Cybersecurity für Medizinprodukte nach Vorgaben des US Department of Defense

Die Veröffentlichung dieses Artikels erfolgt mit freundlicher Genehmigung der Philips GmbH Market DACH, Röntgenstraße 22, 22335 Hamburg

Stefan Trapp

Palmerstraße 31
20535 Hamburg

stefan.trapp@stefan-trapp-consulting.de
www.stefan-trapp-consulting.de

Inhaltsverzeichnis

1 Einleitung

Neben der Betriebssicherheit (Safety), d. h. dem Schutz von Mensch und Umwelt vor physischem Schaden, haben Hersteller von Medizinprodukten auch die Informationssicherheit (Security bzw. Cybersecurity) und damit insbesondere den Schutz von Daten vor Angriffen „von außen“ zu gewährleisten. Dies gilt umso mehr, weil Medizinprodukte und die mit ihnen verknüpften Daten wegen ihrer Bedeutung für Leben, Gesundheit und Privatsphäre von Patienten einen besonders schützenswerten und sensiblen Bereich bilden. [1]

Während die Betriebssicherheit schon lange Zeit Gegenstand gesetzlicher und weiterer regulatorischer Vorgaben ist, z. B. in Form des Risikomanagements gemäß DIN EN ISO 14971, rückt die Informationssicherheit erst in jüngerer Zeit mehr und mehr in den Fokus von Kunden, Gesetzgebern, Aufsichtsbehörden und Produzenten. Getrieben wird diese Entwicklung einerseits durch wachsende Gefahren in Folge fortschreitender Digitalisierung, z. B. die zunehmende Vernetzung oder die wachsende Bedeutung von Informationstechnik und Software gegenüber „klassischer“ Hardware und andererseits durch eine Reihe spektakulärer Cyberangriffe mit gravierenden Folgen für medizinische Einrichtungen und Geräte, vgl. z. B. [2], [3], [4], [5]. Besonders problematisch im Hinblick auf die Informationssicherheit sind in der Medizintechnik die oftmals langen Produktlebenszyklen, die ohne eine geeignete Update-Strategie (von Hersteller und/oder Betreiber) für das lange Verweilen älterer, besonders angreifbarer Technologien (z. B. das Betriebssystem Windows XP) in der installierten Produktbasis sorgen [6].

Als **Cybersecurity-Management** oder **IT-Sicherheitsmanagement** können vorbeugende Methoden zum Schutz aller Arten von Computern, von Computerinformationssystemen, Infrastrukturen, Computernetzwerken, Programmen oder Daten vor Diebstahl, Beschädigung oder Angriffen definiert werden. Zweck des Cybersecurity-Managements ist die Gewährleistung mehrerer Schutzziele: In erster Linie sind dies **Vertraulichkeit** (confidentiality), **Integrität** (integrity) und **Verfügbarkeit** (availability), die sogenannte CIA-Triade [7], [8]. Weitere oft genannte Schutzziele sind **Transparenz** (transparency) − mit den Unterzielen Authentizität (authenticity), Zurechenbarkeit (accountability) und Revisionsfähigkeit (reviewability) − und **Kontingenz** (contingency) [9]. Ein **Cyberangriff** ist ein unerwünschter bzw. unerlaubter und zumeist widerrechtlicher Versuch, die oben genannten Vermögenswerte (öffentlich) zugänglich zu machen, zu ändern, zu deaktivieren, mutwillig funktionsunfähig zu machen, zu zerstören, zu stehlen, sich unbefugten Zugriff darauf zu verschaffen oder sie unbefugt zu nutzen. Ein effektives Cybersecurity-Management unter Nutzung geeigneter Technologien, Prozesse und Maßnahmen verringert das Risiko, d. h. die Wahrscheinlichkeit und die möglichen Auswirkungen, erfolgreicher Cyberangriffe.

