DSI Industrial & Policy Recommendations (IPR) Series

Recommendations for safety and IT security in medical devices

Isabel Skierka (Digital Society Institute, ESMT Berlin)

Issue 6, 2017

The healthcare industry is undergoing great technological transformations. Hospitals are going digital and medical devices – whether implanted in patients' bodies or stationed in hospitals – are equipped with increasing computing power and wireless connectivity. Connected healthcare can offer safer, more efficient, and timely medical service delivery. It also presents great economic opportunities – according to a Roland Berger consultancy firm study, the digital healthcare market is set to grow at average annual growth rates of 21 percent until 2020 (Roland Berger 2016).

Yet, the integration of computing and communication technologies in safety-critical medical systems will expose them to the same network and information security (cybersecurity) threats as other information technology (IT) systems. Research and real-world incidents have shown that IT security risks in healthcare are systemic. Cyber attacks' impact on the privacy of patient data has already been established. More recently, their potential impact on patient health and safety has been raising concerns for healthcare organizations, regulators, and medical device manufacturers alike. The management and governance of related risks requires comprehensive standardization, regulation, and best practices to encompass both IT security and safety.

The below analysis of the convergence of safety and security risks in connected healthcare and recommendations for policy and industry are based on a review of the relevant literature, expert interviews, and a DSI workshop with representatives from health organizations, medical device manufacturers, IT security experts, safety engineers, regulators, and certification bodies.

1. Status

1.1 Cybersecurity incidents in medical devices

For over a decade, researchers have been warning that the level of cybersecurity in safety-critical medical devices is alarmingly low. On August 29, the US Food and Drug Administration (FDA) issued a recall for nearly half a million pacemakers made by Abbott Laboratories (US Food & Drug Administration 2017). The agency found that the devices could be hacked to control pacing or deplete the devices' batteries, with potentially fatal consequences. As a result, all patients whose lives depend on one of the affected pacemaker models, approximately 745,000 persons worldwide, had to visit their doctors to receive a firmware update that patches the security flaws.

Regular patching of cybersecurity vulnerabilities, a practice most people know only from their desktop IT systems, is on the way to becoming a common procedure in health care.

The Abbott pacemaker recall is just the latest in a series of incidents. While no single incident to date has been known to cause deaths by hacking into a pacemaker or insulin pump, several researchers have demonstrated that it is possible. In 2008, a team of researchers first demonstrated attacks against implantable cardiac defibrillators. With the help of a commercially available device programmer, the team was able to extract a patient's private data and reprogram the pacemaker to deny service (Halperin et al., 2008).

Since then, several have demonstrated different possibilities for hacking pacemakers and insulin pumps (Burleson et al., 2012; Marin et al., 2016; Li, Raghunathan, and Jha 2011; Radcliffe 2011). In May of this year, researchers from the security firm WhiteScope discovered a total of 8,665 open and known vulnerabilities in third-party software libraries implemented across four different pacemaker programmers from four different manufacturers (Rios and Butts 2017). This is a failure of enormous proportions.

Not only implantable but also stationary hospital devices are vulnerable to hacking. A 2014 report by the SANS Institute concluded that 94 percent of healthcare organizations have been the victim of a cyber attack, including attacks against medical devices and infrastructure (Filkins 2014). Other reports have shown how vulnerable medical devices served as conduits for hackers to attack hospital networks (Independent Security Evaluators 2016). The "WannaCry" ransomware worm, which compromised the networks of many global corporations earlier this year, also affected medical devices in hospitals and prompted the US Industrial Control System Computer Emergency Response Team (ICS-CERT) and several medical device vendors to issue security alerts about vulnerable devices (ICS-CERT 2017).

These examples and others show that cybersecurity risks in health care are systemic. Many medical devices lack even basic security features, and the resulting risks are externalized. Unfortunately, the parties most affected by the risk – the patients themselves – can do little to improve the security of the devices on which their own health depends.

1.2 Structural obstacles

A number of structural factors amplify cybersecurity threats to medical devices and complicate their protection. As medical devices are increasingly complex and interconnected, they need to be considered as larger systems, composed by different software and hardware components. Hence, security mechanisms need to be implemented across the system with its different layers. For example, some of the functionality of a medical device might lie outside the device, on a server. Moreover, security is contextual. A mobile device like a smart phone can perform critical functions if it is used in a medical context, for example for monitoring or diagnosis purposes. Therefore, securing medical systems requires coordination of responsibilities among manufacturers and operators of different system components.

Tradeoffs between security, safety, and other essential system requirements

Achieving a balance between medical systems' security goals and health care utility and safety is challenging. Most medical devices rely on embedded computer systems, which are constrained in their computation power, memory, and energy consumption. Security mechanisms can slow down their operation, reduce usable battery life and make devices less accessible in emergency situations. Moreover, generic security controls such as password access controls can hamper usability in fast paced clinical environments. Hence, security mechanisms need not only be secure, but also usable, efficient and compatible with the unique circumstances of these systems.

Related dilemmas have been subject to a growing corpus of research and suggestions for innovative encryption and authentication solutions. Yet, to date none of these have been found to be secure enough for implementation attacks (for an overview, see Marin et al., 2016).

Lifecycle conflicts

The life time of medical devices is much longer than the life time of software. A medical device's life time is between 10 and 30 years, which is much longer than the supported life time of most operating systems. As a result, software usually becomes outdated and unsupported over the course of a device's lifetime. As reuse of hardware and software systems in medical devices is common, a medical device is generally a mix of new and old legacy systems. Moreover, legacy systems may no longer be interoperable with newer systems. This leaves vulnerabilities such as misconfiguration and security holes. Medical devices running on the Microsoft Windows XP operating system, for example, no longer receive vital software updates (unless hospitals or manufacturers pay a high fee to Microsoft) – an issue which became dramatically visible during the spread of the WannaCry ransomware worm.

Lack of (timely) security patches

Once a vulnerability is known, devices need to receive timely software security updates. Yet, patching medical devices is much more complicated than patching IT desktop systems (see Bellovin 2017; Brook 2017; Nunnikoven 2017). Patches bear security risks if they interact with the use environment in an unforeseen way or render systems unavailable. Not only must software updates fix security flaws in a particular software system, they must also ensure that they do not cause any unintended effects and incompatibilities concerning other soft- and hardware in the system, including aforementioned legacy systems. Moreover, if software updates are not securely deployed, they can also be manipu-

lated to channel malicious software into systems. Finally, responsibilities for update deployment and installation are not always clear. Hospitals and other medical device users are often dependent on vendors to deploy patches and lose liability claims in case they upgrade or change devices' software independently. Device original equipment manufacturers (OEMs) in turn do not always have access to the software implemented in their devices and are dependent on software suppliers or integrators themselves.

Proprietary and opaque software

Most medical devices rely on proprietary software. Original equipment manufacturers (OEMs) do not have full access to it. Moreover, manufacturers and suppliers are rarely transparent regarding third party software components in their products. Hence, validating the software becomes a difficult task. In testing terms, OEMs must treat software as a 'black box'. Where software vendors make the software accessible to OEMs or to testing and certification labs, some security risks, such as known vulnerabilities or code errors, can be mitigated.

