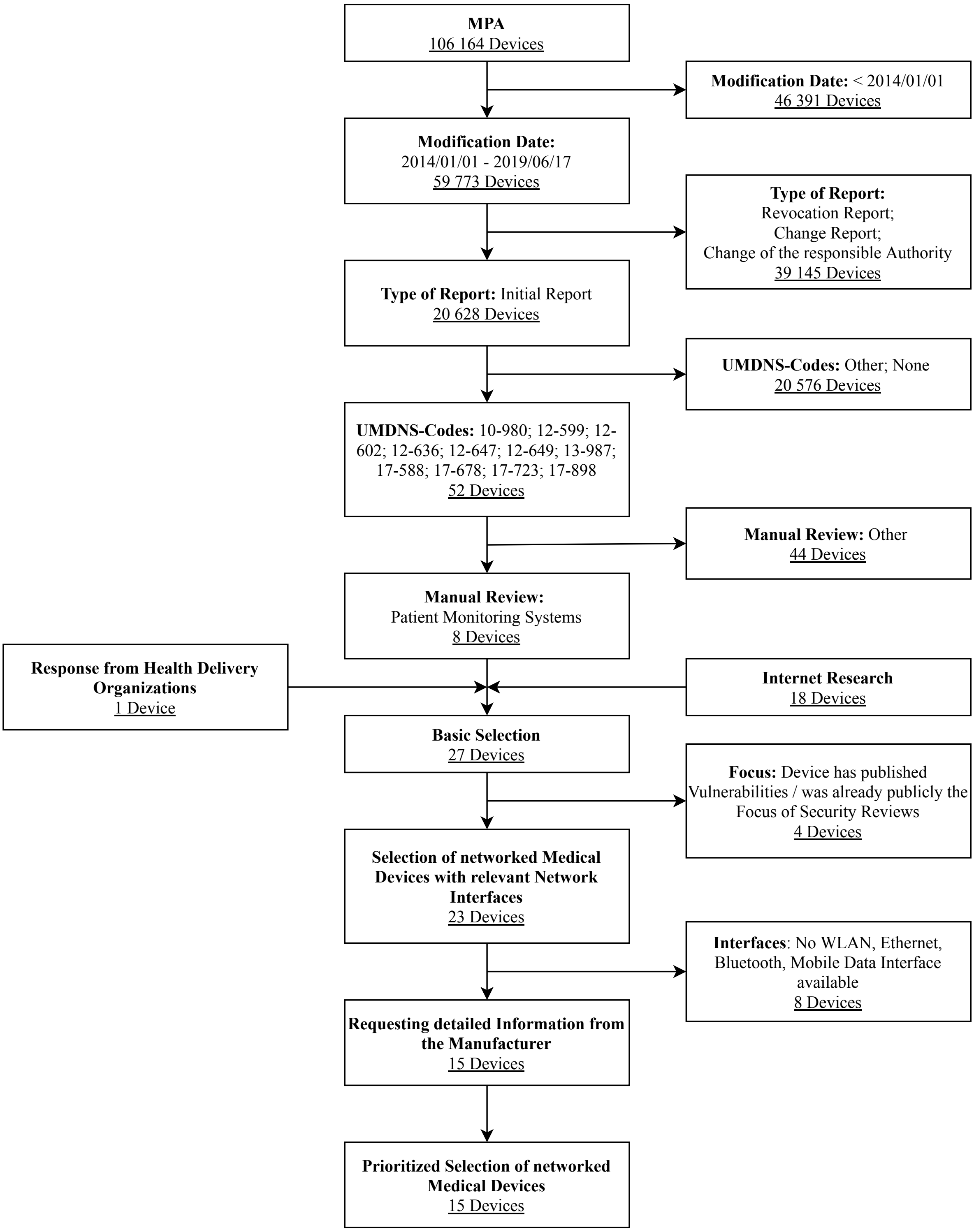

MPA
106 164 Devices
Modification Date: < 2014/01/01
46 391 Devices
Modification Date:
2014/01/01 - 2019/06/17
59 773 Devices
Type of Report:
Revocation Report;
Change Report;
Change of the responsible Authority
39 145 Devices
Type of Report: Initial Report
20 628 Devices
UMDNS-Codes: Other; None
20 576 Devices
UMDNS-Codes: 10-980; 12-599; 12-602; 12-636; 12-647; 12-649; 13-987; 17-588; 17-678; 17-723; 17-898
52 Devices
Manual Review: Other
44 Devices
Manual Review:
Patient Monitoring Systems
8 Devices
Response from Health Delivery Organizations
1 Device
Internet Research
18 Devices
Basic Selection
27 Devices
Focus: Device has published Vulnerabilities / was already publicly the Focus of Security Reviews
4 Devices
Selection of networked Medical Devices with relevant Network Interfaces
23 Devices
Interfaces: No WLAN, Ethernet, Bluetooth, Mobile Data Interface available
8 Devices
Requesting detailed Information from the Manufacturer
15 Devices
Prioritized Selection of networked Medical Devices
15 Devices

Figure 9: Flow chart illustrating the selection process for patient monitors.

4 IT Security Assessment Results

In this section, the scope of the security assessments and their results will be presented ordered by category and not ordered by the point of time the assessment took place. After a short characterization of the medical device's environment and intended medical use, the vulnerabilities identified are elucidated. A black-box approach was used. To make this part available to a broader audience (see Section 1.3), the results will be presented without in-depth technical details. It is important to mention that most of the vulnerabilities disclosed did not affect patient safety and were no longer existent in the devices when this report was published. The remaining vulnerabilities are to be fixed within the next months and mostly due to the project plan and the recently performed assessment.

A more technical explanation of the respective vulnerabilities is available in the respective ICSMAs (ICS Medical Advisories), Common Vulnerabilities and Exposures (CVE) entries and published white papers or blog posts as well as talks which are listed in Section 8.1. The assessment methodology and scoping are explained in Section 6.3. For each assessment, an effort of about 20 person days was invested. Experiences regarding the disclosure process are described in Section 5.

As medical devices are highly regulated products and only operated by trained personnel, it has to be mentioned that the devices assessed in this project can generally not be purchased by any consumer. Consequently, in project ManiMed devices could either be provided by the manufacturer with a testing contract or purchased from project money. The manufacturers provided the majority of devices. The amount of additional information (test accounts, firmware updates, device equipment, documentation, source code, etc.) differed among all participants.

4.1 Assessed Products

The following table lists the devices that have been assessed in this project. Each manufacturer decided whether to be named or to remain anonymous.

Section	Vendor	Product
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	*Anonymized Manufacturer*	*Anonymized Infusion System #1*
4.6.4	*Anonymized Manufacturer*	*Anonymized Infusion System #2*
4.6.5	COPRA System GmbH	Copus (Copra Pump Management System)

Table 2: Assessed Products

4.2 Implantable Pacemakers and Implantable Cardioverter Defibrillators (ICDs)

In this section, the security assessments of two pacemakers and their medical systems are elucidated after a short description of the devices' characteristics and the environment in which they are operated.

4.2.1 Characteristics & Environment

A standard pacemaker continuously stimulates the heart muscle, causing cardiac contraction when the heart's intrinsic rhythm is slow or absent. In contrast, an Implantable Cardioverter Defibrillator (ICD), similar to external defibrillators, monitors the intrinsic heart rhythm and delivers an electric shock to restore a normal heartbeat. In the following, referring to the term pacemaker, we will consider both devices. Pacemakers are classified in the highest medical device risk class III (European Parliament and the Council of the European Union, 2017) being active, implantable medical devices, and having special functional requirements. Due to the exceptional safety requirements, strict validation and verification steps are present throughout the development process.

Pacemakers are implanted in patients' bodies and do not have user interfaces or similar connectivity intended to be used by patients. In periodic pacemaker checkups, telemetry and monitoring protocols are used by specialists to configure and parameterize the pacemakers with so-called programmers. As the implanted pacemakers cannot be explanted and read-out via wired connections, this communication occurs in low-range radio frequency protocols during these routine checkups. The respective frequencies are at around 30 kHz for inductive near-field communication in the MICS band between 402-405 MHz worldwide reserved for communication with implantable medical devices. Sometimes communication is performed via Bluetooth Low Energy (BLE). Devices that are more recent support transferring telemetry data as well as ECG measurements via so-called home monitoring units to a specialist via the internet.

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

This section is about the security assessment of the pacemaker Rivacor 7 VR-T DX, a prototype of the Renamic Neo programming unit, and the Cardio Messenger Smart relay unit, which forwards medical data from the pacemaker to a cloud backend by the German manufacturer Biotronik SE & Co. KG (hereafter referred to as Biotronik).

4.2.2.1 Scope

The following devices were tested: Two Rivacor 7 VR-T DX pacemakers, a Renamic Neo programming unit, and the Cardio Messenger Smart relay unit. As part of the assessment, the exposed interfaces of the different devices, as well as their communication, were analyzed. As the devices exposed several different types of interfaces, the interfaces had to be examined using different tools. The cloud backend was out of scope.

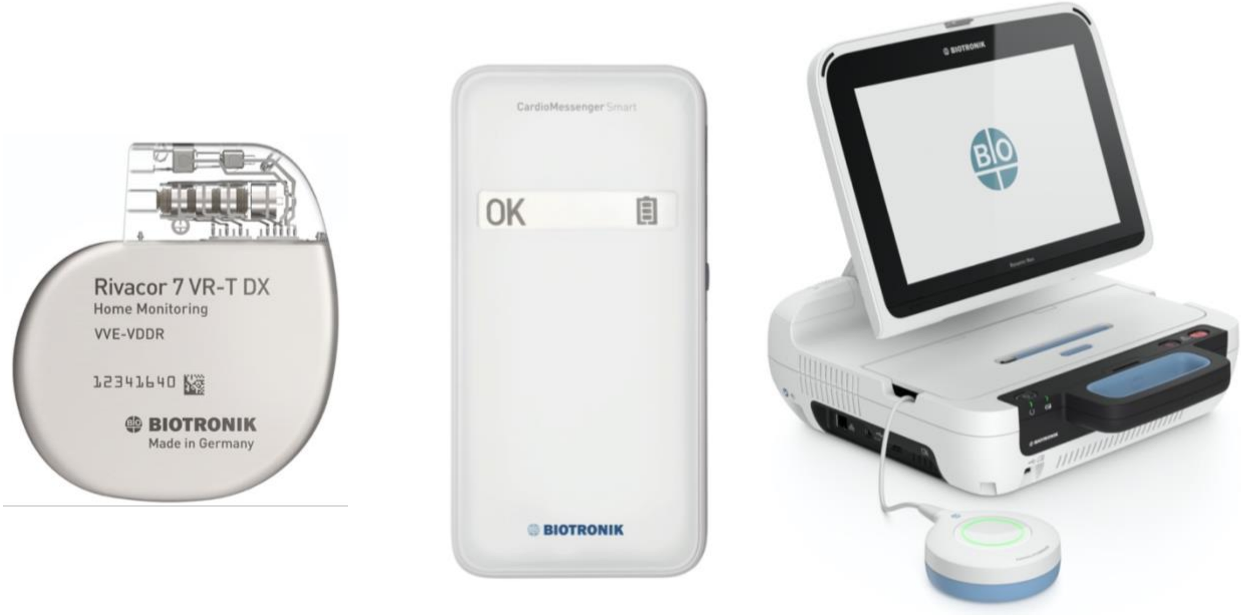


Figure 10: A Biotronik Rivacor 7 VR-T DX pacemaker (left), Cardio Messenger Smart (middle) and a Renamic Neo programming unit (right). (Source: Biotronik)

4.2.2.2 Results

During the assessment of the programming unit, a few crashes of its user interface have been identified. It should be remarked that it was not possible to break out of the graphical interface's confinement to the underlying operating system during the assessment. Hence, no control over the operating system of the programming unit has been achieved in this way.

Apart from the identified crashes, the assessment revealed no further issues for the programming unit. It should be noted that the target of the evaluation was a product prototype. Crashes are likely associated with the prototype state of the software.