Das **US Verteidigungsministerium** (**Department of Defense − DoD**) besitzt mit dem DoD **Risk Management Framework** (**RMF**) einen der umfassendsten existierenden Prozesse zur Beschreibung von IT-Sicherheitsmaßnahmen und zur Autorisierung des Betriebes von Informationssystemen. Das RMF ist auch − neben anderen IT-Systemen − auf Medizinprodukte, die an das DoD verkauft bzw. dort betrieben werden (sollen), anwendbar und umfasst die Cybersicherheit dieser Systeme während ihres gesamten Lebenszyklus. Es handelt sich beim RMF um einen risikobasierten Prozess, der erstens die frühzeitige Implementierung und Dokumentation von organisatorischen und technischen Maßnahmen der Cybersicherheit in der Produkt-Entwicklungsphase fordert und fördert. Zweitens soll auch nach dem Inverkehrbringen des Produkts, in seiner Nutzungsphase beim US DoD, die kontinuierliche Überwachung und Erfüllung der umfassend definierten Cybersecurity-Anforderungen sichergestellt werden.

Dieser Artikel gibt zunächst eine Übersicht über existierende regulatorische Anforderungen zur Cybersecurity in der Medizintechnik und umreißt kurz die Inhalte des US DoD RMF. Anschließend beschreibt er, wie die Philips Healthcare Business Category (BC) Diagnostic X-Ray (DXR) die Anforderungen des RMF erfolgreich umgesetzt hat und für ausgewählte digitale Röntgensysteme eine **Authorization to Operate** (**ATO** − Autorisierung zum Betrieb beim US DoD) erhalten hat.

2 Regulatorische Anforderungen zur Cybersecurity in der Medizintechnik

Die wachsende Bedeutung der Cybersecurity in der Medizintechnik aus ethischen, aber auch aus wirtschaftlichen Gründen spiegelt sich zugleich in einer wachsenden Zahl von regulatorischen Anforderungen in der EU, den Vereinigten Staaten (US FDA), Kanada (Health Canada), China (CFDA), Japan (MHLW) und weiteren Ländern bzw. Regionen der Welt wider. Über konkrete Maßnahmen zur Gewährleistung der Cybersecurity wie Schwachstellenscans und Penetrationstests hinaus (z. B. UL 2900-2-1) werden hier regelmäßig auch umfassendere Anforderungen gestellt, die auf die Erreichung von **Security by Design** [10] zielen. Beispiele solcher Anforderungen sind gut strukturierte Entwicklungs-, Lifecycle- und Service-Prozesse, die Security-Anforderungen von Beginn der Produktentwicklung an berücksichtigen und ihre Erfüllung über den gesamten Produktlebenszyklus bis zur Obsoleszenz sicherstellen. Im weiteren Verlauf dieses Abschnittes wird vorrangig die Situation in den USA und der EU beschrieben.

Die US-amerikanische Bundesaufsichtsbehörde für Lebens- und Arzneimittel (Food and Drug Administration – FDA) hat 2014 bzw. 2016 Medizinprodukt-Richtlinien (Guidances) für das Cybersecurity-Risikomanagement von der Konzeption in der Entwicklungsphase (Content of Premarket Submissions for Management of Cybersecurity in Medical Devices [11]) bis zur Obsoleszenz nach der Nutzungsphase (Postmarket Management of Cybersecurity in Medical Devices [12]) veröffentlicht. Diese vergleichsweise generisch gehaltenen Richtlinien nehmen Bezug auf einige anerkannte Security-Standards, z. B. IEC 80001, IEC 62443 oder das Framework for Improving Critical Infrastructure Cybersecurity des National Institute of Standards and Technology (NIST) [13]. Dennoch sind zur Anwendung dieser Standards auf Geräte und Infrastrukturen im Healthcare-Bereich umfassende Erfahrung und detailliertes Fachwissen notwendig [14]. Ein weiteres einschlägiges Dokument aus dem US-Raum ist der Technical Information Report 57 der Association for the Advancement of Medical Instrumentation (AAMI TIR57), das den Stand der Technik hinsichtlich der Analyse und Bewertung von Cybersecurity-Risiken im Rahmen des Risikomanagements für Medizinprodukte nach EN ISO 14971 repräsentiert.