Divergence of safety and security risk assessments

Risk assessment and testing methods for safety and security of control systems have evolved separately over time. Safety mechanisms are mainly concerned with unintentional/non-malicious threats caused by natural disasters, technical failures or human failure. Security mechanisms additionally address intentional/malicious threats caused by intentional human behavior, for example by hackers. When it comes to attacks, security is a function of a threat agent and its capabilities, intent, and motivation. These are dynamic and constantly evolving. Therefore, security risks cannot be addressed by static risk assessment and management methods, such as functional testing for the presence or absence of specified behavior as well as static risk and failure rate calculation methods. Attacks on security often exploit the existence of unspecified behavior and are found after the software has been released and is in use in larger systems (Bryans 2017). As a result, the security risks need to be managed by the manufacturer after a device has already been marketed. This includes the continuous testing of software for vulnerabilities and the provision of software updates. As control systems in medical devices can be affected by cyber attacks, it is increasingly important to address the combination of safety and security in such modern control systems.

1.3 Standards lag behind

Medical device safety is strictly regulated in Europe and in other countries. Yet, regulation and standards are catching up with digital innovation and have so far insufficiently addressed cybersecurity. Hence, regulators and standardization bodies need to update and extend existing frameworks beyond safety requirements to security.

Political bodies in the US and more recently in Europe have started to take action. So far, the FDA has assumed a leading role in this field. It has issued two sets of guidelines for cybersecurity in medical devices, a pre-market guidance in October 2014 (US Food & Drug Administration 2014), and a post-market guidance in December 2016 (US Food & Drug Administration 2016). They are intended to support manufacturers in fulfilling the requirements of the pre-market approval and post-market monitoring processes with respect to cybersecurity risks throughout a product's entire lifecycle.

However, implementation remains poor. A study by the Ponemon Institute found that only 51 percent of surveyed device makers follow the FDA's guidance to mitigate or reduce inherent security risks in medical devices, and only 44 percent of health organizations follow the guidance (Ponemon Institute 2017). The FDA's enforcement mechanisms, such as the issuance of recalls and safety notices, as well as liability for device failure and reputational damage will raise the cost of bad security for manufacturers.

The European Union (EU) and national oversight bodies in Europe have offered little guidance as to how medical IT security practices and mechanisms should look like, raising the specter of an uneven regulatory patchwork across the continent. Currently, moderate to high-risk medical devices' conformity with safety and performance regulatory requirements are evaluated by certification bodies (so-called 'notified bodies', which are accredited private companies) and overseen by national authorities. If they conform with the requirements, they obtain a CE (Communauté Européenne) label and can be marketed in the entire EU. In May 2017, the EU adopted a new Medical Device Regulation (MDR), which for the first time specifically requires manufacturers to develop devices in accordance with "state of the art" IT security requirements. But the regulation offers little guidance as to how the practices and mechanisms to be followed by manufacturers should look like. This is a problem because standards that combine or complement established criteria for the functional safety of medical devices with appropriate IT security requirements do not yet exist—so there is no established definition of what "state of the art" means for the IT security of medical devices.

Therefore, manufacturers and certification bodies that evaluate devices for their safety are left to define their own medical IT security certification and evaluation frameworks. This creates a risk that cybersecurity standards in health care are fragmenting across Europe and even within EU member states.

Apart from medical device regulation, regulatory frameworks for critical infrastructure security and data protection play important roles for cybersecurity in health care. The European Network and Information Security (NIS) Directive, which has to be implemented in European member states by May 2018, requires operators of essential services, including hospitals, to implement minimum IT security standards and to notify of security breaches. The EU General Data Protection Regulation, which EU member states also have to implement by May 2018, will also apply to software and medical device vendors, as well as to health organizations and makes security and privacy by design and default mandatory.

2. Recommendations

2.1 Policy recommendations

Common medical IT security certification standards

Public authorities, in cooperation with manufacturers and certification bodies, should develop concrete common European IT security criteria as a component of the medical device certification process. The European Commission has recently proposed an EU-wide cybersecurity certification framework that could serve as a basis for the certification of security properties of medical products and processes (European Commission 2017). Within the framework, medical-device-specific schemes and security requirements could serve as a basis for evaluation, testing, and certification of cybersecurity along with other medical system requirements. Such schemes should be harmonized with other international standards as much as possible with the goal of creating internationally applicable schemes that also lower device vendors' transaction costs.

Other guidance can be deduced from international standards for the secure design and development of software components, FDA guidelines, and existing guidelines on Industrial Control Systems (ICS) security. ICS properties are in fact similar to those of medical devices since both are systems in which embedded computers control physical devices' interactions with their environments. Hence, the measures used to secure embedded computer systems in ICS are equally applicable in the healthcare context. Examples for guidance documents include the international draft IEC 62443 standard series on industrial network and system security, the US National Institute of Standards and Technology's (NIST) ICS Security Guide (NIST 2015), and the proposed European cybersecurity certification framework for industrial automated control system components (European Commission 2016).

Promoting transparency of IT security risks and incidents

European and national medical oversight agencies should make information about IT security risks and incidents in medical devices publicly available. At present, national authorities need to submit information about safety incidents to the European Database on Medical Devices (EUDAMED), which is only accessible by EU institutions and national authorities. Per the MDR, most information submitted to EUDAMED will be public in the future.

Information about software vulnerabilities concerning medical devices should also be made accessible to all stakeholders. The Common Vulnerability Scoring System (CVSS) is useful in assessing the information security risk of a vulnerability (in terms of impact on confidentiality, integrity, availability). In order to capture vulnerabilities' impacts on systems' safety and not only on their security, the CVSS or other vulnerability assessment systems should be adapted to the safety context. The MITRE Corporation and the FDA have formed a working group, including medical device manufacturers, healthcare providers, and cybersecurity experts, to develop an approach for using CVSS to score medical device vulnerabilities (Carmody and Zuk 2017).

Information sharing

European and national decision-makers should incentivize information sharing about security threats in the health care sector. Currently, information sharing is fragmented. Safety incidents are reported to national authorities and collected in the Eudamed database. Healthcare organizations classified as "operators of essential services" under the EU NIS Directive will need

to report major security incidents to national information security authorities which differ from the medical CAs. EU institutions and national authorities as well as industry should set up an information sharing system that supersedes these fragmentations and ensures a better sharing of threat information within the healthcare sector. It should additionally promote the exchange of threat information with other sectors. Information sharing networks can be overseen by an Information Sharing and Analysis Center (ISAC), a sectoral coordinating Computer Emergency Response Team (CERT), or national CERTs. In the US, for example, a National Health Information Sharing & Analysis Center (NH-ISAC) provides threat information and exchange services.

2.2 Recommendations for manufacturers and suppliers

Health care is a critical infrastructure. Hospitals, as critical infrastructure operators, and other medical device users are responsible for securely operating medical devices within their networks. As mentioned previously, they are regulated under the EU NIS Directive and the GDPR. The standard IEC 80001 offers guidance on the application of risk management for IT networks incorporating medical devices for health organizations. Within their organizations, hospitals should integrate the management of medical devices, which has traditionally been the task of biomedical technicians, and networks, which has traditionally been under the auspices of the IT department.

The ultimate responsibility for medical device safety lies with their manufacturers. Per EU liability law, original equipment manufacturers (OEMs) are held liable for harm caused by a defective product. In order to mitigate cybersecurity risks as far as possible, manufacturers should implement a number of security related pre-market practices (before the device is marketed) and post-market management mechanisms for monitoring, vulnerability handling, and information sharing.

Several medical device makers have adopted effective processes to implement cybersecurity in devices throughout their life cycle, including responsible patch management and disclosure programs (Draeger 2017; Siemens Healthineers 2017). These can serve as examples in the industry.

Security by design

IT security should not be an afterthought, rather it should be designed into the devices from the start. The design of medical devices should follow proven secure lifecycle standards and secure supply chain management practices. All off-the-shelf hard- and software integrated into devices should be trustworthy and provide high technological assurance. Manufacturers should reduce devices' connectivity to the necessary minimum, and isolate safety critical system components from other potentially vulnerable components within the devices.