During the assessment of the relay unit, no vulnerabilities could be identified. It should be noted that the relay unit exposes only a small attack surface. This attack surface comprises three parts, a USB port for power supply from the relay unit, a modem for mobile communication with the cloud backend, and a chip for radio-communication with the pacemaker. The relay unit‘s SIM card’s PIN was obtained by analyzing the communication between the relay unit and the SIM.

By using a Faraday cage and Base Transceiver Station (BTS), it was possible to connect the relay unit to a GSM network infrastructure controlled by the auditors. By using this setup, it was possible to send SMS directly to the device, but the sent messages did not lead to any exploitable behavior.

The assessment focused on the communication of the pacemaker with the programming unit and the relay unit. The assessment revealed that the pacemaker transferred heart monitor data via a radio frequency protocol to the Cardio Messenger Smart and the Renamic Neo. A low-frequent signal is required to configure the pacemaker with the programming head. With a Software Defined Radio (SDR), it is possible to capture arbitrary signals and demodulate those using Digital Signal Processing (DSP) techniques. For this setup, a USRP with special LFRX/LFTX daughterboards was used together with a ferrite loop stick antenna to capture the low-frequency signals.

4.2.2.3 Impact

Due to reverse engineering complexity, a non-standardized radio protocol without further information, it was not possible to re-implement the radio protocol or re-play radio communication during the assessment. Overall, no vulnerabilities of medium or high impact were identified. The manufacturer fixed all issues resulting in system crashes within a short time range and identified no patient harm.

4.2.3 Medtronic plc - CareLink SmartSync Device Manager System

This section is about the security assessment of two Medtronic Azure pacemakers and the CareLink SmartSync Device Manager system by the American Irish manufacturer Medtronic plc (hereafter referred to as Medtronic). The system enables physicians to program and monitor Bluetooth-enabled implanted cardiac devices with an iPad app.

4.2.3.1 Scope

The inspected systems were the Medtronic CareLink SmartSync Device Manager system including two Azure pacemakers, the CareLink SmartSync Device Manager patient connector and base as well as the respective iPad and mobile app. As part of the assessment, the exposed interfaces of the different devices as well as their communication were analyzed. As the devices exposed several different types of interfaces, the interfaces had to be examined using different tools. The cloud backend was out of scope. The manufacturer provided manuals, firmware updates as well as source code for the iPad app, patient connector and base in addition to the lab setup.

4.2.3.2 Results

During the assessment of the medical device ecosystem three buffer overflows in the patient connector, as well as one integer overflow could be identified. The buffer overflows could lead to errors like segmentation faults when the program is trying to jump to memory addresses that do not contain valid instructions or memory regions that are not permitted to be accessed. Overwriting control flow data could also be exploited to take control of the application.

The likelihood of successful exploitation highly depends on the exploit mitigation features. However, the existence of exploit mitigation features could not be verified during the assessment. A review of the application’s code revealed that vulnerable component performs a calculation based on user input to determine how much memory to allocate for a buffer. For large values, an integer overflow can occur.

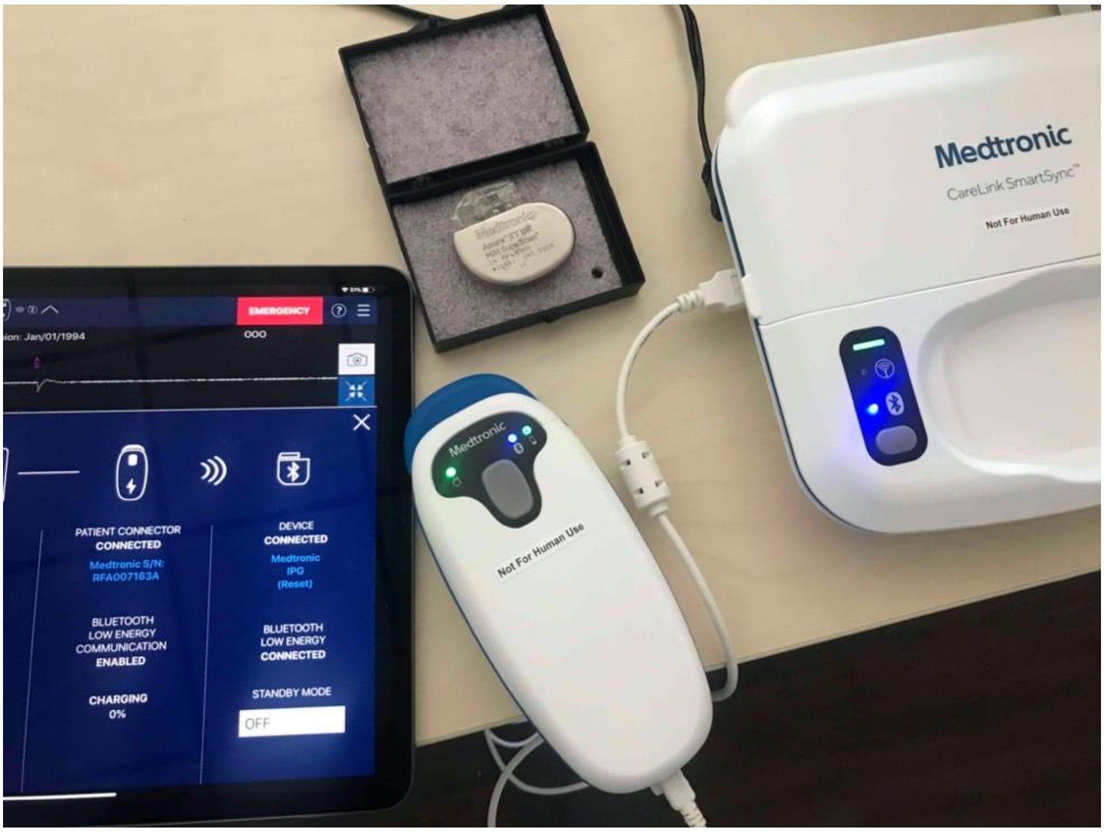


Figure 11: The testing lab of the Medtronic CareLink SmartSync Device Manager system comprising of the base unit (right), a handheld (bottom center) and an iPad with the app (left) as well as a pacemaker (top center). (Source: BSI)

4.2.3.3 Impact

The findings were identified through a code review. An assessment whether the vulnerabilities can be exploited has not been performed. According to the manufacturer, existing security mechanisms hinder attackers from exploiting the identified vulnerabilities. The vendor identified no patient harm and provided an update for the system thereby fixing all reported vulnerabilities.

4.3 Insulin Pumps

In this section, the security assessments of two insulin pumps and their medical system are outlined after a short description of the devices' characteristics.

4.3.1 Characteristics & Environment

An insulin pump is an active medical device used for insulin administration in the treatment of diabetes mellitus (type 1 diabetes). Diabetes mellitus is an autoimmune disease and is based on the lack of insulin due to the destruction of insulin-producing beta cells in the Langerhans islets of the pancreas. An insulin pump is a less invasive alternative to multiple daily injections of insulin and allows for flexible insulin therapy. The Continuous Subcutaneous Insulin Infusion (CSII) therapy with insulin pumps aims to enable automated and on-demand delivery of insulin via thin tubing subcutaneously without the need for injections. According to the German Diabetes Association (DDG) publication German health report -

Diabetes 2020 (DDG, 2019), an estimated 32,000 children and adolescents and 340,000 adults with type 1 diabetes live in Germany. It is estimated that about 45,000 people in Germany use an insulin pump, but no reliable sources for this number exist.

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

This section describes the security assessment of the DANA Diabecare RS insulin pump system by the Korean manufacturer SOOIL Development Co., Ltd. (hereafter referred to as SOOIL).

The DANA Diabecare RS insulin pump is the central component of this therapy system and can be controlled with an application for the mobile operating systems Android and iOS via a Bluetooth Low Energy (BLE) interface. The device is not intended to be used for closed-loop systems.

4.3.2.1 Scope

The inspected components were the communication protocol of the SOOIL DANA Diabecare RS insulin pump with its AnyDANA mobile apps via Bluetooth Low Energy (BLE). The testing method was a black box penetration test without source code insight. Two insulin pumps were available for testing, which were provided by the manufacturer as well as publicly available documentation.

4.3.2.2 Results

During the assessment, different issues were identified, which could affect the security of this device. First, the device's manual recommends using weak device keypad lock PINs to easily disable the device lock. Moreover, all pumps have a default PIN. The PIN chosen by users is disclosed without authentication via the Bluetooth Low Energy (BLE) interface, too. An attacker with physical access to the pump and in possession of the PIN is able to unlock a locked pump, change the pump configuration, and administer an insulin bolus. Further, the physician PIN for gaining access to the pump's physician menu is the same for all pumps and cannot be changed without contacting the support. An attacker with access to this PIN and physical access to a pump is able to change the pump's configuration such as the maximum daily insulin dose.

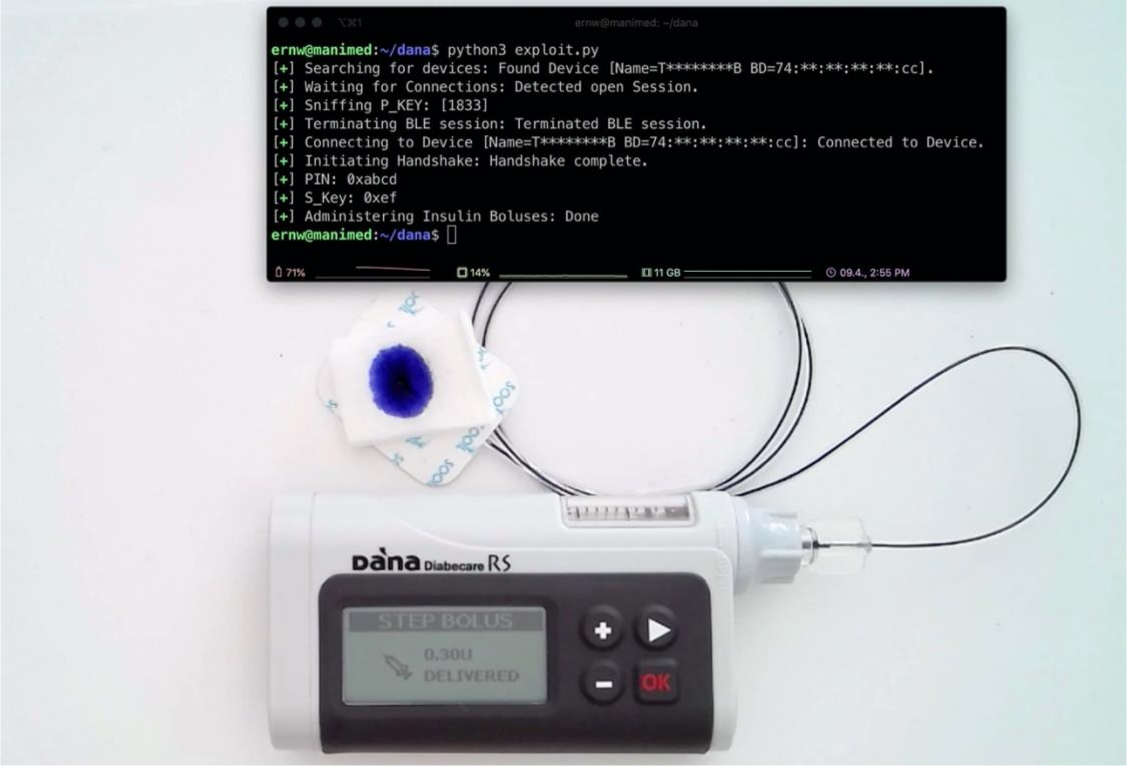
Besides, multiple client-side controls that can be bypassed were identified. The device keypad lock PIN is validated by mobile applications instead of being validated by the pump. An attacker can omit the check when communicating with the pump.

All cryptographic keys and their key material used for the application-layer encryption of BLE messages are generated deterministically, e.g. depending on the insulin pump's hardware clock and transmitted via clear text BLE messages. Further, the authentication of the communicating party only relies on the possession of the pairing key which also is transmitted in clear during every communication initiation. Additionally, the protocol implemented on top of BLE has no replay protection measures.

A detailed technical discussion of the assessment's results is can be retrieved from a publicly available white paper (Suleder, 2020) including a video of the exploit (ERNW Research GmbH, 2020).