Zu den Regularien der EU zur Informationssicherheit von Medizinprodukten zählen die Verordnungen (EU) 2017/745 über Medizinprodukte (Medical Device Regulation – MDR, insbesondere Anhang I) und 2017/746 über in-vitro Diagnostika (In-Vitro Diagnostic Medical Devices Regulation – IVDR). In den grundlegenden Sicherheits- und Leistungsanforderungen wird dort Cybersecurity als Teil des Risikomanagements nach ISO 14971:2019 eingefordert (IT-Security-Analyse). Die MDR löst die älteren Richtlinien über Medizinprodukte (93/42/EWG – MDD) und aktive implantierbare Medizinprodukte (90/385/EWG – AIMD) nach einem Übergangszeitraum (26. Mai 2020 bzw. 26. Mai 2022) ab. Ähnlich wie bei den Richtlinien der FDA gilt auch hier, dass die konkrete Erfüllung dieser eher generisch formulierten Cybersecurity-Anforderungen für Medizinprodukthersteller schwierig ist, weil gegenwärtig noch keine (harmonisierten) europäischen Normen existieren. Allerdings arbeiten die Gremien mit der IEC/TR 60601-4-5 an einer neuen Norm für die Cybersecurity von Medizin-

produkten, die sich auf die Normenreihe IEC 62443 (insbesondere 62443-4-2) aus der Industrieautomatisierung stützt.

Neben den oben angesprochenen spezifischen Cybersecurity-Regularien für Medizinprodukthersteller sind noch eine Reihe anderer Anforderungen zu berücksichtigen. Dies sind etwa

1. allgemeine Bestimmungen für Medizinprodukthersteller, z. B. die IEC 62304 über die wichtigsten Lebenszyklus-Prozesse von Medizingeräte-Software,
2. Vorschriften für die Betreiber von Medizinprodukten, in Deutschland beispielsweise die Medizinprodukte-Betreiberverordnung (MPBetreibV), in den USA z. B. der Health Insurance Portability and Accountability Act (HIPAA) zum Schutz von Patientendaten,
3. allgemeingültige Bestimmungen wie z. B. die EU Datenschutz-Grundverordnung (DSGVO bzw. GDPR – General Data Protection Regulation) oder die Normenreihen ISO/IEC 15408, 27001 und 27034, die auch für Medizinprodukte anzuwenden sind, sowie
4. zusätzliche nationale Empfehlungen oder Sicherheitsstandards wie die US-amerikanische Federal Information Processing Standard Publication 140-2 (FIPS PUB 140-2, Sicherheitsanforderungen für kryptographische Module) oder die Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI).

Das US DoD als besonders cybersecurity-sensibler Kunde für Medizinprodukte hat mit seinem RMF über die bisher genannten Regularien hinausgehende, eigene Cybersecurity-Anforderungen entwickelt. Die vom DoD anerkannte Erfüllung dieser Anforderungen durch Medizinprodukthersteller ist Voraussetzung für deren Lieferungen an das US DoD. Der folgende Abschnitt beschäftigt sich näher mit dem US DoD RMF.

3 Das US DoD Risk Management Framework (RMF)

Das DoD RMF beschreibt den DoD-Prozess zur Identifikation, Implementierung, Bewertung und zum Management von Cybersicherheitsfunktionen und -diensten. Es definiert außerdem Sicherheitskontrollen für die Autorisierung des Betriebs von Informationssystemen (IS) und Informationstechnologie-Plattformen (PIT) für Einrichtungen des DoD. Das RMF basiert im Wesentlichen auf zwei Publikationen des National Institute of Standards and Technology (NIST): Special Publication 800-37 [15] und Special Publication 800-53 [16]. Es umfasst nach einer Vorbereitungsphase der Hersteller-Organisation (Prepare) – wie in Abbildung 1 gezeigt – sechs Phasen: (1) Kategorisieren des Informationssystems, (2) Auswählen von Sicherheitsmaßnahmen, (3) Implementieren von Sicherheitsmaßnahmen, (4) Bewerten von Sicherheitsmaßnahmen, (5) Autorisieren des Informationssystems (ATO) und (6) Überwachen der Effektivität der Sicherheitsmaßnahmen. Der Prozess verläuft parallel zum Systemlebenszyklus, wobei die RMF-Aktivitäten bereits zu Programm- bzw. Entwicklungsbeginn gestartet werden sollten. Ein RMF-Projekt für ein Produkt wird aktiv (active), wenn das angebotene Produkt vom US DoD (z. B. Army, Navy oder Air Force) entweder tatsächlich gekauft wurde oder bereits in der installierten Basis vorhanden ist.