Integrated safety and security risk assessment

Manufacturers as well as notified certification bodies should apply integrated safety and security risk assessment and management methods to medical devices. Research in this field has presented a number of integrated risk assessment methods for (industrial) control systems that can complement established medical device risk management standards, for example the SAHARA or Unified Security and Safety Risk Assessment Methods (Chockalignam et al., 2016). The aforementioned FDA pre-market cybersecurity guidelines as well as the IEC 62433 standard offer additional guidance in this field.

Transparency about device security and risks

Device manufacturers and vendors should transparently declare how their devices fulfill medical IT security requirements. The manual for devices should not only include directions for their use, but also a threat model of the device in use contexts to clearly demonstrate the risks of the device's use. This would give device operators and users the necessary information about security trade-offs and the ability to decide about related risks.

Software and hardware suppliers should be equally transparent and explain the security mechanisms and threat models of their software and the effects of its use in a device.

Patch management

Manufacturers should operate an effective and usable patch management system. Once a vulnerability is known, devices need to receive timely software security updates. Since software updates themselves bear security risks, they should be tested in use environments before being deployed. Moreover, device makers

need to implement secure channels for the deployment of updates in order to prevent their manipulation.

Vulnerability reporting

Manufacturers should operate a vulnerability reporting program through which they collaborate with third parties who discover software security flaws. Many medical device manufacturers, including Siemens, Draeger, Medtronic, and Philips, have implemented coordinated vulnerability disclosure programs throughout the past years (I am the Cavalry 2017). These developments are encouraging. Standards ISO/IEC 29147: Information Technology – Security Techniques – Vulnerability disclosure and ISO/IEC 30111:2013 Information Technology – Security Techniques – Vulnerability handling processes provide guidelines for manufacturers and their adoption should be promoted by public institutions.

3. References

Bellovin, S.M. (2017). Patching is hard. SMBlog. https://www.cs.columbia.edu/~smb/blog/2017-05/2017-05-12.html (accessed October 30, 2017).

Brook, C. (2017). Patches pending for medical devices hit by WannaCry. Threatpost, May 18. https://threatpost.com/patches-pending-for-medical-devices-hit-by-wannacry/125758/ (accessed October 30, 2017).

Bryans, J. W. (2017). The internet of automotive things: Vulnerabilities, risks and policy implications. *Journal of Cyber Policy* 2 (2): 185-194.

Burleson, W., S. Clark, B. Ransford, and K. Fu. (2012). Design challenges for secure implantable medical devices. *DAC*, June 3-7, San Francisco, California, USA.

Carmody, S. and M. Zuk. (2017). The evolving state of medical device cybersecurity. *HIMSS Annual Conference, Feb 19-23.* http://www.himssconference.org/sites/himssconference/files/pdf/16FINAL.pdf (accessed October 30, 2017)

Chockalingam, S., D. Hadžoismanović, W. Pieters, A. Teixera, and P. van Gelder. (2016). Integrated safety and security risk assessment methods: A survey of key characteristics and applications. *The 11th International Conference on Critical Infrastructure Security*.

Draeger (2017). Cybersecurity. https://www.draeger.com/en_uk/Hospital/Insights-to-Solutions/Cybersecurity (accessed December 7, 2017).

European Commission. (2016). Introduction to the European IACS components Cybersecurity Certification Framework (ICCF). https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf (accessed October 30, 2017).

European Commission. (2017). COM(2017) 477 final. The EU cybersecurity certification framework. *Proposal for a Regulation of the European Parliament and of the Council*. https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework (accessed October 30, 2017).

Filkins, B. (2014). Healthcare cyberthreat report: Widespread compromises detected, compliance nightmare on the horizon. *SANS Institute InfoSec Reading Room*. https://www.sans.org/reading-room/whitepapers/analyst/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735 (accessed October 30, 2017).

Fox-Brewster, T. (2017). Medical devices hit by ransomware for the first time In US hospitals. *Forbes*, May 17. http://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/ (accessed October 30, 2017).

Halperin, D.,Heydt-Benjamin, B. Ransford, S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno and W. Maisel. (2008). Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero Power Defenses. *IEEE Symposium on Security and Privacy*.

I Am The Cavalry (2017). An overview of vulnerability disclosure programs. https://www.iamthecavalry.org/resources/disclosure-programs/ (accessed December 7, 2017).

ICS-CERT (2017). Indicators associated with WannaCry ransomware (Update I). May 15. https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-135-01I (accessed October 30, 2017).

Independent Security Evaluators. (2016). Hacking hospitals. February 23. https://www.securityevaluators.com/hospitalhack/securing_hospitals.pdf (accessed October 30, 2017).

Johnson, C. (2012). CyberSafety: On the interactions between cybersecurity and the software engineering of safety-critical systems. In *Achieving system safety*, ed. C. Dale and T. Anderson. London: Springer Verlag.

Leverett, E., R. Clayton, and R. Anderson. (2017). Standardisation and certification in the 'Internet of Things'. *16th Annual Workshop on the Economics of Information Security (WEIS)*. http://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/05/WEIS_2017_paper_23.pdf (accessed October 30, 2017).

Li, C., A. Raghunathan, and N. K. Jha. (2011). Hijacking an insulin pump: Security attacks and defences for a diabetes therapy system. *Proceedings of the 13th IEEE International Conference on e-Health Networking, Applications, and Services, Healthcom '11.*

Marin E., D. Singelée, F. D. Garcia, T. Chothia, R. Willems, and B. Preneel. (2016). On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them. *ACSAC '16 Proceedings of the 32nd Annual Conference on Computer Security Applications: 226-236.* https://www.esat.kuleuven.be/cosic/publications/article-2678.pdf (accessed 30 September, 2017).

National Institute for Standards and Technology (2015). SP 800-82, Revision 2. Guide to industrial control systems (ICS) security.

Nunnikhoven, M. (2017). WannaCry & the reality of patching, 14 May. Retrieved from http://blog.trendmicro.com/wannacry-reality-of-patching/ (accessed October 30, 2017).

Ponemon Institute. (2017). Medical device security: An industry under attack and unprepared to defend. https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/medical-device-security-ponemon-synopsys.pdf (accessed October 30, 2017).

Radcliffe, J. (2011). Hacking medical devices for fun and insulin: Breaking the human SCADA system. *Black Hat Conference 2011.*

Rios, B. and J. Butts. (2017). Security evaluation of the implantable cardiac device ecosystem and architecture and implementation interdependencies. *WhiteScope Security Report,* May 17. https://drive.google.com/file/d/0B_GspGER4QQTYkJfaVlBeGVCSW8/view (accessed August 31, 2017).

Roland Berger Consultants (2016). Digital healthcare market to average 21 percent growth per year through 2020. September 28. https://www.roland-berger.com/en/press/Digital-health-market-to-average-21-percent-growth-per-year-through-2020.html (accessed October 30, 2017).

Siemens Healthineers (2017). Cybersecurity at Siemens Healthineers. https://www.healthcare.siemens.com/medical-imaging-it/cybersecurity (accessed December 7, 2017).

US Food & Drug Administration (2014). Content of premarket submissions for management of cybersecurity in medical devices. Guidance for industry and Food and Drug Administration staff. https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf (accessed October 30, 2017).

US Food & Drug Administration (2016). Postmarket management of cybersecurity in medical devices. Guidance for industry and Food and Drug Administration staff. https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf (accessed October 30, 2017).