4.3.2.3 Impact

The combination of the identified vulnerabilities empowers an attacker to hijack the insulin pump. To perform an attack, an attacker needs to be in close proximity of the insulin pump sniffing a single communication between a DANA Diabecare RS insulin pump and an application-layer paired mobile application. No BLE pairing is required. Afterward, attackers can use all functionalities that are utilizable via BLE. This may lead to serious patient harm as the manufacturer acknowledged.



```
ernw@manimed:~/dana$ python3 exploit.py
[+] Searching for devices: Found Device [Name=T********B BD=74:**:**:**:**:cc].
[+] Waiting for Connections: Detected open Session.
[+] Sniffing P_KEY: [1833]
[+] Terminating BLE session: Terminated BLE session.
[+] Connecting to Device [Name=T********B BD=74:**:**:**:**:cc]: Connected to Device.
[+] Initiating Handshake: Handshake complete.
[+] PIN: 0xabcd
[+] S_Key: 0xef
[+] Administering Insulin Boluses: Done
ernw@manimed:~/dana$ 
```

Figure 12: The DANA Diabecare RS insulin pump after an attacker hijacked the BLE session and administered multiple insulin boluses (shown with blue ink). (Source: ERNW)

The manufacturer prepared an update for the insulin pump thereby fixing all identified vulnerabilities. The Field Safety Notice (FSN) was announced in March and updated in May 2020 by the BfArM (SOOIL Development Co. Ltd, 2020). To temporarily reduce the risk of potential patient harm, the manufacturer recommends disabling the insulin pump's BLE functionality by putting it in airplane mode. Being in airplane mode, the insulin pump's therapeutic purpose can be preserved as it is optional to control the device via mobile applications. Furthermore, it must be noted that the device implements safety features such as a maximum daily dose or bolus block. These settings can only be configured on the pump and therefore not be circumvented by an attacker in close proximity.

4.3.3 Ypsomed AG – mylife YpsoPump System

This section elucidates the security assessment of the mylife YpsoPump system from the Swiss manufacturer Ypsomed AG.

The mylife YpsoPump insulin pump is the central component of this therapy system. It can transmit delivery data to a mobile application called mylife App for the mobile operating systems Android and iOS via Bluetooth Low Energy (BLE) interface. The pump cannot be controlled via BLE and, therefore, cannot be used to build a closed-loop system. The mylife App can transfer data to the mylife Cloud. The system offering a web application aims to ease communication between diabetics and healthcare professionals with the mylife therapy management solution for therapy data.

4.3.3.1 Scope

The assessment focused on the communication protocol between mylife YpsoPump and mylife Android App as publicly available in the Google PlayStore and the communication between mylife App and mylife backend. The mylife backend and a respective web frontend were not the focus of the assessment. Two insulin pumps were provided by the manufacturer, as well as test accounts and publicly available documentation.

Figure 13: One of the Ypsomed mylife YpsoPump insulin pumps tested in project ManiMed. (source: BSI)

4.3.3.2 Results

The communication between YpsoPump and mylife App is authenticated by credentials derived from publicly available information in addition to BLE pairing mechanisms. Further, the pump's battery may be drained by unauthenticated Bluetooth GATT writes, resulting in the pump vibrating.

More vulnerabilities were identified in the communication between the mylife App and the mylife backend. The mobile application and backend of the test environment communicated via HTTP and transmitted data symmetrically encrypted. In production, the communication took place via HTTPS, but the HTTP endpoint without transport-layer encryption was available, too. The key and initialization vector of the symmetric encryption were hardcoded in the mobile application's code.

Software and third-party components used are partially outdated and contain publicly known vulnerabilities. However, none of these vulnerabilities could be exploited during the test. Additionally, a password policy for the mobile application and the front end was missing. When submitting the registration form, a password hash is returned. Furthermore, a reflection of the user password during the login process while downgrading the connection from HTTPS to HTTP could be observed.

4.3.3.3 Impact

The abovementioned vulnerabilities have no impact on the main functions of the insulin pump. Furthermore, no compromise of the mobile application was possible. The communication between the mobile application and the backend was vulnerable to man-in-the-middle attackers. Many of the vulnerabilities were fixed with configuration changes. The manufacturer addressed the design and logic flaws by updating the backend, front-end, and mobile applications from a short-term perspective. The manufacturer identified no patient harm and rolled out an update.

4.4 Ventilators

In this section, the security assessment of one ventilator is described.

4.4.1 Characteristics & Environment

Ventilators are medical devices that provide temporary ventilatory support or respiratory assistance to patients who cannot breathe independently or require assistance to maintain adequate ventilation because of illness, trauma, or drugs (e.g., anesthetics) (WHO, 2011). Individual devices are built to meet stationary use requirements in hospitals or portable use. The devices also differ in capabilities regarding adult, pediatric, and neonatal ventilation and possible modes of ventilation. As failures may result in severe patient harm, ventilation systems are classified as life-critical systems. Several measures must be taken to ensure that the devices are highly reliable, including their power supply. Most devices do not have extensive external communication interfaces other than connectivity for documentation to a PDMS via, e.g., serial interfaces.

4.4.2 Hamilton Medical AG – HAMILTON-T1

This section elucidates the security assessment of the HAMILTON-T1 from the Swiss manufacturer Hamilton Medical AG (hereafter referred to as Hamilton). The HAMILTON-T1 ventilator is a portable ventilator approved for use in ambulances, helicopters, and airplanes. A configuration for military use exists.

4.4.2.1 Scope

Apart from the HAMILTON-T1 device, the manufacturer provided publicly available manuals and a firmware image. The device implements a USB and a reserved Ethernet port.

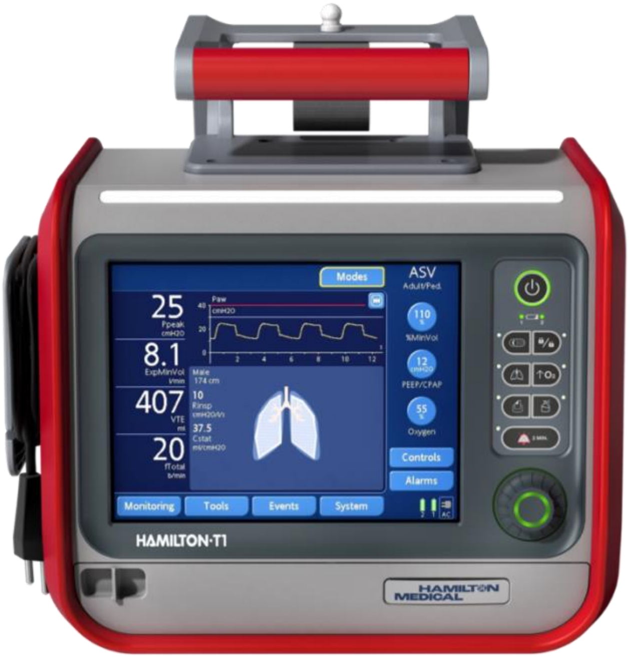


Figure 14: The tested HAMILTON-T1 ventilator. (Source: Hamilton)

4.4.2.2 Results

The HAMILTON-T1 uses a default code to enter the configuration menu of the device. This code can be found in the manual. By entering the configuration menu, it was possible to load a tampered configuration file via a USB flash drive, which resulted in an undefined state of the device. This configuration file is secured using a checksum. The checksum for tampered configurations is exposed in an error log, which is accessible to attackers. All attacks require physical access.

4.4.2.3 Impact

The identified vulnerabilities caused the device to be dysfunctional. As a result, the device did not boot. A hardware exchange of the device's logic board was necessary to recover the device. The manufacturer identified no patient harm. The manufacturer prepared an update for the ventilator, thereby fixing all critical vulnerabilities.

4.5 Patient Monitors

In this section, the security assessments of two patient monitors and their medical system are outlined after a short characterization of the devices' characteristics.

4.5.1 Characteristics & Environment

Patient monitoring solutions are used to continuously measure vital signs of patients during transport or hospitalization. The connectivity and features such as data storage, alarming functionality, and connectivity to central medical information systems of marketed products differ depending on their use case.

Patient monitors in ambulances are mostly not connected to medical systems and are used by emergency physicians and to assess the current vital signs of patients and to alert when these values exceed pre-determined ranges.

In clinical settings, patient monitors are further used to document patients' vital signs in electronic health records and to help clinicians make informed decisions. These continuous patient monitoring systems might be used during complex surveillance setups in critical care units, in operation theatres, during diagnostics or basic bedside monitoring. Different products for portable and stationary use as well as complex interconnected systems with automatic hand-over between different screens in treatment rooms, long-term data analytics and connectivity to ventilators and anesthesia devices exist. For more complex environments often dedicated infrastructure for, e.g., data storage and networks are needed.

4.5.2 Innokas Yhtymä Oy – VC150 Patient Monitor

This section elucidates the security assessment of the VC150 system by the Finnish manufacturer Innokas Yhtymä Oy. The VC150 vital signs monitor is intended to monitor a single patient's vital signs at the site of care or during intra-hospital transport. The VC150 vital signs monitor provides a small, portable monitoring alternative for sub-acute hospital and non-hospital settings. The monitor is for use on adult, pediatric, or neonatal patients.

4.5.2.1 Scope

The manufacturer provided manuals and a firmware update file. In the scope of the assessment was the device's networking functionality, which included protocols such as HL7 v2.x and its administrative web interface and the UI presented on the device's touchscreen. A lab with an HL7 v2.x messaging engine was set up to allow for testing the interface.

4.5.2.2 Results

The VC150's administrative web interface is vulnerable to a stored Cross-Site Scripting vulnerability. Further, the device can be shut down via keystroke injection. An attacker with one-time physical access to the USB ports can thus reboot the system and disrupt measurements performed by the patient monitor.

The device sends HL7 v2.x messages, such as observation results to HL7 v2.x capable electronic medical record (EMR) systems. A user with malicious intent can tamper these messages by injecting HL7 v2.x segments into the HL7 v2.x messages with a connected barcode reader. Hence, attackers can tamper data transmitted to further network-connected systems. This identified vulnerability is detailed in a blog post published in April 2020 (Suleder, 2020).

4.5.2.3 Impact

Attackers cannot inject entire HL7 v2.x messages. Further, attackers cannot control the messages' destinations. It must be noted that specific HL7 v2.x messages are specified to only contain a limited subset of all available HL7 v2.x message segments. Network-connected systems usually validate messages received from patient monitors. Therefore, attackers may only be able to inject these selected segments into a message. However, this enables attackers aware of HL7 v2.x message structures to inject arbitrary observation results, leading to misdiagnosis or medical errors. The manufacturer identified no patient harm, implemented fixes, and rolled out an update.

4.5.3 Philips Medizin Systeme Böblingen GmbH – IntelliVue System

This section explains the security assessment of the IntelliVue system from Philips Medizinsysteme Böblingen GmbH (hereafter referred to as Philips) a German subsidiary of the Dutch manufacturer Koninklijke Philips N.V.

Philips IntelliVue patient monitors are intended to be used for monitoring and recording of, and to generate alarms for, multiple physiological parameters of adults, pediatrics, and neonates. Philips Patient Information Center iX (PIC iX) is a real-time patient monitoring solution that consolidates physiological data from patient monitors and clinical information systems. This monitoring system is intended for use in professional healthcare facilities by trained healthcare professionals. They are not intended for home use.

The IntelliVue system not only allows communication between monitors and the Patient Information Center iX but as well communication between individual monitors.

4.5.3.1 Scope

In scope of the security assessment were the communication between one Patient Information Center iX surveillance station and two IntelliVue MX850 patient monitors along with network infrastructure components. The operating system hardening of the PIC iX server host as well as the provided network infrastructure were out of scope of this assessment.