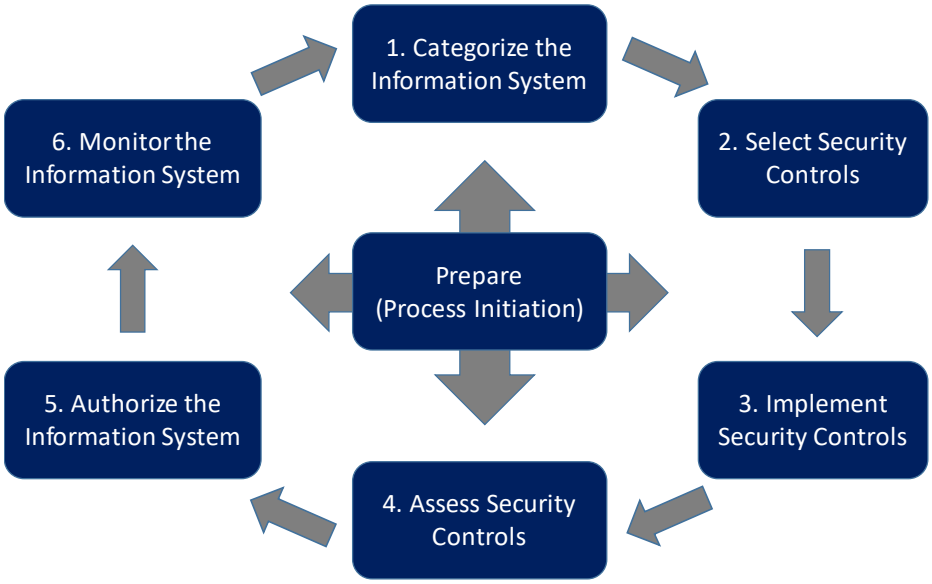

Abbildung 1: Phasenmodell des US DoD Risk Management Framework (RMF) [15]

Produkte müssen das RMF-Akkreditierungsverfahren durchlaufen, um eine Betriebsgenehmigung (ATO) zu erhalten. Dieser Prozess dauert in der Regel zwischen 6 und 18 Monaten. Eine erteilte ATO ist maximal 36 Monate gültig, möglicherweise aber auch kürzer, wenn sie unter Auflagen erteilt wurde (ATO-Contingent – ATO-C). Die ATO von Systemen, die an das US DoD verkauft wurden, muss jedoch insgesamt mindestens 6 Jahre lang aufrechterhalten werden. Daher muss die erneute Zulassung rechtzeitig, mindestens 6 Monate vor dem Fälligkeitsdatum der vorherigen ATO, erfolgen.

Bedeutsam für Medizinprodukthersteller sind insbesondere folgende Elemente des RMF:

- Umfangreiche Dokumentationsanforderungen und -vorgaben, die sich aufgrund neuer Revisionen oder Vorlagen häufig ändern.
- Eine große Anzahl technischer Implementierungsleitfäden (Security Technical Implementation Guides – STIGs), die sehr detailliert Sicherheitsanforderungen definieren. Dabei gibt es zwei grundsätzliche Arten von STIGs: Automatisiert zu testende STIGs (Scans/Benchmarks) und manuell zu beantwortende. Auch Kombinationen aus beiden Varianten kommen vor. Speziell die Bearbeitung manueller STIGs ist vergleichsweise aufwendig.