US Food & Drug Administration (2017). Firmware update to address cybersecurity vulnerabilities identified in Abbott's (formerly St. Jude Medical's) implantable cardiac pacemakers. *FDA Safety Communication,* August 29. https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm (accessed August 31, 2017).

The DSI Industrial & Policy Recommendations (IPR) Series is published by the Digital Society Institute of ESMT Berlin, http://dsi.esmt.org.

DSI Industrial & Policy Recommendations (IPR) Series

Empfehlungen zur Cybersicherheit von Medizingeräten

Isabel Skierka (Digital Society Institute, ESMT Berlin)

Ausgabe 6, 2017

Die Gesundheitsversorgung durchläuft einen digitalen Wandel. Medizingeräte - ob im Körper der Patienten implantiert oder in Krankenhäusern stationiert – und ganze Krankenhäuser sind immer ‚smarter' vernetzt, Arbeitsprozesse laufen fast ausschließlich sofware-basiert ab. Die vernetzte Medizin kann eine sicherere, effizientere und schnellere Versorgung bieten. Auch die wirtschaftlichen Wachstumschancen der Gesundheitsbranche steigen. Laut einer Studie der Unternehmensberatung Roland Berger (2016) soll der digitale Gesundheitsmarkt bis 2020 durchschnittlich um 21 Prozent pro Jahr wachsen.

Die Integration von Computer- und Kommunikationstechnologien in sicherheitskritische medizinische Systeme birgt jedoch auch Cybersicherheitsrisiken. Die Ergebnisse mehrerer IT-Sicherheitsstudien und auch reale Vorfälle haben über die vergangenen Jahre hinweg verdeutlicht, dass Cybersicherheitsrisiken in der Gesundheitsversorgungen mittlerweile systemisch sind. Nicht nur die Auswirkung von Cyber-Angriffen auf die Privatsphäre von Patientendaten, sondern auch auf Leib und Leben der Patienten bereitet Gesundheitsorganisationen, Regulierungsbehörden und Herstellern von Medizinprodukten Kopfzerbrechen. Wie dieses Papier zeigt, erfordert der Umgang der damit verbundenen Risiken umfassende Standardisierung, Regulierung und Best Practices, die sowohl Safety- als auch IT-Sicherheitsmechanismen umfassen.

Die nachfolgende Analyse und Empfehlungen basieren auf einer Literaturanalyse, Experteninterviews und den Ergebnissen eines DSI Workshops am 18.10.2017 in Berlin, an dem Vertreter von Gesundheitsorganisationen, Medizinprodukteherstellern, IT-Sicherheitsexperten, Konformitätsbewertungsstellen und Regulierungsbehörden teilnahmen.

1. Ausgangslage

1.1 Cybersicherheits-Vorfälle in Medizingeräten

Seit etwa einem Jahrzehnt warnen Forscher vor gravierenden Cybersicherheits-Mängeln in Medizingeräten. Am 29. August 2017 leitete die US-amerikanische Arzneimittelbehörde Food and Drug Administration (FDA) zuletzt einen Rückruf von knapp einer halben Million Herzschrittmacher des Herstellers Abbott Laboratories ein (US Food & Drug Administra-tion 2017). Der Behörde lagen Ergebnisse vor, nach denen Hacker sich durch Sicherheitslücken im Schrittmacher lebensbedrohlichen Zugriff auf die Funktionen des Geräts hätten verschaffen können. Unter Ausnutzung der Schwachstelle hätte ein Angreifer so die Frequenz der Impulse kontrollieren oder die Batterie des Geräts erschöpfen und damit den Stillstand des Schrittmachers einleiten können. Die potentiellen Folgen wären fatal. Infolge des Rückrufs mussten alle Patienten, die eines der betroffenen Herzschrittmacher-Modelle im Körper tragen, ihre Ärzte aufsuchen um ein Firmware-Update zur Behebung der Sicherheitsmängel zu erhalten. Weltweit sind etwa 745.000 Menschen betroffen.

Das regelmäßige Patchen von Cybersicherheitslücken kennen die meisten Menschen nur von ihren Desktop IT-Systemen. Doch in Zukunft wird auch das regelmäßige Patching von Medizingeräten, Autos oder Haushaltsgeräten zur Gewohnheit werden.

Der Abbott-Herzschrittmacher-Rückruf ist nur der jüngste aus einer Reihe von Vorfällen. Obwohl

bisher kein einziger bekannter Sicherheitsvorfall in einem Herzschrittmacher oder einer Insulinpumpe einen Todesfall verursacht hat, haben mehrere Forscher gezeigt, dass dies möglich ist. Im Jahr 2008 demonstrierte ein Forscherteam erstmals Angriffe auf implantierbare Herz-Defibrillatoren. Mit Hilfe eines kommerziell erhältlichen Geräteprogrammierers war es dem Team möglich, die privaten Daten eines Patienten zu extrahieren und den Herzschrittmacher so umzuprogrammieren, dass er den Dienst verweigerte (Halperin et al., 2008).

Seitdem haben mehrere Forscher und IT-Sicherheitsexperten verschiedene Möglichkeiten für das Hacken von Herzschrittmachern und Insulinpumpen aufgezeigt (Burleson et al., 2012; Li, Raghunathan und Jha 2011; Marin et al., 2016; Radcliffe 2011). Im Mai 2017 entdeckten Forscher des Sicherheitsunternehmens WhiteScope insgesamt 8.665 offene und bekannte Schwachstellen in Software-Bibliotheken von Drittanbietern, die über vier verschiedene Schrittmacher-Programmierer von vier verschiedenen Herstellern implementiert wurden (Rios und Butts 2017). Diese Software-Bibliotheken lassen sich meist nicht mehr im implantierten Gerät updaten. Das ist ein Designfehler extremen Ausmaßes.

Nicht nur implantierbare sondern auch stationäre Geräte im Krankenhaus sind anfällig für Hacker-Angriffe. Ein Bericht des SANS-Instituts aus dem Jahr 2014 kommt zu dem Schluss, dass 94 Prozent aller Gesundheitsorganisationen in den USA Opfer eines Cyber-Angriffs geworden sind, betroffen waren auch medizinische Geräte und Infrastrukturen (Filkins 2014). Andere Berichte zeigen, wie Hacker verwundbare Medizingeräte gezielt als Einfallstore in Krankenhausnetzwerke nutzen um sensible Daten zu erbeuten (Independent Security Evaluators 2016). Der Ransomware-Wurm „WannaCry“, welcher im Mai 2017 die Netzwerke vieler global agierender Konzerne infizierte, befiel auch zahlreiche Medizingeräte in Krankenhäusern. Der Vorfall veranlasste das US Industrial Control System Computer Emergency Response Team (ICS-CERT) und mehrere Hersteller medizinischer Geräte, Sicherheitswarnungen über gefährdete Geräte zu veröffentlichen (ICS-CERT 2017).

Diese und andere Beispiele zeigen, dass Cybersicherheitsrisiken im Gesundheitswesen systemisch sind. Vielen Medizinprodukten fehlen sogar grundlegende Sicherheitseigenschaften. Die daraus resultierenden Risiken werden externalisiert. Leider können die am stärksten betroffenen Parteien - die Patienten selbst - wenig tun, um die Sicherheit der Geräte, von denen ihre eigene Gesundheit abhängt, zu verbessern.