Figure 15: A Philips IntelliVue MX850 patient monitor (left) and PIC iX Surveillance Station (middle + right). (Source: Philips)

4.5.3.2 Results

During the security assessment of the Patient Information Center iX application, multiple Cross Site-Scripting (XSS) vulnerabilities could be identified. Beyond that a kiosk breakout could be observed. From a network perspective, the application could be crashed via a single specially crafted packet to a network-facing service. The crash lead to a reboot of the application. An additional persistent crash could be observed in the certificate enrollment service via SCEP by providing tampered certificate signing requests. While running, this certificate enrollment service is vulnerable to a practical brute-forcing attack, which enables attackers to obtain trusted certificates to connect to patient monitors. This crash only impacts the certificate enrollment service, which runs only when enrolling new devices.

The IntelliVue MX850 patient monitor improperly checks for certificate revocations, which enables attackers with access to a trusted certificate to obtain a Man-in-the-Middle (MitM) position between the patient monitor and the server application. This position could be used to crash the patient monitor or potentially modify transmitted data. The monitor reboots after crashing, which takes about 20 seconds. In this time no vital signs are measured and transmitted to the Patient Information Center iX application.

4.5.3.3 Impact

Chaining the crash of the Patient Information Center iX application, improper certificate revocation check of the patient monitor, as well as the crash of the monitor, an attacker in possession of a valid client certificate can cause a sustained Denial of Service (DoS) of the IntelliVue monitoring system. To date, Philips has not received any reports of exploitation of these issues or of incidents from clinical use that have been associated with this issue. The manufacturer identified no reports of patient harm. In the event of monitoring interruption, there is a possibility of delayed patient treatment, however, to successfully exploit these vulnerabilities, an attacker would need to gain either physical access to surveillance stations and patient monitors, or access to the medical device network. The manufacturer is preparing to release an update to fix the vulnerabilities.

4.6 Infusion & Syringe Pumps

In this section, the security assessments of three syringe and infusion pump systems and a pump management system are presented after a short specification of the systems' features.

4.6.1 Characteristics & Environment

During therapy, the need to administer drugs to patients arises. Many of these drugs need to be administered in a specific dose range. This dose range, in which drugs are the most effective and not causing harm, is called the *therapeutic window* in medicine. In favor of manual delivery or administration, infusion systems strive to ensure safe therapies and remove dose errors. Because patients may receive multiple drugs at a time, administering multiple drugs to patients is needed. This need is where medical syringe or large volume pumps come into play. Syringe and infusion pumps are active medical devices used to administer fluids such as nutrients and drugs in the right dose, at the right time, in the right concentration to ensure the best therapeutic purpose. In hospitals, often large numbers of these devices are present.

The pumps need to be reliant and safe to prevent injury or even death from, e.g., overdosage or air in the tubing system and easy to use as often multiple pumps work in parallel. Consequently, only trained medical staff is allowed to operate and monitor the use of these pumps, which themselves contain robust safety mechanisms and alarm functionalities.

The prevalent therapy systems on the market comprise the syringe and infusion pumps grouped in a docking station (hereafter referred to as dock). This dock functions as a power supply for the pumps and often has a shared communication interface to the clinical network implemented. The prevalent pumps mostly do not contain other communication interfaces than communicating with the dock via, e.g., infrared. Newer generations of smart infusion systems feature various communication interfaces such as e.g., Wi-Fi. In most cases, a central management system allows us to monitor and configure the pumps regarding drug library transfer and sometimes installing pump updates. Many systems allow an automatic data transfer of administered drugs and dosages to connected Electronic Medical Records (EMR).

4.6.2 B. Braun Melsungen AG – Space System

This section details the security assessment of the Space infusion and syringe system from the German manufacturer B. Braun Melsungen AG (hereafter referred to as B. Braun).

The B. Braun therapy system comprises different infusion and syringe pumps grouped into docks with a communication module called SpaceCom. A central management software called OnlineSuite allows monitoring pumps and configure drug libraries.

4.6.2.1 Scope

The inspected systems were the SpaceCom communication module, two Infusomat Space infusion pumps and two Perfusor Space syringe pumps, and central management software called Online Suite with a full feature set license.

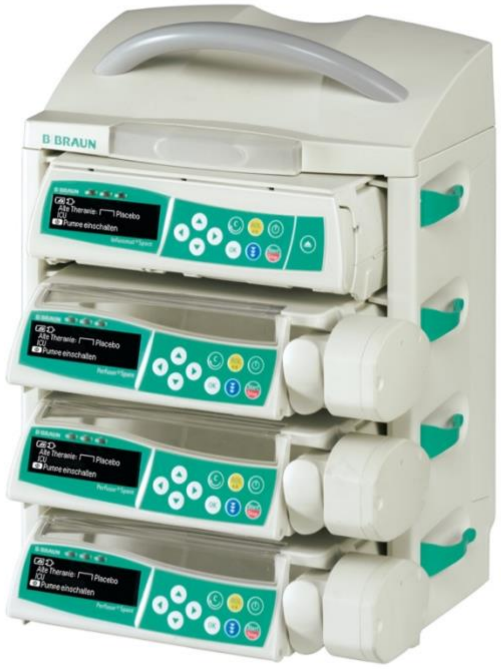


Figure 16: The B. Braun Melsungen Space system comprised a SpaceStation including a SpaceCom communication module, one Infosomat Space infusion pump, and three Perfusor Space syringe pumps.
(Source: B. Braun Melsungen AG)

4.6.2.2 Results

Issues with the OnlineSuite application's file upload and file download functionalities were identified during the security assessment. These vulnerabilities allow unauthenticated attackers to upload and download arbitrary files from and to the OnlineSuite server. This vulnerability can be exploited to either cause a Denial of Service (DoS) of the web application or to execute arbitrary code on the server.

Multiple issues concerning the session management and authentication were identified in the SpaceCom's administrative web interface. The application is vulnerable to a session fixation attack that allows an attacker to forge controlled session tokens for users.

Multiple injection vectors such as Cross-Site Scripting (XSS) and unvalidated redirects and forwards were identified in the web application. Furthermore, the login page is vulnerable to XPath injections that enable attackers to extract usernames and password hashes. An authenticated arbitrary file upload vulnerability combined with an unvalidated symbolic link and local privilege escalations enables attackers to execute commands as the root user.

Firmware images are protected against modifications with a hash that is included in the image's header. An attacker can tamper with firmware images and calculate valid checksums to provide manipulated firmware images.

4.6.2.3 Impact

The vulnerabilities result in a compromise of the Online Suite as well as the SpaceCom. Attackers might be able to prepare attacks to further connected systems such as Electronic Medical Record (EMR) systems. The integrity or operation of the infusion and syringe pumps is not affected. The manufacturer identified no patent risk. Updates were provided for the OnlineSuite as well as the SpaceCom and announced to the customers.

4.6.3 Anonymized Infusion System #1

This section presents the security assessment of an infusion system. This system can consist of a central management component, a docking station, and infusion pumps. Pumps can also function independently without a central management component. The central management can collect and report infusion information of all pumps and docking stations. The docking station allows to group individual pumps and update drug libraries on each pump.

4.6.3.1 Scope

In scope of the assessment were the communication within the lab environment, which included two pumps, two docks as well as the central applications and an API. Not in the scope of the security assessment were the manufacturer-supplied lab equipment hardening as well as hardening of the server host.

4.6.3.2 Results

During the assessment of the medical device system, multiple vulnerabilities were identified. The analysis of the pump yielded only a minor issue. For the central component's API an information disclosure in means of a directory listing and web service specification disclosure was identified.

Multiple severe vulnerabilities were identified for the dock. An outdated web server with several publicly known vulnerabilities is used. Additionally, the dock offers both, a transport-layer protected and unprotected interface. Further, the device can be rendered unreachable via unauthenticated specially crafted HTTP requests. However, the power supply of the device will not be affected. Moreover, the management interface has an insecure and broken session management as well as missing access controls. The web application implements authentication and session management mechanisms on the client-side and, hence, does not protect authentication attributes sufficiently.

Web applications used by the central component are susceptible to multiple Cross-Site-Scripting (XSS) vulnerabilities.

Additionally, one web application contains hardcoded service user credentials. The application's frontend denies the use of these credentials in means of a client-side control.

4.6.3.3 Impact

Unauthenticated, attackers with either physical access to the dock or access to the hospital network can render the dock persistently unreachable via specially crafted HTTP requests. None of the identified vulnerabilities could result in the loss of PII or PHI and do not cause any harm to the patient. The manufacturer plans an update for Q1/2021 thereby fixing all identified vulnerabilities.

4.6.4 Anonymized Infusion System #2

This section details the security assessment of a system that comprises different infusion and syringe pumps that can be grouped into docks with a communication module. An external communication interface allows to monitor pumps and configure drug libraries or to continuously transfer infusion data to clinical systems.

4.6.4.1 Scope

The inspected systems were the provided docking station as well as all external interfaces, one syringe pump and one infusion pump.

4.6.4.2 Results

During the assessment of the medical device system multiple vulnerabilities were identified. Multiple buffer overflows for network services provided by the docking station as well as in the pump’s firmware could be identified. Basic exploiting mitigations features such as Position Independent Executable (PIE) and the use of Stack Cookies were missing. Furthermore, debug symbols were not stripped.

The communication between the device and multiple services misses transport layer encryption. Transmitted credentials were identified to be stored in a reversible format. In addition, the underlying protocol to external information systems misses to verify the identity of communicating parties.

4.6.4.3 Impact

The buffer overflows could lead overwriting control flow data to take control of the application and execute arbitrary instructions. An attacker could exploit this vulnerability to crash the program or execute arbitrary system commands. The likelihood of successful exploitation highly depends on present exploit mitigation features that are either compiled into the application like non-executable stacks or stack canaries, and the mitigations that are applied by the execution environment, like Address Space Layout Randomization (ASLR). One buffer overflow was exemplarily exploited during the assessment leading to unauthenticated, arbitrary remote code execution.

The manufacturer has addressed all points that needed to be improved in close collaboration with both the assessment team and the PDMS manufacturer. Besides eliminating the buffer overflows, the mitigation features PIE, Stack Cookies were enabled, and the debug symbols stripped.

The missing identity verification for communicating parties in the protocol to external information systems might allow attackers to flood the systems with rogue devices and spoof existing pumps or external systems such as a PDMS.

No tampering of the pumps was possible, neither of the infusion parameters, infusion running status nor software or drug library settings. The manufacturer identified no safety impact.

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

This section details the security assessment of the pump management system "Copus" from the German manufacturer COPRA System GmbH (hereafter referred to as COPRA).

The pump management system, which is intended to work as a middleware between third-party pump systems and a PDMS, offers a variety of external communication interfaces allowing to monitor pumps and to continuously transfer infusion data to clinical systems.

4.6.5.1 Scope

The inspected systems were the Copus REST and Websocket APIs, Copus WardViewer, Copus Cockpit application and one external interface to an infusion pump system.

4.6.5.2 Results

During the assessment of the pump management system, which at the time of the assessment was still in a prototype state, multiple vulnerabilities were identified.

The REST API does not support transport layer encryption and authentication against the service is only possible via HTTP Basic Authentication. Besides, an API for Websocket communication was identified to be unauthenticated.

Furthermore, hardcoded user credentials were identified for these services which are used to automatically authenticate against the REST API with the Copus WardViewer application. It should be noted again, that the target of the evaluation was a product prototype. These mechanisms are likely associated with the prototype state of the software.

In addition to these findings, a vulnerability concerning the protocol between the infusion system's docking stations and the Copus information system could be identified. The Copus Cockpit has no means to verify the identity of communicating parties. Further, this interface misses transport layer encryption. These findings cannot be solely attributed to the Copus interface as major design changes in the interface's contract need to be implemented on the client and server side.

4.6.5.3 Impact

The Copus Cockpit has no means to verify the identity of communicating parties. Servers may be flooded with rogue docks and existing pumps can be spoofed by an attacker. This may lead to fake infusions documented in the Copus relayed to connected PDMS systems. Transferring data in clear might allow third parties to access sensitive information, for example, pump and infusion data. The vulnerabilities in the Copus authentication mechanisms via the REST and WebSocket APIs as well as the authentication bypass via hardcoded credentials might allow unauthorized third parties to access sensitive information, for example, pump and infusion data.