Als allgemeine Leitlinie für das RMF kann das Push-Prinzip bezeichnet werden: Geforderte Artefakte sollten dem DoD immer proaktiv, gemäß Absprache geliefert werden. Beispiele sind monatliche Statusberichte auf Basis des Vulnerability-Scanners „Tenable Nessus“ oder die Bereitstellung gegebenenfalls notwendiger Software-Updates.

4 Erfüllung der RMF-Anforderungen bei Philips Healthcare DXR

Diagnostic X-Ray (DXR) ist eine Geschäftseinheit (Business Category – BC) der Sparte Healthcare des niederländischen Philips Konzerns. Entwickelt, produziert und vertrieben werden digitale Radiographie- und Durchleuchtungssysteme (Fluoroskopie). Diese basieren auf der gemeinsamen Software-Plattform „Eleva“.

Schon vor der Initiierung des RMF-Prozesses für seine Produkte hat DXR Maßnahmen zur Verbesserung der Produkt-Cybersecurity bei Design, Verifikation, Herstellung und im Betrieb in der Klinik eingeführt. So wurde entsprechend qualifiziertes Personal (z. B. Product Security Officer, Security Architect) aufgebaut, Cybersecurity-Anforderungen bereits in der Entwicklungsphase integriert, regelmäßige Software-Schwachstellen-Scans und Penetrationstests etabliert und technische und administrative Möglichkeiten zum Patchen der Systeme der installierten Basis mit Sicherheits-Updates geschaffen. Beispiele derartiger Maßnahmen in Produkt- und Software-Design im Hinblick auf Cybersecurity sind

- Hard- und Software-Firewalls,
- Betriebssystem- und Applikations-Härtung (hardening),
- User- und User-Group-Management (Principle of Least Privilege – PoLP),
- einstellbare Kennwort-Regeln und/oder Zwei-Faktor-Authentisierung,
- Audit Trail, d. h. Aufzeichnung und Nachverfolgbarkeit von Aktionen am System,
- Whitelisting und/oder Viren-Scanner,
- Verschlüsselung und sichere Übertragungsprotokolle (z. B. Secure Dicom auf Basis von TLS),
- Vermeidung überflüssiger Software, Dienste, Ports und Protokolle, Accounts oder Account-Rechte,
- Schaffung der softwaretechnischen Voraussetzungen für sichere und effiziente Software-Updates (lokal beim Kunden oder remote per Internet),
- tatsächlich durchgeführte, regelmäßige Aktualisierung durch Patches und Updates inklusive der im System enthaltenen third-party Software,
- Anwendung etablierter Sicherheitsstandards und entsprechend zertifizierter Software-Komponenten.

Um Produkte an das US DoD liefern zu können, wurde darüber hinaus der in Abbildung 2 dargestellte Produktlebenszyklus für DoD-Systeme mit den im Folgenden beschriebenen Phasen realisiert.