1.2 Strukturelle Hürden

Eine Reihe von strukturellen Faktoren verstärken die Cybersicherheitsgefahren für Medizingeräte und erschweren deren Schutz. Da Medizinprodukte immer komplexer und vernetzter werden, müssen sie als Systeme betrachtet werden, die sich aus verschiedenen Soft- und Hardwarekomponenten zusammensetzen. Daher müssen Sicherheitsmechanismen systemübergreifend innerhalb der verschiedenen Ebenen implementiert werden. Beispielsweise könnte ein Teil der Funktionalität eines Medizinprodukts außerhalb des Geräts auf einem Server liegen. Darüber hinaus ist Sicherheit kontextabhängig. Ein mobiles Endgerät wie ein Smartphone kann kritische Funktionen übernehmen, wenn es im medizinischen Kontext, das heißt zu Überwachungs- oder Diagnosezwecken, eingesetzt wird. Die Absicherung medizinischer Systeme erfordert daher eine Koordination der Verantwortlichkeiten zwischen Herstellern und Betreibern verschiedener Systemkomponenten.

Kompromisse zwischen „Safety“, Cybersicherheit und anderen grundlegenden Systemanforderungen

Die Sicherung von Medizingeräten gegen Cyber-Angriffe oder -vorfälle ist nicht trivial. Geräte müssen mehrere, nicht immer kompatible Systemanforderungen erfüllen, wobei Cybersicherheit nur eine ist. Vor allem müssen Geräte in ihrer Einsatzumgebung – dem menschlichen Körper oder auf einer Krankenhausstation – uneingeschränkt wie intendiert funktionieren um Leib und Leben des Patienten zu schützen („Safety“). Die meisten medizinischen Geräte sind auf eingebettete Computersysteme angewiesen, die in ihrer Rechenleistung, ihrem Speicher und ihrem Energieverbrauch eingeschränkt sind. Cybersicherheitsmechanismen wie Verschlüsselungs- oder Authentifizierungsmaßnahmen können den Betrieb verlangsamen, die Batterielaufzeit verkürzen oder Geräte in Notsituationen unzugänglich machen. Darüber hinaus können generische Sicherheitskontrollen wie Passwort-Zugriffskontrollen die Benutzerfreundlichkeit in schnelllebigen klinischen Umgebungen beeinträchtigen. Daher müssen Sicherheitsmechanismen nicht nur sicher, sondern auch nutzbar, effizient und mit den einzigartigen Gegebenheiten dieser Systeme kompatibel sein.

Die damit verbundenen Dilemmata sind Gegenstand einer zunehmenden Anzahl von Forschungsarbeiten und Vorschlägen für innovative Verschlüsselungs- und Authentifizierungslösungen. Bislang hat sich jedoch keines dieser Systeme als sicher genug gegen spezialisierte Angriffe erwiesen (für einen Überblick siehe Marin et al., 2016).

Lebenszykluskonflikte

Die Lebensdauer von Medizingeräten (etwa 10 bis 30 Jahre) ist länger als die unterstützte Lebensdauer der meisten Betriebssysteme und Anwendungssoftware. Diese Diskrepanz führt dazu, dass Software im Laufe der Lebensdauer eines Geräts in der Regel veraltet und nicht mehr unterstützt wird. Da die Wiederverwendung von Hard- und Softwaresystemen in medizinischen Geräten weit verbreitet ist, ist ein Medizinprodukt in der Regel eine Mischung aus neuen und alten Systemen („legacy Systeme"). Außerdem ist es möglich, dass „legacy" Systeme nicht mehr mit neueren Systemen interoperabel sind. Dadurch entstehen Schwachstellen wie Fehlkonfigurationen und Sicherheitslücken. Medizinische Geräte, die auf dem veralteten Betriebssystem Microsoft Windows XP laufen, erhalten beispielsweise keine Software-Updates mehr (es sei denn, Nutzer zahlen eine hohe Gebühr an den Hersteller Microsoft). Während der Verbreitung des WannaCry-Wurms, der eine Schwachstelle in Windows-Betriebssystemen ausnutzte, wurden die Konsequenzen fehlender Sicherheits-Updates deutlich.

Verzögerte oder fehlende Sicherheits-Updates

Sobald eine Schwachstelle bekannt ist, muss die Software in betroffenen Geräten rechtzeitig ein Sicherheitsupdate erhalten. Doch das „Patchen" von medizinischen Geräten ist viel komplizierter als von IT-Desktop-Systemen (siehe Bellovin 2017; Brook 2017; Nunnikoven 2017). Patches selbst bergen Sicherheitsrisiken, wenn sie auf unvorhergesehene Weise mit der Nutzungsumgebung interagieren oder die Verfügbarkeit von Systemen beeinträchtigen. Software-Updates müssen nicht nur Sicherheitsmängel in einem bestimmten Softwaresystem beheben, sie müssen auch sicherstellen, dass sie keine unbeabsichtigten Auswirkungen und Inkompatibilitäten in Bezug auf andere Soft- und Hardware im System, einschließlich der oben genannten „legacy" Systeme, verursachen. Darüber hinaus können Software-Updates, wenn sie nicht auf einem sicheren Weg bereitgestellt werden (auf einem gesicherten Server verfügbar, signiert, sicher an das Gerät übertragen), auch manipuliert werden, um schädliche Software in Systeme zu leiten. Außerdem sind die Verantwortlichkeiten für die Bereitstellung und Installation von Updates nicht immer deutlich. Krankenhäuser und andere Anwender medizinischer Geräte sind oft darauf angewiesen, dass die Hersteller Patches bereitstellen und verlieren Haftungsansprüche, falls sie selbstständig Änderungen an der Gerätesoftware vornehmen. Gerätehersteller wiederum haben nicht immer Zugriff auf die in ihren Geräten implementierte Software und sind von Software-Lieferanten oder Integratoren abhängig.

Proprietäre und undurchsichtige Software

Die meisten medizinischen Geräte sind auf proprietäre Software angewiesen. Auch Gerätehersteller haben oft keinen uneingeschränkten Zugriff auf die Software. Darüber hinaus sind Hersteller und Zulieferer selten transparent, was Softwarekomponenten von Drittanbietern in ihren Produkten betrifft. Die Validierung der Software ist daher eine schwierige Aufgabe. In Bezug auf das Testen müssen Konformitätsstellen und Hersteller Software oft als eine "Black Box" betrachten. Um Sicherheitsrisiken zu minimieren, müssen Softwareanbieter die Software Herstellern und Test- und Zertifizierungslaboren transparent zugänglich machen.

Divergenzen bei der Bewertung von Sicherheitsrisiken

Risikobewertungs- und Testmethoden für die „Safety" (funktionale Sicherheit) und Cybersicherheit von Kontrollsystemen haben sich im Laufe der Zeit separat entwickelt. „Safety"-Mechanismen befassen sich hauptsächlich mit unbeabsichtigten/nicht schädlichen Bedrohungen, die durch Naturkatastrophen, technische Ausfälle oder menschliches Versagen verursacht werden.

IT-Sicherheitsmechanismen adressieren zusätzlich vorsätzliche Bedrohungshandlungen. Das Ausmaß der Bedrohung hängt vom Bedrohungsakteur und seinen Fähigkeiten, Absichten und seiner Motivation ab. Cyberbedrohungen sind dynamisch und entwickeln sich ständig weiter. Daher können IT-Sicherheitsrisiken nicht durch statische Risikobewertungs- und -management-Methoden, wie zum Beispiel Funktionstests auf das Vorhandensein oder Nichtvorhandensein von spezifiziertem Verhalten sowie statische Risiko- und Ausfallratenberechnungsmethoden, bekämpft werden. Angriffe auf die Sicherheit nutzen oft die Existenz von unspezifiziertem Verhalten aus und werden erst gefunden, nachdem die Software veröffentlicht wurde und in größeren Systemen im Einsatz ist (Bryans 2017). Daher müssen die Sicherheitsrisiken vom Hersteller gemanagt werden, nachdem ein Gerät in Verkehr gebracht wurde. Dazu gehört das kontinuierliche Testen von Software auf Schwachstellen und die Bereitstellung von Software-Updates. Da Kontrollsysteme in Medizinprodukten von Cyber-Attacken betroffen sein können, wird es immer wichtiger, die Kombination von „Safety" und IT-Sicherheit zu berücksichtigen.