All these problems were analyzed by COPRA and the infusion system' during the evaluation phase and partly solved directly. In a first concept the communication between the docks and Copus was encrypted and secured by client and server certificates. Furthermore, all critical information, such as access data, was removed from the software products. For COPRA internal communication the HTTPS or WSS protocol for encrypted communication will be used in the future. Furthermore, all secrets used for the communication will be replaced by new ones. None of the identified vulnerabilities could cause any patient harm. Most vulnerabilities were fixed immediately.

5 Experiences from Vulnerability Disclosures

In this section, experiences from eleven coordinated disclosure processes (CVDs) in project ManiMed are described and three different categories of maturity about handling identified vulnerabilities and subsequent disclosure processes are presented.

From the authors' experience, appropriate disclosure frameworks and rules ease and simplify the processes, especially when the manufacturer is not aware of coordinated disclosure processes. This framework should include a guide to establish secure communication channels by exchanging S/MIME certificates or PGP keys. Further, rules for the collaboration, such as periods for responding, involved persons, and a "vulnerability disclosure process manager" role may be defined. Status update meetings should be scheduled regularly. Ideally, every manufacturer of active medical devices provides public contact information for reporting vulnerabilities and enabling efficient CVD processes.

Process deliverables such as an in-depth analysis of the reported vulnerabilities, proposed remediation or mitigation, a residual risk analysis, and a timeline for the patch development and rollout should be stipulated. The parties should agree on publications, the vulnerability disclosure, and other public communications such as advisories in the later process. Further, an accurate statement of remediation and mitigations on a solely technical level may help manufacturers address the identified vulnerabilities. This and the aforementioned points may differ between every disclosure. Manufacturers which are familiar with these processes and already have a mature process or framework to handle vulnerabilities ease disclosures. Often manufacturers publish a Coordinated Vulnerability Disclosure statement that points out rules, procedures, and commitments from the manufacturers so that notifying parties can know what to expect.

With respect to medical devices, manufacturers need to analyze whether reported security vulnerabilities may affect the device's essential performance or patient safety. Researchers may demonstrate observed unintended device behavior, but the manufacturer must perform the safety risk evaluation.

Theoretically, three different categories of disclosure process maturity could be observed throughout the course of project ManiMed. Although these different categories suggest a certain distinctness, the actual experiences with individual manufacturers were actually in between different categories. Especially changes over time could be observed. Some manufacturers started really well, displaying a high maturity in handling disclosure processes, but towards the end communication and participation shifted significantly. On the other hand, others started with considerable difficulties, but showed exemplary handling of vulnerabilities towards the end. Overall the project demonstrates that all participating manufacturers highly value safety, security, and continuous improvement and were not averse to challenging their own processes.

5.1 Category 1: High Maturity

In these kinds of coordinated vulnerability processes, the manufacturers are experienced or familiar with such processes and know-how to coordinate the analysis internally, implement and roll out unplanned bug-fix and security patch releases. Proper timelines of the CVD tasks and further steps are presented as well as contact persons defined proactively. In most cases, staff with security roles are involved that monitor and coordinate the CVD. A fast response, including in-depth technical descriptions of remediation plans, is presented. The process is self-propelled by the manufacturer and does not require further external impulses by the project team. The topics under discussion are the disclosure, assignment of CVEs, and publication of a security advisory.

5.2 Category 2: Middle Maturity

Here manufacturers usually admit being inexperienced regarding the respective processes and ask for appropriate help. The project team provides information about the processes to technical teams as well as decision-makers. Sometimes particular coaching is required, e.g. to explain why patch releases for medical device ecosystems, that would be superseded soon, can still be a valuable option and in fact be necessary in certain instances. The processes are based on professional and transparent communication. In the end, the released patches represent technically appropriate and clean remediation of all identified vulnerabilities in an extended but reasonable time.

5.3 Category 3: Low Maturity

Inexperience in handling security vulnerabilities is very distinctive in this category. The process usually starts with an initial motivation and voluntary participation, which then changes into a stagnant progress and can even end in artificial delays, manifesting itself through ambiguous statements about future actions.

To make matters even more complicated, some manufacturers employ a strict information policy, which strictly prohibits sharing confidential information. Under this circumstance, it can be challenging to manage a CVD process, as often not all identified vulnerabilities are eliminated at once. Residual risk analysis or effort assessment is almost always carried out to prioritize the vulnerabilities. Manufacturers may accept a subset of the vulnerabilities since their criticality is too low, or the effort required to remedy is high. Helping a manufacturer to assess, whether a vulnerability needs to be fixed immediately or if a potential risk can be accepted until a future major release, is nearly impossible under the before mentioned strict information policy.

Consequently, these processes generally suffer from different sources of delays. These can be as simple as finding a responsible contact person within the company or be much more complicated internal processes. Therefore, these processes tend to be more complicated and elongated than with manufacturers exhibiting a higher maturity in handling disclosures.

6 Conclusion and Outlook

This section concludes the project's execution, experiences, and results, thereby providing an outlook on potential further investigations or even projects. First, it is focused on the conclusions from the market analysis and the conclusion drawn from it and, in particular, about the process of gathering information about medical devices. Second, the execution and the results of the security assessments is regarded and further focuses on answering the following questions:

1. Is the current state of published information sufficient to identify technologies, including communication interfaces in medical devices?
2. Based on the security assessments' results, what can be inferred about the overall IT security posture of connected medical devices, and what are general recommendations to improve the IT security posture?
3. What precautions can vendors take to ensure a timely and efficient response to a security issue within one of their medical devices? What is the present level of IT security maturity?

After discussing the results of the IT security assessments a conclusion of the CVD processes is be drawn and finally an outlook follows.

6.1 Conclusions from Market Analysis

As mentioned in Section 3.1.1, one source of information about medical devices was the MPA database. When the Medical Device Regulation comes into effect, EUDAMED will be the central database where information on medical devices must be made available during the European market's approval process However, in the project, the EUDAMED database was not used.

A few issues have been identified regarding the MPA database while collecting data used for this project. First, the database does not provide technical information about the communication interfaces of the medical devices. As the main reason for the market analysis was to identify medical devices with an appropriate attack surface (e.g., wireless communication interfaces such as Bluetooth or physical interfaces such as USB). This information could not be retrieved from the database and had to be collected by other means, for example, via the datasheets provided by the FDA (in the case that the device is listed there). Providing such information would not only be valuable for the data collection process performed within this project. However, it may also be of interest to patients with a technical interest to understand medical devices' communication interfaces in a particular device category. It remains to be observed how far the EUDAMED database can provide such information. However, from the authors' perspective, a database providing technical information about the communication interfaces is useful for different audiences. The information that should be contained in such a database for a medical device is the types of interfaces (i.e., USB 3.0, Ethernet) and a reference to the interfaces' technical datasheet.

Moreover, during the information gathering using the MPA database, it was found that not necessarily all approved devices on the German market have been listed within this database. Reasons that could be identified were product families that build a construction system to enable flexibility, compatibility between multiple products of the same product family, which resulted in listing the individual part separately. Further, the database does not contain sufficient information about medical software certified as *Software as Medical Device* (SaMD). Other possibilities for not identifying all products could be that only access to the public part of the database is possible for private parties.

6.2 Conclusions from Security Assessments

In total, more than 150 vulnerabilities were reported to manufacturers in scope of the project. It became apparent during the assessment that the vulnerabilities were often found in the accompanying infrastructure but rarely in medical devices. For example, infusion pumps were usually found to be robust because they perform their function regardless of their infrastructure status, i.e., even if the infrastructure is down. However, the stations for the pumps were usually less secured, and more vulnerabilities could be identified there. On the one hand, this is expected since the stations usually provided more communication interfaces such as Ethernet ports. On the other hand, these stations usually communicate directly with the pumps and provide an attacker's interface for potential access to the pumps. Often, the infrastructure components are classified as an accessory for medical devices. This classification makes it easier to apply modifications afterward, but this may also lead to a view that the infrastructure components' security is less critical. Nevertheless, it should be remarked that a medical device's security assessment should always include the accompanying infrastructure components to get a realistic evaluation of the device's security posture in its operating environment.

It should be mentioned that the security assessments' results may be affected by certain biases. Since the project's vendor participation was voluntary, it was expected that those vendors were most likely to cooperate that already possess a certain maturity in their IT-security processes. To prevent this bias's existence, the ManiMed project team contacted the vendors after finishing the market analysis instead of applying to get their devices assessed. However, it should be mentioned that it was also one of the project's goals to support the participating vendors in identifying existing room for improvement in their IT-security processes and close these gaps. Although it was not evaluated if a bias existed and how large it was. The project certainly helped the participating vendors to improve their overall IT-security posture. Insofar, the project collectively affected the participating vendors in a positive way.

As mentioned in Section 6.1, another bias may exist due to the selection criteria imposed on medical devices. Although these selection criteria have been carefully chosen and the device categories contain critical functionalities, these criteria cannot ensure that the performed security assessments apply to the entire German device market. Therefore, it should be noted here that this was not the intent of the project to test the entire medical device landscape in Germany. However, the intent was to get a gross estimate of the German medical device market's IT-security posture, based on which further considerations can be made.

The security assessments also demonstrated that the IT-security posture varies significantly between vendors and highly depends on their maturity. Therefore, the question arises on how the maturity and the different vendors' IT-security posture can be raised to an equally high level. On the one hand, this certainly depends on the legal framework that defines the requirements based on which medical devices are approved for the market. On the other hand, this depends on the vendor's motivation to proactively consider IT-security related topics. This motivation shows whether the vendors implement and enforce a secure development life cycle for their medical devices in combination with a timely and effective response to disclosed vulnerabilities, not only because it is legally mandated.

Overall, the large number of vulnerabilities identified during the project demonstrates room for improvement in the medical device sector. Different parties, such as regulators and vendors, must increase efforts to raise the devices' security levels.

6.3 Common Issues

To support vendors and operators of medical devices in this endeavor and to improve the overall IT-security posture, we will summarize here common issues identified during the security assessments and provide suggestions on how to fix them.

6.3.1 Types of vulnerabilities

It is not uncommon for security vulnerabilities to arise due to discrepancies between a socio-technical system's specified and real behavior. This discrepancy can hardly be identified in documentation audits and specification reviews. Well-proven means are external penetration tests, in which a complex, active medical device is examined in-depth before productive use. Dependent on the device functionality, external medical and non-medical, wireless and wired network interfaces, Bluetooth and USB interfaces, update, maintenance, and configuration mechanisms are examined for vulnerabilities, and existing security measures are checked effectiveness. During these tests, design, implementation, and configuration errors can be observed. As such, vulnerabilities can be classified into three classes: design errors, implementation errors, and configuration errors (Boehm, 1984).

Configuration errors can occur at any application stack level, such as network services, operation systems, platforms, and web servers. Typical examples for configuration errors are default accounts, weak configurations of cryptographic libraries, and mechanisms or information disclosures such as version numbers or error messages. These errors depend on the specific operational environment and often come with other operational deficits such as outdated software. The vulnerabilities may be easily fixed by changing the configuration and applying updates and patches. The remediation may be appropriate but not sufficient as fundamental missing mechanisms cause them. These vulnerabilities shed light on missing configuration and operation concepts such as appropriate security hardening across any part of the application stack and processes to continuously assess the system's status and maintain it, for example, through proper patch management. It becomes clear that this denotes a shared responsibility between medical device manufacturers and operators.

Implementation errors can happen when a functionality’s specified and real behavior differ due to a coding issue. For example, an application is vulnerable to attack when user-supplied data is not validated, filtered, length-checked, or sanitized by the application and, therefore, insecurely processed. The vulnerable code needs to be fixed to remediate these issues, which can be tricky when interfaces to libraries or other application interfaces (API) have to be changed. These efforts will lead to a patch as the final artifact or may come along with regular updates. Learning from these defects by incorporating defensive and secure programming techniques combined with unit and integration testing is a step towards changing the software development culture within an organization into one that produces more secure code having a feedback loop in the development lifecycle.

Vulnerabilities that represent design errors can occur when mechanisms or interfaces are designed without a dedicated security-focus or when mechanisms can be bypassed or rendered ineffective. Often these issues arise due to insecure interaction between components and entities in communication systems that are assumed to be trusted. The complexity of fixing design flaws depends on the affected parts of the system. Single libraries or applications may be fixed easier than communication interfaces to external systems or environments as these need to change the respective interface contracts to avoid compatibility issues too.