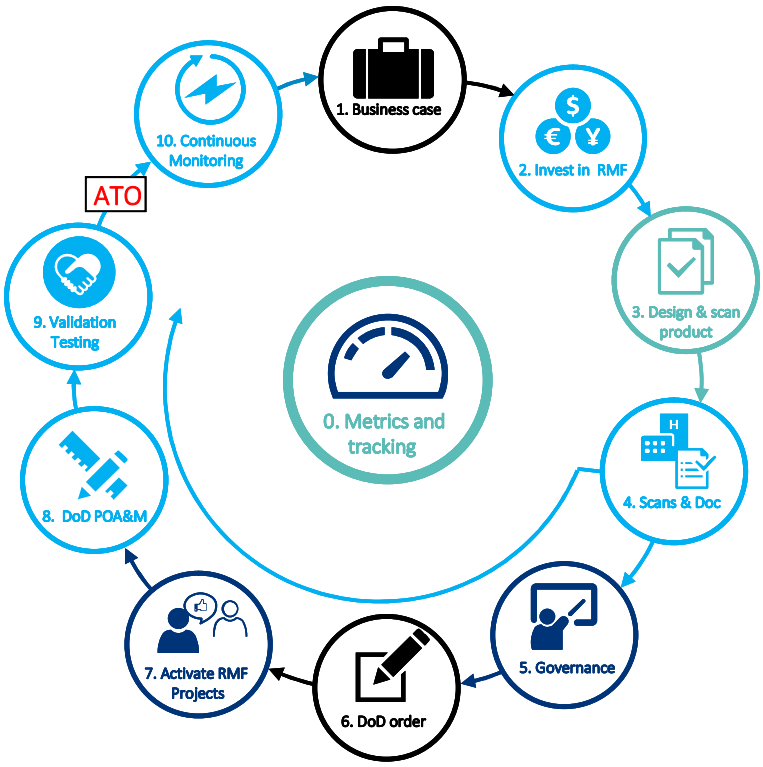

Abbildung 2: Produktlebenszklus für das US DoD bei Philips DXR. Quelle: Philips

1. **Produktspezifischer Business Case:** Die Philips US-Vertriebsorganisation für Regierungsverkäufe stellt einen aus ihrer Sicht profitablen Business Case bereit und benennt einen möglichen Pilotkunden innerhalb des DoD („Sponsor“).
2. **Roadmapping und Investitionsentscheidung:** Die BC DXR prüft entsprechende Business Cases im Rahmen des regelmäßigen Roadmappings und entscheidet über die Investition in eine RMF-Akkreditierung eines Produkts oder einer auf der Eleva-Software-Plattform basierenden Produktfamilie. Erforderliche Ressourcen werden eingeplant. Sorgfältig beachtet werden müssen im Roadmapping die RMF-Kosten über die gesamte Produktlebensdauer. Nur Beträge, die im initialen Verkaufsangebot an das DoD genannt sind, können später auch in Rechnung gestellt werden. Nachforderungen sind weitgehend ausgeschlossen. Zudem werden in der Regel langfristige Produkt-Upgrade-Pfade über die gesamte Produktlebensdauer beim DoD benötigt, z. B. Upgrades des nicht mehr durch Microsoft gewarteten Windows 7 auf Windows 10. Im Gegensatz zu den regelmäßigen „kleineren“ Sicherheits-Patches besteht hier allerdings eventuell die Möglichkeit, diese „großen“ Upgrades in Rechnung zu stellen.
3. **Design und Scans zur Erfüllung der RMF-Anforderungen:** DXR entwickelt und realisiert einen „Plan zur kontinuierlichen Überwachung“ von Produktzertifizierung und –konformität. Unterstützt wird die BC dabei durch Field-Marketing-Security-Experten der Philips US-Vertriebsorganisation, die die Schnittstelle zwischen Philips und den zuständigen Stellen des DoD bilden.
4. **Scans und Dokumentation:** Während des gesamten RMF-Prozesses werden monatlich aktualisierte Software-Scans mit dem „Tenable Nessus“ Vulnerability-Scanner und die relevanten STIGs (s. o.) mit dem DoD ausgetauscht. Die geforderte Dokumentation nach Vorgaben des DoD (z. B. Vendor Control List, Hardware-/Software-Inventar etc.) wird bereitgestellt und fortlaufend verbessert bzw. aktualisiert.
5. **Steuerung und Qualitätssicherung der RMF-Produktreife:** Die Field-Marketing-Security-Experten der Philips US-Vertriebsorganisation sichern die Qualität und termingerechte Bereitstellung sämtlicher Artefakte für das DoD.
6. **DoD Bestellung aktiviert den DoD RMF-Prozess:** Eine Bestellung des DoD bei der Philips US-Vertriebsorganisation für Regierungsverkäufe aktiviert den eigentlichen RMF-Prozess mit dem Ziel die ATO zu erlangen.
7. **Aktivierung und Management der laufenden RMF Projekte:** Fortlaufend werden Scans und Security-Dokumentation mit dem DoD ausgetauscht und verbessert. Dies geschieht weiterhin unterstützt durch die Field-Marketing-Security-Experten der Philips US-Vertriebsorganisation als Schnittstelle zwischen BC und DoD.
8. **DoD Aktionsplan (Plan of Action and Milestones – POA&M):** In Zusammenarbeit mit dem Sponsor beim DoD wird ein Aktionsplan (POA&M) erstellt, um etwaig verbliebene Sicherheitslücken bis zur ATO zu beseitigen. Nachweise für erzielte Fortschritte werden laufend zwischen BC und DoD ausgetauscht.
9. **DoD Validierungstest, abschließende Bewertung und Entscheidung über ATO:** Das DoD führt eine Validierung und abschließende Bewertung des Produkts durch und entscheidet über die Erteilung der ATO.
10. **Monatliches kontinuierliches Monitoring zur Beseitigung von Sicherheitslücken:** DXR stellt weiterhin (also sowohl pre-market als auch post-market), während der gesamten ATO-Laufzeit, monatliche Security-Scans bereit, analysiert potenzielle Risiken im Product Security Incident Response Team (PSIRT) und stellt bei Bedarf Sicherheitspatches innerhalb der vom RMF vorgegebenen Fristen (30/90/180/365 Tage),