1.3 Regulierung und Standards hinken hinterher

Die „Safety“ von Medizinprodukten ist in Europa und in anderen Ländern strikt reguliert. Dennoch sind viele gesetzliche Regeln und Standards von der digitalen Innovation überholt. Daher müssen Regulierungsbehörden und Normungsgremien die bestehenden Rahmenbedingungen über die „Safety“-anforderungen hinaus aktualisieren und auf die IT-Sicherheit ausweiten.

Politische Gremien in den USA und in jüngster Zeit auch in Europa haben begonnen Cybersicherheit aktiv anzugehen. Die amerikanische FDA hat in diesem Bereich eine führende Rolle übernommen. Sie hat zwei Richtlinien für die Cybersicherheit von Medizinprodukten herausgegeben, eine Pre-Market Guidance im Oktober 2014 (US Food & Drug Administration 2014) und eine Post-Market Guidance im Dezember 2016 (US Food & Drug Administration 2016). Sie sollen die Hersteller dabei unterstützen, die Anforderungen der Zulassungs- und Post-Market-Überwachungs-Prozesse im Hinblick auf Cybersicherheitsrisiken über den gesamten Lebenszyklus eines Produkts zu erfüllen.

Die Umsetzung scheint jedoch mangelhaft. Eine Studie des Ponemon-Instituts ergab, dass nur 51 Prozent der befragten Gerätehersteller den Richtlinien der FDA folgen, um inhärente Cybersicherheitsrisiken in Medizinprodukten zu mindern oder zu reduzieren und nur 44 Prozent der Gesundheitsorganisationen den Richtlinien folgen (Ponemon Institute 2017). Die Durchsetzungsmechanismen der FDA, wie zum Beispiel die Einleitung von Rückrufen und Veröffentlichung von Sicherheitshinweisen, sowie die Haftung für Geräteausfälle und Reputationsschäden werden zukünftig die Kosten für mangelnde Cybersicherheit für die Hersteller erhöhen.

Die Europäische Union (EU) und die nationalen Aufsichtsbehörden in Europa haben bisher wenige Hinweise für die Implementierung von Cybersicherheitsmechanismen in Medizingeräten gegeben. Ohne einheitliche europäische Standards droht ein Flickenteppich von unterschiedlichen Prüfmaßnahmen und Sicherheitsniveaus von Geräten diesem Bereich. Derzeit wird die Konformität von Medizinprodukten mittlerer bis hoher Risiken mit den sicherheits- und leistungsrechtlichen Anforderungen von Konformitätsbewertungsstellen (sogenannte "Benannte Stellen", die akkreditierte Privatunternehmen sind) bewertet und von nationalen Behörden überwacht. Wenn sie den Anforderungen entsprechen, erhalten sie ein CE-Zeichen (Communauté Européenne) und können in der gesamten EU vermarktet werden. Im Mai 2017 verabschiedete die EU eine neue Medizinprodukteverordnung (MDR), welche die Hersteller erstmals ausdrücklich dazu verpflichtet, Geräte nach dem „Stand der Technik“ der IT-Sicherheitsanforderungen zu entwickeln. Die Verordnung bietet jedoch wenig Anhaltspunkte dafür, wie die von den Herstellern zu befolgenden Praktiken und Mechanismen aussehen sollten. Denn Standards, die etablierte Kriterien für die funktionale Sicherheit (Safety) von Medizinprodukten mit entsprechenden IT-Sicherheitsanforderungen kombinieren oder ergänzen, gibt es noch nicht - und so gibt es auch keine etablierte Definition dafür, was der „Stand der Technik“ für die IT-Sicherheit von Medizinprodukten bedeutet.

Hersteller und Konformitätsbewertungsstellen, die Geräte auf ihre Sicherheit überprüfen, müssen daher ihre eigenen Zertifizierungs- und Bewertungsrahmen für die medizinische IT-Sicherheit definieren. Dies birgt die Gefahr, dass die Cybersicherheitsstandards im Gesundheitswesen in ganz Europa und sogar innerhalb der EU-Mitgliedsstaaten immer weiter auseinanderbrechen.

Neben der Regulierung von Medizinprodukten spielen regulatorische Rahmenbedingungen für die Sicherheit kritischer Infrastrukturen und den Datenschutz eine wichtige Rolle für die Cybersicherheit im Gesundheitswesen. Die europäische Richtlinie zur Netzwerk- und Informationssicherheit (NIS-Richtlinie), die in den europäischen Mitgliedstaaten bis Mai 2018 umgesetzt werden muss, verpflichtet Betreiber kritischer Infrastrukturen, darunter Krankenhäuser, zur Umsetzung von IT-Mindeststandards und zur Meldung von Sicherheitsverletzungen. Die EU-Datenschutzgrundverordnung, die die EU-Mitgliedsstaaten ebenfalls bis Mai 2018 umsetzen müssen, gilt auch für Software- und Medizinproduktehersteller sowie für Gesundheitsorganisationen und schreibt Sicherheit und Privacy „by design and default“ gesetzlich vor.

2. Empfehlungen

2.1 Empfehlungen an politische Entscheidungsträger

Gemeinsame Standards für die Zertifizierung medizinischer IT-Sicherheit

Behörden sollten in Zusammenarbeit mit Herstellern und Zertifizierungsstellen konkrete gemeinsame europäische IT-Sicherheitskriterien als Bestandteil des Zertifizierungsprozesses für Medizinprodukte entwickeln. Die Europäische Kommission hat kürzlich einen EU-weiten Zertifizierungsrahmen für die Cybersicherheit vorgeschlagen, der als Grundlage für die Zertifizierung von Sicherheitseigenschaften von Medizingeräten und -prozessen dienen könnte (European Commission 2017). Innerhalb dieses Schemas könnten medizintechnische Systeme und Sicherheitsanforderungen als Grundlage für die Bewertung, Prüfung und Zertifizierung der Cybersicherheit sowie anderer medizinischer Systemanforderungen dienen. Solche Systeme sollten so weit wie möglich mit internationalen Standards harmonisiert werden und somit international anwendbare Systeme schaffen, die auch die Transaktionskosten der Gerätehersteller senken.

Weitere Hinweise lassen sich aus internationalen Standards für das sichere Design und die Entwicklung von Softwarekomponenten, FDA-Richtlinien und bestehenden Richtlinien zur Sicherheit von industriellen Kontrollsystemen (ICS) ableiten. Die Eigenschaften von ICS sind in der Tat vergleichbar mit denen von Medizinprodukten, da es sich bei beiden um Systeme handelt, in denen eingebettete Computer die Wechselwirkungen physikalischer Geräte mit ihrer Umgebung steuern. Die Maßnahmen zur Sicherung von eingebetteten Computersystemen im industriellen Kontext sind daher auch im Gesundheitswesen anwendbar. Beispiele für Leitfäden sind der internationale Entwurf der Normreihe IEC 62443 zur industriellen Netzwerk- und Systemsicherheit, der ICS Security Guide (NIST 2015) des US National Institute of Standards and Technology (NIST) und der vorgeschlagene europäische Zertifizierungsrahmen für die Cybersicherheit von Komponenten industrieller automatisierter Steuerungssysteme (Europäische Kommission 2016).