Remediation and mitigation should always keep a moderate eye on the criticality of a vulnerability. A customer information or temporary measure can also be sufficient until remedial action is taken downstream. In some cases, vulnerabilities must be fixed together if they affect the product as a whole. Often, not all identified vulnerabilities are eliminated at once. Residual risk analysis or effort assessment is almost always carried out to prioritize the vulnerabilities. A subset of the vulnerabilities may be accepted since their criticality is too low, or the effort required to remedy is too high.

6.3.2 Patch Management

One major issue that is present for medical devices and nearly all IT areas is patch management. However, patch management may play a more critical role in medical devices when exploiting a vulnerability. Here, the question arises how a patch can be securely rolled out to devices affected by a vulnerability. The disclosure process of vulnerabilities and the secure development process of the patch will be discussed in Section 6.4. However, it should be mentioned here that they are also essential to provide a patch on time. The following part only focuses on the process of providing patches for devices.

The rollout process of the patch consists of several sub-steps:

- Development and patch validation
- Providing the patch in a secure way
- Announcing the patch
- Provisioning of the patch in a secure way

Of course, these steps may depend on the type of device that needs to be updated. For example, it is much simpler to apply a patch for a patient monitor that provides an update mechanism by inserting a USB stick with the new firmware or via the Internet than updating an implant within a patient's body. Depending on the device type and patching processes' complexity, it also needs to be determined who should be authorized to perform such an update. Here, it should be considered that the average person may not be aware of security updates for their devices, i.e., this person should not be responsible for deploying such a patch. Therefore, two options exist a) trained personnel provisions the patch via the provided provisioning mechanism or b) the device performs automatic updates via an Internet connection. However, it should be noted that the second option requires a secure infrastructure used for these automatic updates.

Nevertheless, there are general guidelines that should be followed in this process. First, as stated in the previous passage, the patch should be provided securely. This means that the patch file should be cryptographically signed with a private key accessible by the vendor. Of course, the device to which the patch should be applied to must also cryptographically verify the firmware's signature. This verification ensures that unauthorized parties cannot tamper with patch files, and only vendor-approved patch files are applied. However, this also mandates that the vendor maintains a public key infrastructure and develops processes for cases when the corresponding private key is compromised. As an additional measure, the patch file may also be provided in an encrypted way. However, as the cryptographic key to decrypt the patch file must be present on the device, this measure usually does not prevent a sophisticated attacker from obtaining the decrypted patch file as he may, for example, read out the key from memory via special hardware. Therefore, signing is the most crucial part, as it proves that the patch file comes from a trustworthy source.

If a mechanism to provide and verify signed patch files cannot be implemented, another option would be to provide the patch file on an HTTPS secured website, where the domain is under control of the vendor. Providing the file in this way implicates that the vendor provided the file as it is present on his website. However, a downside is that when the patch file is provisioned to the device, the device can no longer verify the patch file's validity as no cryptographic signature is present. Hence, if the file gets compromised after it has been downloaded from the corresponding website (for example, if the device used to download the file is compromised), it cannot detect such a modification.

Affected patients need to be notified that a patch needs to be applied to their devices. Therefore, a communication channel must be established in advance to ensure that all patients using a medical device can be reached. Finally, this announcement should also include what the patients must do to ensure that the patch is applied. It should be mentioned that this process might also vary depending on the type of device. Devices usually only used in hospitals and are not possessed by the patient directly may require other communication channels than devices such as insulin pumps that the patient continually carries.

Overall, vendors should devise a detailed patch management process before releasing a medical device to ensure that patches can be rolled out promptly and securely. They have to consider several factors in establishing such a factor, such as how the patch is provided, who applies the patch, and how it is communicated in the first place that a patch is available.

6.3.3 Operational Environment

Another noteworthy point is that it is often not well-defined in which environments medical equipment should be operated. Hence, discrepancies exist between the operating environments that vendors assume and the operating environments that the operators of the medical devices find. For example, a vendor may assume that his device is operated in an isolated network environment, where no other devices are placed, assuming that no devices can communicate with the device's services in this case. However, the medical device operator may and should assume that the device can be operated in any network and that its security does not depend on the network environment. This discrepancy in the assumptions can lead to severe security issues. For example, if a hospital network does not use any segmentation, all devices can communicate. It can also be the case that the guest network for patients is directly incorporated here, i.e., patients connecting to the guest network with their laptops or mobile devices may access the corresponding devices if there is no segmentation. Suppose the services exposed by the medical devices are designed with the assumption that devices are operated in an isolated network. In that case, the devices' security is affected when, for example, no authentication is in place.

Sometimes, reducing these design flaws is achieved by demanding operating environment security requirements as a single defense line. This approach shifts the effort for and the assurance of the system's security to the operator, which cannot be accepted as it contradicts respective defense-in-depth and security by design approaches.

Therefore, it should be concluded that vendors need to provide clear guidelines for the environments in which the devices are operated. Vendors should always assume the device is operated in an unsecured environment and that the device's services can be assessed. Therefore, services need to be protected by mandatory protection measures following a defense-in-depth approach, such as authentication/authorization mechanisms. Vendors should clearly state the security implications that arise from operating the device in an insecure environment.

Nevertheless, operators of medical devices should also consider segmenting their network to isolate networks for medical devices as an additional defense layer. This segmentation reduces the risk that an unsecured service of a device is unnecessarily exposed. The design of network segments and their interconnection via firewalls with appropriate rules can imply significant effort depending on the network's size and the number of devices.

6.3.4 Authentication, Authorization and Access Controls

Moreover, authentication mechanisms often pose an issue for different types of medical devices. First, as stated above, these mechanisms may not even exist if it is assumed by the vendor that the device is operated in a secure environment. Implications that arise of these assumptions are explained in Section 6.3.3.

Second, the authentication mechanism can be weak or even have vulnerabilities that allow rendering it ineffective. This mechanism typically provides the gateway to the device's core functionalities. It should be analyzed in detail in security assessments such that weaknesses or vulnerabilities can be identified within the development lifecycle.

Third, the management of authentication factors such as passwords may pose an issue. That is, often, devices have default accounts with default passwords, and the operators of the devices are not required to change these passwords during or after the provisioning of the device. Sometimes, it may also not be possible to deactivate such accounts or reconfigure their passwords. Attackers may then use these default accounts with their default passwords to access the devices.

Hence, vendors should implement mechanisms that force changing such passwords during the device's provisioning phase. However, device-specific considerations may play a role here. An over engineering of security mechanisms may lead to situations in which a health professional cannot access essential device functionality. Therefore, it cannot be just mandated that all devices need to have proper mechanisms in place such that the authentication factors are changed during the provisioning of the device.

Nevertheless, if authentication factors are changed during the device setup, a process needs to be established for distributing these factors to the operating staff. As a result, these mechanisms need to be appropriate and effective but often represent a compromise between security and medical functionality. This compromise needs to be well laid out. A discussion based on a device's different operation modes such as configuration mode, maintenance mode, and medical operation mode often resolves complex security problems into smaller problems with more comfortable but secure solutions. The BSI document "Cyber Security Requirements for Network-Connected Medical Devices" (BSI, 2018) may be worth a consideration.

6.3.5 Communication Protocols

During the security assessments, each vendor uses its own set of partially proprietary communication protocols for external device connectivity interfaces. Often proprietary protocols have been implemented to a large extent. This vendor locked environments lead to a large variety of communication protocols used in the same environment for similar purposes due to systematic incompatibility.

On the one hand, this variety makes it difficult to establish clear security guidelines for the used communication protocols. On the other hand, in some development cases, the need for custom protocols may exist. Further, operators hardly can demand and specify security requirements in public tenders, when the provided solutions are black boxes whose security mechanisms and protocols cannot be assessed in an easy way. This missing transparency worsens with every new system operated. Nevertheless, a set of standard communication protocols with precise security requirements would reduce the room for misunderstandings or mistaken implementations that may result in vulnerabilities. Overall, such interoperability endeavors would need to be based on a joint effort of all involved parties.

6.4 Conclusions from Coordinated Vulnerability Disclosures

In this section, experiences from the disclosure processes are presented and concluded, especially those, which are considered fundamental for performing coordinated vulnerability disclosures and important to improve medical devices' security.

The coordinated vulnerability disclosure process followed by the authors is commonly used by security researchers to report vulnerabilities and laid out in Section 2.11. The respective experiences are presented in Section 5 and it can be concluded that the way of handling the discovery of security vulnerabilities varies considerably between different manufacturers. Any CVD process is time-consuming and requires enormous effort and resources. The transparent handling of vulnerabilities and their disclosure is one of the crucial points in this project and in every CVD process. Security should be part of the product's lifecycle and regarded in the risk assessment. There might be a misconception that products with published security vulnerabilities are of worse quality than products with no known vulnerabilities. This bias is called observation bias, as only manufacturers who actively communicate their efforts and learning processes are perceived. In contrast, the belief that remaining unrecognized in terms of security vulnerabilities protects manufacturers and their products is a misconception as no incident has happened yet. Anyone in the market may observe efforts to keep incidents and vulnerabilities confidential and sealed in alignment with the security principle by obscurity. Every system and security mechanisms should be considered public as the quote "we shall assume that the enemy knows the system being used" (Shannon, 1949) by Claude Shannon from 1949 in the context of his work on Communication Theory of Secrecy Systems states regarding cryptographic systems.

To ease and accelerate processes, especially when the manufacturer is not familiar with CVDs, a respective disclosure framework and rules are highly recommended. Additionally, the vendor should establish a transparent process to respond to such security issues and to mitigate the resulting risks on time. For this, the vendor should provide contact information where such issues can be reported, usually a dedicated email address. Since the reported issues often contain critical information about the identified vulnerability, a secure mechanism to communicate via encrypted emails, for example, by providing a PGP public key along with the email address should be provided.

After an issue has been reported, the manufacturer should acknowledge the issue's receipt on time (e.g., within one workday). The receipt of the vulnerability report should trigger several internal processes:

- Corresponding subject matter experts need to be assigned to evaluate if the report is valid.
- The subject matter experts need to determine the tasks to fix the vulnerability, and corresponding personnel needs to be assigned to these tasks.
- The risk posed by the vulnerabilities needs to be assessed.

Based on the risk, appropriate parties need to be included in the process, for example, because of further legal requirements of reporting such issues or for technical advice. The manufacturer is aware of his products hence he can perform an accurate risk analysis and the finder determines the technical complexity and technical impact of a vulnerability.

Another outcome from the disclosure processes within the project ManiMed is that facilitating the communication between manufacturers and authorities such as BSI and BfArM may speed up processes. Further, the technical analysis of the vulnerabilities eases the identification of organizational measures to reduce the risk of patient safety impairment temporarily. A deactivation of services or networking functionality may retain a device's therapeutic or diagnostic purpose while gaining enough time to implement technical fixes. Additionally, the products often implement additional safeguards that may also help in implementing temporary measures.

Apart from any disclosure process, it would be beneficial to have a legal framework that formalizes this process's requirements. Current German legal frameworks mainly focus on safety aspects of medical devices and are concerned with security issues only as far as they affect safety. A legal framework for the disclosure process of all security issues (not only those that may have a safety impact) would provide vendors with a clear guideline on the required steps when they received information about a vulnerability in their product.

6.5 Outlook

Achieving a high-level of IT-security is not a one-time task but a complicated and time-consuming process. We will provide an outlook on potential further investigations that can help raise the overall IT-security level of medical devices.

First, to gain regular insights into the state of IT-security of medical devices, it is necessary to perform such security assessments regularly and in an appropriate and realistic test environment. Project ManiMed provided valuable insights on medical devices' IT-security posture only at this specific point of time. It is indispensable to perform such assessments regularly (e.g. each three to five years) to evaluate the improvement on security.

Second, to gain a broader view of medical devices' IT-security state, it is crucial to include a broader set of devices and additional device categories as well as the accompanying infrastructure. However, to keep the size of such a project manageable, it makes sense to devote an own project for each device category or groups of device categories (e.g. radiology equipment) that should be assessed. Overall, this would allow for a detailed and comprehensive statement about the IT-security of specific device categories. In general, it is expected that manufacturers carry out such tests regularly in their own interest.