abhängig von der Dringlichkeit, bereit. Sicherheitspatches müssen auf DoD-Systemen in der Regel durch einen Service-Ingenieur on-site installiert werden, da die Systeme im Allgemeinen keine Internetverbindung besitzen dürfen. Wenn vom DoD gefordert, erfolgt die Erstellung eines Aktionsplans (POA&M) zum zeitgerechten Schließen von Sicherheitslücken. Für im Medizinprodukt enthaltene third-party Software-Komponenten besteht darüber hinaus seitens des DoD die Forderung, dass diese mindestens 24 Monate über das System-Produktionsende hinaus noch von ihrem jeweiligen Hersteller Support erhalten müssen.

Die erfolgreiche Implementierung des geschilderten Prozesses bei Philips Healthcare DXR hat im Januar 2020 zur Erteilung einer ATO für zwei Produkte der Eleva-Produktfamilie geführt, nämlich für das digitale Radiographiesystem DigitalDiagnost und das nahbediente digitale Durchleuchtungsgerät ProxiDiagnost.

5 Fazit

Medizinprodukthersteller müssen sicherstellen, dass ihre Geräte die sich fortlaufend ändernden (oftmals wachsenden) regulatorischen Vorgaben erfüllen. Dies gilt auch und in steigendem Maße für die Anforderungen im Bereich Cybersecurity. Durch die fortschreitende Digitalisierung und Vernetzung von Medizinprodukten und einige spektakuläre Cyberattacken mit umfangreichen negativen Auswirkungen in jüngerer Zeit erhält die Cybersecurity bei Kunden und Anbietern inzwischen wachsende Aufmerksamkeit. Eine erfolgreich umgesetzte Cybersecurity-Strategie, die zu einem hohen Sicherheitsstandard der Produkte führt und sich effektiv an Vertriebsorganisation und Kunden kommunizieren lässt, wird damit zunehmend auch zu einem wichtigen Differenzierungsmerkmal im Wettbewerb.

Das US DoD ist ein besonders cybersecurity-sensibler Kunde für Medizinprodukte und macht die Erfüllung der in seinem RMF definierten Anforderungen zur Voraussetzung für sämtliche Lieferungen. Philips Healthcare Diagnostic X-Ray ist es gelungen, für auf der Eleva-Softwareplattform basierende Röntgensysteme die notwendige Autorisierung zum Betrieb beim US DoD (ATO) zu erlangen. Hierfür mussten einerseits organisatorische Voraussetzungen in Form neuer und adaptierter Unternehmensprozesse geschaffen werden. Andererseits galt es, softwaretechnische Maßnahmen zu realisieren, mit denen der geforderte hohe Cybersecurity-Status für das US DoD nachvollziehbar erreicht, regelmäßig überprüft und dauerhaft, während des gesamten Produktlebenszyklus beim US DoD, aufrechterhalten werden kann.