Förderung der Transparenz von IT-Sicherheitsrisiken und -vorfällen

Europäische und nationale medizinische Aufsichtsbehörden sollten Informationen über IT-Sicherheitsrisiken und Vorfälle in Medizingeräten öffentlich zugänglich machen. Derzeit müssen die nationalen Behörden Informationen über sicherheitsrelevante Vorkommnisse an die Europäische Datenbank für Medizinprodukte (Eudamed) übermitteln, die nur für EU-Institutionen und nationale Behörden zugänglich ist. Laut MDR werden die meisten Informationen, die an Eudamed übermittelt werden, in Zukunft öffentlich zugänglich sein.

Informationen über Software-Schwachstellen in Bezug auf Medizinprodukte sollten auch für alle Stakeholder zugänglich gemacht werden. Das Common Vulnerability Scoring System (CVSS) ist nützlich bei der Bewertung des Informationssicherheitsrisikos einer Schwachstelle (in Bezug auf die Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit). Um die potenziellen Auswirkungen von Schwachstellen auf die Systemsicherheit zusätzlich zur funktionalen Sicherheit („Safety") zu erfassen, sollten CVSS oder andere Schwachstellenbewertungssysteme an den Cybersicherheitskontext angepasst werden. Die MITRE Corporation und die FDA haben eine Arbeitsgruppe gebildet, in der Hersteller von Medizinprodukten, Anbieter von Gesundheitsdienstleistungen und Cybersicherheitsexperten gemeinsam einen Ansatz für die Verwendung von CVSS zur Bewertung von Schwachstellen bei Medizinprodukten entwickeln (Carmody und Zuk 2017).

Informationsaustausch

Europäische und nationale Entscheidungsträger sollten sich für einen besseren Informationsaustausch über Cybersicherheitsbedrohungen im Gesundheitswesen einsetzen. Derzeit ist die gemeinsame Nutzung von Informationen fragmentiert. Sicherheitszwischenfälle werden den nationalen Behörden gemeldet und in der Eudamed-Datenbank gesammelt. Gesundheitsorganisationen, die nach der EU-NIS-Richtlinie als „Betreiber kritischer Infrastrukturen" eingestuft sind, müssen größere Sicherheitsvorfälle an nationale Informationssicherheitsbehörden melden, die sich von den medizinischen CAs unterscheiden. EU-Institutionen und nationale Behörden sowie die Industrie sollten ein Informationsaustauschsystem einrichten, das einen besseren Austausch von Informationen über Bedrohungen im Gesundheitssektor gewährleistet. Außerdem sollte sie den Austausch von Informationen über Bedrohungen mit anderen Sektoren fördern. Der Informationsaustausch könnte über ein neutrales Information Sharing and Analysis Center (ISAC), ein sektorales koordinierendes Computer Emergency Response Team (CERT) oder nationale CERTs ablaufen. In den USA beispielsweise stellt ein National Health Information Sharing & Analysis Center (NH-

ISAC) Bedrohungsinformationen und Austauschdienste zur Verfügung.

2.2 Empfehlungen für Hersteller und Lieferanten

Das Gesundheitswesen ist eine kritische Infrastruktur. Krankenhäuser als Betreiber kritischer Infrastrukturen und andere Anwender medizinischer Geräte sind für den sicheren Betrieb medizinischer Geräte in ihren Netzwerken verantwortlich. Wie bereits erwähnt sind sie durch die EU-NIS-Richtlinie und die GDPR geregelt. Die Norm IEC 80001 bietet Leitlinien für die Anwendung des Risikomanagements in IT-Netzwerken mit Medizinprodukten für Gesundheitsorganisationen. Krankenhäuser sollten in ihren Organisationen das Management von Medizingeräten, welches traditionell Aufgabe der Biomedizintechniker ist und von Netzwerken, die traditionell unter der Schirmherrschaft der IT-Abteilung stehen, integrieren und verbinden.

Die letztendliche Verantwortung für die Sicherheit von Medizingeräten liegt bei den Herstellern. Nach dem EU-Haftungsrecht haften die Hersteller für Schäden, die durch ein fehlerhaftes Produkt verursacht werden. Um Cybersicherheitsrisiken so weit wie möglich zu minimieren, sollten Hersteller eine Reihe von sicherheitsrelevanten Praktiken vor dem Inverkehrbringen (bevor das Gerät auf den Markt gebracht wird) und Post-Market-Management-Mechanismen für die Überwachung, Umgang mit Schwachstellen und den Informationsaustausch implementieren.

Mehrere Hersteller medizinischer Geräte haben effektive Verfahren eingeführt, um die Cybersicherheit in Geräten während ihres gesamten Lebenszyklus zu gewährleisten, einschließlich eines verantwortungsbewussten Patch-Managements und eines strukturierten Prozesses zum Umgang und der Behebung von Schwachstellen (Draeger 2017; Siemens Healthineers 2017). Diese können in der Branche als Vorbild dienen.

Sicherheit 'by design'

Sicherheit sollte von vornherein in den Entwicklungsprozess und die Geräte integriert werden. Bei der Entwicklung von Medizinprodukten sollten Hersteller bewährte Standards für sichere Lebenszyklen und ein sicheres Supply-Chain-Management beachten. Alle handelsüblichen Hard- und Softwareprodukte, die in Geräte integriert sind, sollten nachweisbar vertrauenswürdig und sicher sein. Hersteller sollten die Konnektivität von Geräten auf das notwendige Minimum reduzieren und sicherheitskritische Systemkomponenten von anderen potenziell anfälligen Komponenten innerhalb der Geräte isolieren.

Integrierte Bewertung von Sicherheitsrisiken

Hersteller sowie benannte Zertifizierungsstellen sollten integrierte Methoden zur Bewertung und zum Management von Sicherheitsrisiken auf Medizinprodukte anwenden. Die Forschung auf diesem Gebiet hat eine Reihe von integrierten Risikobewertungsmethoden für (industrielle) Kontrollsysteme vorgestellt, die etablierte Standards für das Risikomanagement von Medizinprodukten ergänzen können, wie zum Beispiel SAHARA oder Unified Security and Safety Risk Assessment Methods (Chockalignam et al., 2016). Die bereits erwähnten FDA-Vorvermarktungsrichtlinien für Cybersicherheit sowie die Norm IEC 62433 bieten zusätzliche Hilfestellung in diesem Bereich.

Transparenz über Gerätesicherheit und -risiken

Gerätehersteller und -verkäufer sollten transparent erklären, wie ihre Geräte die Anforderungen an die medizinische IT-Sicherheit erfüllen. Das Handbuch für Geräte sollte nicht nur Gebrauchsanweisungen enthalten, sondern auch ein Bedrohungsmodell des Geräts in Gebrauchskontexten, um die Risiken der Verwendung des Geräts deutlich zu machen. Dies würde Gerätebetreibern und Anwendern die notwendigen Informationen über Sicherheitskompromisse und die Möglichkeit geben, über die damit verbundenen Risiken zu entscheiden.

Software- und Hardwarelieferanten sollten gleichermaßen transparent sein und die Sicherheitsmechanismen und Bedrohungsmodelle ihrer Software sowie die Auswirkungen ihrer Verwendung in einem Gerät erläutern.