Third, the way of handling the discovery of security vulnerabilities varies considerably between different manufacturers. A disclosure framework and rules that manufacturers agree and adhere to eases and accelerates processes. It would be desirable to harmonize such processes on an international level.

Fourth, it is favored to reduce burdens of establishing clear security guidelines for medical communication environments. The often vendor-locked environments lead to various communication protocols used in the same environment for similar purposes due to systematic incompatibility. Targeting for greater interoperability can create more transparent and observable systems that use a shared security infrastructure such as a PKI, rather than rebuild security infrastructure in each closed environment. These efforts may massively reduce the efforts needed for operation.

ManiMed is the first project of its kind and the results are groundbreaking in terms of the number of identified vulnerabilities, the number of devices and classes assessed, cooperation and the subsequent disclosure processes. The project results hopefully encourage manufacturers to challenge their processes as professional handling, communication and a secure lifecycle enhance trust and ensure security throughout the lifecycle of the product.

7 IT Security Assessment Methodology & Scope

A general methodology and scope for assessing connected medical devices have been prepared and illustrated to provide the reader with background information on the questions that an IT security assessment is supposed to answer.

The presented sections and methodologies do not claim completeness, nor should they be regarded as mandatory solutions. The assessment of medical devices is highly specialized. Each assessment is individual regarding the device's medical use case, present interfaces, used technologies, and assumptions to its environment.

The sections are compiled from a security auditor's view who assesses the device from a black-box perspective. It should be noted that the methodology cannot be used to determine how probable it is from an a priori point of view that one of the described vulnerabilities is residing within the device. Other factors, such as if and how unit tests focusing on security aspects are conducted during the Software Development Lifecycle of the product, and the size of the vendor's security department would need to be included to estimate an a priori security posture. A guideline for medical devices (where such points are discussed) has been compiled by the BSI (BSI, 2018). The presented methodology, therefore, complements the BSI documents from a security assessment perspective

Most of the steps and tests are directly motivated by vulnerabilities that affect the corresponding interface, functionality, application, or hardware. However, specific points do not directly correspond to a vulnerability but are necessary as a preliminary step to learn more about the target device.

Due to the complexity of medical devices and their environments, a practical security assessment should focus on the device itself and the device's environment. Consequently, a security assessment should draw connections between the communicating components as a vulnerability in a system's subcomponent that may affect other components, devices, or interfaces.

7.1 Methodology: Attack Surface Analysis

Documentation will be taken into account if provided by manufacturers or publicly available to assess devices' attack surface. This documentation includes design documents such as architecture specifications, product, and software specifications, development documentation such as interfaces, communication flow diagrams, implementation guides, communication protocol specifications, and conformance statements for medical communication standards such as DICOM or HL7v2.x and more. Furthermore, used technology stacks and third-party software, open-source libraries, and operating systems are of interest.

The information-gathering phase aims to collect as many details as possible of the device and its environment to assess its attack surface for further analysis. To achieve this, running and exposed services, used protocols, disclosed technologies and their version numbers, used operating systems, basic device behavior, and administrative interfaces are collected. Exceptional functionality and complex mechanisms within the devices and their software are documented for further in-depth analysis by inspecting the device's or application's offered functionality.

The gathered information is categorized by the software’s or device’s mode of operation as proposed by the BSI recommendations for medical device manufacturers (BSI, 2018):

A) **Medical operation mode according to intended medical purpose:** In this operating mode, the product is used for its intended medical use, such as measuring vital signs or administering insulin boluses.

B) **Configuration of the device:** In this operating mode, the device is being configured for its intended medical use. This includes both cybersecurity configurations that ensure a secure technical operation as well as the settings necessary for medical operation mode (for example, parameters adapted to the patient).

C) **Technical maintenance:** In this operating mode, updates from the manufacturer or third-party providers are being installed, and necessary calibrations or adjustments are being made.

Further, the different components of the communication systems and communication flows are documented. Besides the medical device itself, there might be further components that are worth assessing:

- Device firmware and software updates
- Mobile applications that interact wirelessly with the device via WLAN, NFC, Bluetooth, etc.
- Management and Control Software
- Service and support software for advanced configurations of the device and its environment
- Server applications, network infrastructure, and interfaces to clinical systems
- Administrative (web) interfaces

7.2 Methodology: Communication Interfaces & Protocols

This section describes methodologies for performing security analyses of medical devices' interfaces, which become more and more critical as more and more devices are networked.

Security assessments might be performed following a white-box or a black-box approach. Experiences show that white-box security assessments are more effective and efficient in assessing a target's attack surface while reducing the effort needed to assess the device. Following a black-box approach generally requires more resources to achieve a comparable result as to a white box test. Albeit, chances to miss vulnerabilities will still be higher for a black-box approach, and some issues might only be verified vaguely.

Proprietary communication protocols are being analyzed. In scope are, Man-in-the-Middle attacks, eavesdropping of the communication, downgrading of used ciphers, employed cryptography, and the authentication process. Tests that are performed include, but are not limited to, secure authentication, secure communication (encryption), authentication mechanisms, security assessment of session management, integrity checks. If needed, communication interfaces are setup and mocked in a small lab to assess,e.g., medical interfaces.

The communication is based on a plethora of standardized, open, or proprietary communication protocols using interfaces such as:

- Ethernet, WLAN & Cellular Networks
- Bluetooth & Bluetooth Low Energy (BLE)
- Universal Serial Bus (USB)
- Radio-Frequency Identification (RFID) & Near Field Communication (NFC)
- Serial Interfaces (e.g., RS-232)
- Debug Interface (e.g., UART, JTAG)

7.3 Methodology: Hardware and Embedded Platforms

The analysis of the hardware components is typically performed in three steps, as described in the following. Depending on the complexity of a target device or platform, the steps are also applied to each sub-component. This way, even complex systems can be reliably assessed by using the divide-and-conquer principle.

The central aspect is reconnaissance work on both passive and active components used within the device and drawing rough schematics. Research on publicly available documentation is performed, creating a portfolio of built-in parts to map documented interfaces and identify potential security features. Above this, noticeable pads, contacts, and headers on the PCB/device are identified and mapped with the associated chips and their function.

7.3.1 Active Analysis of Identified Interfaces

All identified interfaces are evaluated concerning their functionality and usage. Identified headers are used for active communication with the device while tagging every single pin/pad function. Accessible interfaces are used to extract data and to communicate with the device. If possible, this also contains the extraction of configuration data and firmware.

Another aspect of this step is using logic analyzers to tap into single components' communication lines and identifying system commands and parameters.

7.3.2 Manual Access to Memory Components

Memory chips that were identified during the previous steps but could not be accessed via the available buses will be physically extracted from the circuit. Then all available data will be obtained via the protocols supported by the chip.

7.4 Methodology: Mobile Application

Most mobile apps used in medical contexts process confidential or sensitive data and communicate with internet-facing backends or nearby medical devices and equipment. Apps are assessed with the following approach that covers the most relevant aspects.

7.4.1 Static Analysis

During static analysis, all files locally stored by the application/container are analyzed in detail. For this purpose, the files are extracted and, depending on the format, unpacked or decrypted. Subsequently, all files are scanned for potentially critical information (i.e., credentials, URLs).

Static analysis is carried out for various states of the app. In this context, the state of an app can best be described by the difference between a recently installed but unused version of an app in contrast to the same application after a user has configured and used it for the first time.

The static analysis aims to identify how an application handles both persistent files/data (like credentials) and temporary files.

7.4.2 Dynamic Analysis

During dynamic analysis or runtime analysis, an app/container is analyzed using debuggers or specialist tools like *snoop-it*. During the analysis, variables, processes, and functions are manipulated at runtime. A core aspect of dynamic analysis is interaction with the app’s actual GUI, where malicious and faulty input is used to identify potential flaws and risks. The purpose of dynamic analysis is to rate data handling during runtime and the efficiency of local access controls and input validations.

7.4.3 Communications Analysis

During communication analysis, the proxy setting is used to redirect all data from and to the app through an attack proxy. Data transmitted via HTTPS or protected by SSL or TLS is decrypted, if possible. If the application ignores the device’s proxy settings, the traffic is routed through a transparent proxy. This communication analysis aims to identify flaws concerning data in transit and evaluate the amount and type of data transmitted.

Apps may also transmit data via other communication channels such as Bluetooth or NFC. The corresponding communication does not traverse the attack proxy. Therefore, this communication must be analyzed by other means, for example, by analyzing the relevant functions of the app via static analysis (see Section 7.4.1). The communication may also be analyzed with special hardware that allows sniffing the traffic. Afterward, the recorded traffic can be analyzed further.

7.4.4 Implementation Testing

Implementation testing is used to find flaws in a program by sending malformed/semi-malformed data in a (semi-) automated fashion and evaluating a system's behavior processing this data. This so-called protocol fuzzing modifies the values of a packet delivered to the target and might contain values the component cannot deal with (e.g., resulting in a crash). The implementation test will verify the correct forwarding and handling of packets on both the network and application layer.

7.5 Methodology: Web Application

Web applications are used in medical contexts, such as patient portals, process confidential or sensitive data, and communicate with Internet-facing backends or nearby medical devices. Furthermore, administrative web applications to manage the medical devices’ environment, such as in-hospital networks, may exist. In this section, the focus of the security assessment of various web applications is explained.

7.5.1 Documentation & Automated Assessment

Based on a manual simulated use of the application, its structure is documented to identify potential attack vectors (see Section 7.1). For example, URLs, request methods, encryption (e.g., SSL), request parameters, and used cookies are documented. This documentation is used for all further manual tests.

An automated assessment is carried out using a web application vulnerability scanner that examines the application based on the documented structure. The results will be verified manually and, where necessary and appropriate, supported by an experienced auditor's additional tests to eliminate false positives and verify actual vulnerabilities.

The automated scan includes *spidering* (i.e., identifying endpoints within the application by following links within the application in an automated way) of the web application, identifying parameters in form fields, or query parameters. Further web server vulnerabilities are assessed. Basic tests for injection attacks (SQL Injection, Cross-Site Scripting, …) and undesired behavior, such as causing application errors, are performed. Potentially vulnerable functionalities such as file uploads and downloads are identified, and information disclosures in error messages, stack traces, or HTML comments are collected.

7.5.2 Client-Side and Server-Side Controls

Many web applications implement controls on the client-side. This module checks if security-relevant controls that are implemented on the client are also implemented on the server-side. The assessment comprises, but is not limited to, URL parameters, HTTP cookies, HTTP headers, hidden fields, length limitations in form fields, or validations done in client scripts.

7.5.3 Authentication

The authentication mechanisms of a webserver or application are analyzed for potential attacks and best practice violations. The assessment includes, but is not limited to:

- Strength of the implemented method(s)
- Dictionary- or Brute-Force-Attacks including customized dictionaries
- Certificate checks (key length, trusted CA, cipher strength, extensions)
- Password reset procedures
- Password policies
- Hardcoded credentials
- Manufacturer and service accounts
- Man-in-the-Middle-Attacks

7.5.4 Session Management

The session management of the web application will be analyzed for:

- Predictability of session tokens
- Encrypted transmission of the session tokens, including the analysis for proper encryption methods
- Cookie attributes
- Session termination
- Cross-Site Request Forgery/Session Fixation

7.5.5 Access Controls/Role Management

If a web application uses different user roles (e.g. admin, standard user, guest user), it must be checked whether access controls are implemented and enforced thoroughly. At least two user accounts (A, B) for each role are required to carry out those tests. The following privilege escalation tests are performed:

- Vertical privilege escalation: Is administrative functionality accessible by low privileged or anonymous users?
- Horizontal privilege escalation: Can user A access data of user B?

7.5.6 Injection Attacks

Automated tools are not able to reveal all vulnerabilities within a web application. Hence, it is necessary to analyze all input parameters further manually. Manual testing includes a general assessment of the input validation concept (design and actual implementation), SQL Injection, Cross-Site Scripting (XSS), LDAP Injection, OS Command Injection, File Inclusion, Path Traversal, or Template Injection. This is highly dependent on the specific application, its technology, and its complexity.