Patch-Management

Hersteller sollten ein effektives und anwendbares Patch-Management-System betreiben. Sobald eine Schwachstelle bekannt ist, müssen die Geräte rechtzeitig Software-Sicherheitsupdates erhalten. Da Software-Updates selbst Sicherheitsrisiken bergen, sollten sie vor dem Einsatz in einer Einsatzumgebung getestet werden. Darüber hinaus müssen Gerätehersteller sichere Kanäle für die Bereitstellung von Updates implementieren, um deren Manipulation zu verhindern.

Schwachstellen-Meldesystem

Hersteller sollten ein Schwachstellen-Meldesystem betreiben, mit dem sie mit Dritten zusammenarbeiten, die Sicherheitslücken in der Software entde-

cken. Viele Hersteller medizinischer Geräte, darunter Siemens, Draeger, Medtronic und Philips, haben in den letzten Jahren koordinierte Programme zur Offenlegung von Schwachstellen implementiert (I am the Cavalry 2017). Diese Entwicklungen sind ermutigend. Die Normen ISO/IEC 29147: Information Technology - Security Techniques - Vulnerability Disclosure und ISO/IEC 30111:2013 Information Technology - Security Techniques - Vulnerability Handling Processes liefern Richtlinien für die Hersteller und ihre Übernahme sollte von öffentlichen Institutionen gefördert werden.

3. Referenzen

Bellovin, S.M. (2017). Patching is hard. SMBlog. https://www.cs.columbia.edu/~smb/blog/2017-05/2017-05-12.html (letzter Zugriff am 30.10.2017).

Brook, C. (2017). Patches pending for medical devices hit by WannaCry. Threatpost, May 18. https://threatpost.com/patches-pending-for-medical-devices-hit-by-wannacry/125758/ (letzter Zugriff am 30.10.2017).

Bryans, J. W. (2017). The internet of automotive things: vulnerabilities, risks and policy implications. *Journal of Cyber Policy* 2 (2): 185-194.

Burleson, W., S. Clark, B. Ransford, and K. Fu. (2012). Design challenges for secure implantable medical devices. *DAC*, June 3-7, San Francisco, California, USA.

Carmody, S. and M. Zuk. (2017). The evolving state of medical device cybersecurity. *HIMSS Annual Conference, Feb 19-23.* http://www.himssconference.org/sites/himssconference/files/pdf/16FINAL.pdf (letzter Zugriff am 30.10.2017)

Chockalingam, S., D. Hadžoismanović, W. Pieters, A. Teixera, and P. van Gelder. (2016). Integrated safety
and security risk assessment methods: A survey of key characteristics and applications. *The 11th International Conference on Critical Infrastructure Security*.

Draeger (2017). Cybersecurity. https://www.draeger.com/en_uk/Hospital/Insights-to-Solutions/Cybersecurity (letzter Zugriff am 07.12. 2017).

European Commission. (2016). Introduction to the European IACS components Cybersecurity Certification Framework (ICCF). https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf (letzter Zugriff am 30.10.2017).

European Commission. (2017). COM(2017) 477 final. The EU cybersecurity certification framework. *Proposal for a Regulation of the European Parliament and of the Council*. https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework (letzter Zugriff am 30.10.2017).

Filkins, B. (2014). Healthcare cyberthreat report: Widespread compromises detected, compliance nightmare on the horizon. *SANS Institute InfoSec Reading Room*. https://www.sans.org/reading-room/whitepapers/analyst/health-care-cyber-threat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735 (letzter Zugriff am 30.10.2017).

Fox-Brewster, T. (2017). Medical devices hit by ransomware for the first time In US hospitals. *Forbes*, May 17. http://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/ (letzter Zugriff am 30.10.2017).

Halperin, D.,Heydt-Benjamin, B. Ransford, S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno and W. Maisel. (2008). Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero Power Defenses. *IEEE Symposium on Security and Privacy*.

I Am The Cavalry (2017). An overview of vulnerability disclosure programs. https://www.iamthecavalry.org/resources/disclosure-programs/ (letzter Zugriff am 07.12.2017).

ICS-CERT (2017). Indicators associated with WannaCry ransomware (Update I). May 15. https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-135-01I (letzter Zugriff am 30.10.2017).

Independent Security Evaluators. (2016). Hacking hospitals. February 23. https://www.securityevaluators.com/hospitalhack/securing_hospitals.pdf (letzter Zugriff am 30.10.2017).

Johnson, C. (2012). CyberSafety: On the interactions between cybersecurity and the software engineering of safety-critical systems. In *Achieving system safety*, ed. C. Dale and T. Anderson. London: Springer Verlag.

Leverett, E., R. Clayton, and R. Anderson. (2017). Standardisation and certification in the 'Internet of Things'. *16th Annual Workshop on the Economics of Information Security (WEIS)*.

http://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/05/WEIS_2017_paper_23.pdf (letzter Zugriff am 30.10.2017).

Li, C., A. Raghunathan, and N. K. Jha. (2011). Hijacking an insulin pump: Security attacks and defences for a diabetes therapy system. *Proceedings of the 13th IEEE International Conference on e-Health Networking, Applications, and Services, Healthcom '11.*

Marin E., D. Singelée, F. D. Garcia, T. Chothia, R. Willems, and B. Preneel. (2016). On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them. *ACSAC '16 Proceedings of the 32nd Annual Conference on Computer Security Applications: 226-236.* https://www.esat.kuleuven.be/cosic/publications/article-2678.pdf (letzter Zugriff am 30.09.2017).

National Institute for Standards and Technology (2015). SP 800-82, Revision 2. Guide to industrial control systems (ICS) security.

Nunnikhoven, M. (2017). WannaCry & the reality of patching, 14 May. Retrieved from http://blog.trendmicro.com/wannacry-reality-of-patching/ (letzter Zugriff am 30.10.2017).

Ponemon Institute. (2017). Medical device security: An industry under attack and unprepared to defend. https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/medical-device-security-ponemon-synopsys.pdf (letzter Zugriff am 30.10.2017).

Radcliffe, J. (2011). Hacking medical devices for fun and insulin: Breaking the human SCADA system. *Black Hat Conference 2011.*

Rios, B. and J. Butts. (2017). Security evaluation of the implantable cardiac device ecosystem and architecture and implementation interdependencies. *WhiteScope Security Report*, May 17. https://drive.google.com/file/d/0B_GspGER4QQTYkJfaVlBeGVCSW8/view (letzter Zugriff am 31.08.2017).

Roland Berger Consultants (2016). Digital healthcare market to average 21 percent growth per year through 2020. September 28. https://www.rolandberger.com/en/press/Digital-health-market-to-average-21-percent-growth-per-year-through-2020.html (letzter Zugriff am 30.10.2017).

Siemens Healthineers (2017). Cybersecurity at Siemens Healthineers. https://www.healthcare.siemens.com/medical-imaging-it/cybersecurity (letzter Zugriff am 7.12.2017).

US Food & Drug Administration (2014). Content of premarket submissions for management of cybersecurity in medical devices. Guidance for industry and Food and Drug Administration staff. https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf (letzter Zugriff am 30.10.2017).

US Food & Drug Administration (2016). Postmarket management of cybersecurity in medical devices. Guidance for industry and Food and Drug Administration staff. https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf (letzter Zugriff am 30.10.2017).

US Food & Drug Administration (2017). Firmware update to address cybersecurity vulnerabilities identified in Abbott's (formerly St. Jude Medical's) implantable cardiac pacemakers. *FDA Safety Communication*, August 29. https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm (letzter Zugriff am 31.08.2017).

DSI Industrial & Policy Recommendations (IPR) Series is published by the Digital Society Institute of ESMT Berlin, http://dsi.esmt.org.