7.5.7 Logic Flaws

Logical flaws within a web application result from predetermined procedures that were created by the developers. During this assessment, these procedures will be modified, and the behavior of the application will be checked. Typical tests include:

- Manipulation of HTTP headers
- Deletion of parameters
- Assessment of multi-stage functions
- Intentional causing of errors
- Assessment of upload and download functionality
- Assessment of update and configuration export or import functionality.

7.5.8 Information Disclosure

During the complete assessment, the web application's output is monitored for information that is not supposed to be available, such as version information, internal hostnames, IP addresses, default files/folders/content, and source code. Such information may be used by an attacker to prepare further, more sophisticated attacks.

7.5.9 Application Server Assessment

The tests that will be performed for the web/application server include, but are not limited to, an enumeration of other services, tests for known vulnerabilities, identification of default content, black-box test for insecure configurations, check for insecure SSL/TLS usage.

7.6 Methodology: Infrastructure, Network & Server

All network infrastructure devices and server systems will be checked for configuration errors and known vulnerabilities, both on a system and protocol level. Automated tools are used for the initial assessment. The results allow a more in-depth analysis of the discovered systems conducted based on the auditors' experiences, specialized, or specially developed tools.

The assessment contains operating system fingerprinting, authentication checks, checks for default accounts, enumeration and test of running services, configuration errors, use of insecure management methods such as telnet over untrusted networks or protocol misconfigurations, and vulnerabilities on the network layer.

8 Appendix

In this part, additional information, further references or supplemental material is provided.

8.1 List of Vulnerabilities, Advisories and External References

The following sections list the security advisories and security notifications (see Section 8.1.1), publications, blog posts and articles (see Section 8.1.2), as well as talks, presentations and interviews (see Section 8.1.3) that were created in the context of the ManiMed project.

The vulnerabilities shall be acknowledged to Julian Suleder, Birk Kauer, Nils Emmerich, Raphael Pavlidis, Linda Huischen, Jens Beyermann, Florian Bausch, Gregor Debus, Dennis Kniel, Dr. Andreas Dewald of ERNW Research GmbH, Dr. Oliver Matula and Dennis Mantz of ERNW Enno Rey Netzwerke GmbH.

8.1.1 Security Advisories and Notifications

The following security advisories were published by manufacturers or the ICS-CERT:

- 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 Publications

The following publications were released in context of project ManiMed:

- 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 Talks

The following publications were given in context of project ManiMed:

- Julian Suleder, Dina Truxius. **Entdeckung und Veröffentlichung von Sicherheitslücken in einer Insulinpumpe.** IT-Tage 2020. December 10, 2020. Frankfurt, 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 Truxuis**. 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 Template Letter

The following template has been used for the letters sent to selected hospitals in Germany. A translation to English can be found below.

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,

____

English Translation

BSI-Project ManiMed: Security assessment of connected medical devices

The digital transformation is already prevalent in many areas of life. In the healthcare industry more and more medical devices are interconnected such that the number of medical high-tech devices in hospitals rises continuously. Our research demonstrates that medical devices often only contain basic security measures. In the clinical environment these devices are, among other things, infusion pumps, implants or large medical devices such as CT or MRT. Especially in a clinical environment, the highly complex and critical field of application as well as the long lifecycle and intensive usage of the devices poses a serious problem as it is not uncommon that basic security measures are missing. A defective or manipulated device can pose a massive threat to a patient's life.

The Federal Office for Information Security (BSI) in its role as the central IT-security agency of the German state seeks to sensitize vendors and the public about IT-security risks of networked medical products. As a reaction to the often-fatal security reports of connected medical device, the BSI initiated the project Manipulation of Medical Devices - ManiMed and has selected us as the contractor. In this project, an analysis of the IT-security state of these devices based on security assessments should be performed.

For the selection of the medical devices, we would like to get a realistic view on devices used during the daily routine in clinics in order to get the most added value from the project, since the value for society by identifying vulnerabilities is significantly larger for frequently used devices than for less widespread devices.

As an operator of medical devices in Germany, you can contribute to this course. If devices can be selected for the assessment, which are operated by you, you benefit yourself as eliminated vulnerabilities in these devices provide a security gain for you and your patients. Due to this reason, we would like to ask you to inform us, which networked medical devices you have purchased in the past five years or plan to purchase in the future. Even a selection of such devices would be of help. We guarantee that we use the provided information in a confidential manner.

If you have any questions, I together with the BSI are at your disposal and we would be happy to receive your response.

Best regards,

____

8.3 Questionnaire

Two versions of the questionnaire exist: a long and a short version. The long version of the questionnaire has been sent to vendors of certain device categories where the Internet research and the research via the MPA database did not provide the required information. A short version has been prepared as an alternative if vendors do not respond to the long version.

The following questions where part of the long version of the questionnaire (questions have been sent in German to the vendors; English translation is provided here for each question).

1. Hardware

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

English: 1.1 Does the device possess Ethernet interfaces? If yes, please provide data sheets.

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

English: 1.2 Does the device possess WLAN interfaces? If yes, please provide data sheets.

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

English: 1.3 Does the device possess Bluetooth interfaces? If yes, please provide data sheets.

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

English: 1.4 Does the device possess RFID or NFC interfaces? If yes, please provide data sheets.

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

English: 1.5 Does the device possess cellular communication modules (e.g. 2G, 3G, 4G)? If yes, please provide data sheets.

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

English: 1.6 Does the device possess USB interfaces? If yes, please provide data sheets.

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

English: 1.7 Does the device possess Thunderbolt interfaces? If yes, please provide data sheets.

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

English: 1.8 Does the device possess serial interfaces? If yes, please provide data sheets.

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

English: 1.9 Does the device possess display interfaces (e.g. VGA, HDMI, Display Port)? If yes, please provide data sheets.

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

English: 1.10 Does the device possess additional hardware interfaces (incl. other radio transmission interfaces)?

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

English: 1.11 Do the processors of the device possess any debugging interfaces (e.g. UART, JTAG, SPI)?

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

English: 1.12 Does the device possess a Trusted Platform Module (TPM)?

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

English: 1.13 Can external data storage be connected to the device and be used (e.g. external SD card, external USB storage)?

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

English: 1.14 Is a BIOS or UEFI firmware used within the product?

1.15 Kann das Produkt von externen Datenspeichern booten?

English: 1.15 Can the product boot from external data storages?

1.16 Kann das Basisprodukt durch zusätzliche Komponenten erweitert werden?

English: 1.16 Can the core roduct be extended with additional components?

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

English: 1.17 Which processors with which processor architectures (e.g. x86-64, ARM7, MIPS) are used? Please provide data sheets for the processors.

2. Software

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

English: 2.1 Which operating system (incl. version number) is used on the device (e.g. 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?

English: 2.2 Does the device use a web server that can be accessed with a browser over one of the interfaces listed in Section 1?

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?

English: 2.3 Does the device possess a remote-control service (e.g. telnet, SSH, RDP), which can be accessed with a tool over one of the interfaces listed in Section 1?

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?

English: 2.4 Does an external application exist (e.g. in the form of a mobile app) that can be used to communicate with or configure the device?

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

English: 2.5 Which programming languages are used for the development of software services of the product (e.g. C/C++, Java, Python)?

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

English: 2.6 Does an update mechanism exist for the software/firmware of the device? If yes, please provide details on this mechanism.

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?

English: 3.1 Does the device communicate with systems from a private/public 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)?

English: 3.2 Do external software solutions exists that have to be set up for the operation of the device and that are used to communicate with the device over one of the interfaces listed in Section 1 (e.g. an external web server component)?

3.3 Nutzt das Produkt unverschlüsselte Kommunikationskanäle?

English: 3.3 Does the device use unencrypted data channels?

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

English: 3.3. For encrypted data channels, which cryptographic methods are used?

4. Sonstiges (Miscellaneous)

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

English: 4.1 Which security standards (e.g. Common Criteria, Protection Profiles, norms) is the device compliant to?

4.2 Welche der folgenden Datentypen werden auf dem Produkt verarbeitet:

English: 4.2 Which of the following data types are processed on the device:

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

English: 4.2a Demographic data (e.g. name, address)

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

English: 4.2b Medical data (e.g. medical history, indication, imaging data)

4.2c Sonstige vom Benutzer eingegebene Daten

English: 4.2c Other data entered by the user

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

English: 4.3 Does the device possess an emergency function (“break-glass”) that can be used to obtain the data described under Section 4.2.

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

English: 4.4 In the past, did the product have any security vulnerabilities that have been publicly announced?

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

English: 4.5 Was the product part of a security assessment (e.g. penetration test) in the past, which was reported by the press?

The following questions where part of the short version of the questionnaire (questions have been sent in German to the vendors; English translation is provided here for each question).

1. Hardware

1.1 Besitzt das Produkt Ethernet-Schnittstellen?

English: 1.1 Does the device possess Ethernet interfaces?

1.2 Besitzt das Produkt WLAN-Schnittstellen?

English: 1.2 Does the device possess WLAN interfaces?

1.3 Besitzt das Produkt Bluetooth-Schnittstellen?

English 1.3: Does the device possess Bluetooth interfaces?

1.4 Besitzt das Produkt RFID bzw. NFC-Schnittstellen?

English 1.4: Does the device possess RFID or NFC interfaces?

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

English: 1.5 Does the device possess cellular communication modules (e.g. 2G, 3G, 4G)?

1.6 Besitzt das Produkt USB-Schnittstellen?

English: 1.6 Does the device possess USB interfaces?

1.7 Besitzt das Produkt Thunderbolt-Schnittstellen?

English: 1.7 Does the device possess Thunderbolt interfaces? If yes, please provide data sheets.

1.8 Besitzt das Produkt serielle Schnittstellen?

English: 1.8 Does the device possess serial interfaces?

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

English: 1.9 Does the device possess display interfaces (e.g. VGA, HDMI, Display Port)?

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

English: 1.10 Can external data storage be connected to the device and be used (e.g. external SD card, external USB storage)?

1.11 Kann das Basisprodukt durch zusätzliche Komponenten erweitert werden?

English: 1.11 Can the base product be extended with additional components?

2. Software

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

English: 2.1 Which operating system (incl. version number) is used on the device (e.g. 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?

English: 2.2 Does the device use a web server that can be accessed with a browser over one of the interfaces listed in Section 1?

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?

English: 2.3 Does the device possess a remote-control service (e.g. telnet, SSH, RDP), which can be accessed with a tool over one of the interfaces listed in Section 1?

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?

English: 2.4 Does an external application exist (e.g. in the form of a mobile app) that can be used to communicate with or configure the device?

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

English: 2.5 Which programming languages are used for the development of software services of the product (e.g. C/C++, Java, Python)?

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

English: 2.6 Does an update mechanism exist for the software/firmware of the device?

3. Kommunikationskanäle (Communication Channels)

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

English: 3.1 Does the device communicate with systems from a private/public 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)?

English: 3.2 Do external software solutions exists that have to be set up for the operation of the device and that are used to communicate with the device over one of the interfaces listed in Section 1 (e.g. an external web server component)?

4. Sonstiges (Miscellaneous)

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

English: 4.1 Which security standards (e.g. Common Criteria, Protection Profiles, norms) is the device compliant to?

4.2 Welche der folgenden Datentypen werden auf dem Produkt verarbeitet:

English: 4.2 Which of the following data types are processed on the device:

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

English: 4.2a Demographic data (e.g. name, address)

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

English: 4.2b Medical data (e.g. medical history, indication, imaging data)

4.2c Sonstige vom Benutzer eingegebene Daten

English: 4.2c Other data entered by the user

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

English: 4.3 Does the device possess an emergency function (“break-glass”) that can be used to obtain the data described under Section 4.2.

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

English: 4.4 In the past, did the product have any security vulnerabilities that have been publicly announced?

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

English: 4.5 Was the product part of a security assessment (e.g. penetration test) in the past, which was reported by the press?

Bibliography

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

Nachname, V. (2019). *Titel eingetragen.* Bonn als Ort: Verleger eingetragen.

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 ERNW Research GmbH: 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