Die Akkreditierung eines Medizinprodukts gemäß RMF erfordert beim Hersteller umfassendes Know-how sowie entsprechende Prozesse und Ressourcen. Wegen der resultierenden langfristigen Verpflichtungen und der erheblichen Investitionen, die sich über den gesamten Produktlebenszyklus beim DoD erstrecken, muss die strategische Entscheidung für eine Akkreditierung unbedingt auf Basis eines tragfähigen Business Case getroffen werden.

6 Literatur

[1] N. N.: Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte. Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-CS 132, Version 1.0 vom 02.05.2018, im Internet: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_132.html?nn=6656412, abgerufen am 09.02.2020.

[2] Steiner, H.: Warum Vernetzung Kliniken angreifbar macht. Hessischer Rundfunk, hr-iNFO, 09.09.2018, im Internet: https://www.hr-inforadio.de/programm/dossiers/cybercrime-warum-vernetzung-kliniken-angreifbar-macht,cybercrime-vernetzung-kliniken-100.html, abgerufen am 09.02.2020.

[3] Sextl, J.: Klinikum Fürstenfeldbruck von Hackern angegriffen. Abendzeitung Digital, 17.11.2018, im Internet: https://www.abendzeitung-muenchen.de/inhalt.erfolgreiche-cyber-attacke-klinikum-fuerstenfeldbruck-von-hackern-angegriffen.c18f2de7-ada2-46f9-8367-5cb52615fa64.html, abgerufen am 09.02.2020.

[4] N. N.: Zurück zu Bleistift und Papier: Schadsoftware legt Klinikserver lahm. Heise online, 17.07.2019, im Internet: https://www.heise.de/newsticker/meldung/Zurueck-zu-Bleistift-und-Papier-Schadsoftware-legt-Klinikserver-lahm-4473927.html, abgerufen am 09.02.2020.

[5] Ries, U.: Geht doch: Rückruf angreifbarer Insulinpumpen nach über zwei Jahren. Heise online, 19.07.2019, im Internet: https://www.heise.de/security/meldung/Geht-doch-Rueckruf-angreifbarer-Insulinpumpen-nach-ueber-zwei-Jahren-4475601.html?wt_mc=rss.ho.beitrag.atom, abgerufen am 09.02.2020.

[6] Schäfer, K.: Cybersecurity in der Medizintechnik – eine reale Bedrohung. DeviceMed − Das Community-Portal, 01.03.2019, im Internet: https://www.devicemed.de/-cybersecurity-in-der-medizintechnik-eine-reale-bedrohung-a-804236/, abgerufen am 09.02.2020.

[7] Weis, E.: Vertraulichkeit, Integrität und Verfügbarkeit − Schutzziele der Informationssicherheit. Brandmauer IT Security Blog, 11.07.2018, im Internet: https://www.brandmauer.de/blog/it-security/schutzziele-der-informationssicherheit, abgerufen am 09.02.2020.

[8] Darms, M.; Haßfeld, S.; Fedtke, S.: IT-Sicherheit und Datenschutz im Gesundheitswesen – Leitfaden für Ärzte, Apotheker, Informatiker und Geschäftsführer in Klinik und Praxis. Wiesbaden: Springer Vieweg, 2019.

[9] Bedner, M.; Ackermann, T.: Schutzziele der IT-Sicherheit. DuD − Datenschutz und Datensicherheit 05/2010, S. 323 – 328, im Internet: https://www.uni-kassel.de/fb07/fileadmin/datas/fb07/5-Institute/IWR/Roßnagel/veroeffentlichungen/-bedner_ackermann_schutzziele_der_it_sicherheit_dud_2010_323.pdf, abgerufen am 09.02.2020.

[10] Santos, J. C. S.; Tarrit, K.; Mirakhorli, M.: A Catalog of Security Architecture Weaknesses. 2017 IEEE International Conference on Software Architecture (ICSA), im Internet: https://design.se.rit.edu/papers/cawe-paper.pdf, abgerufen am 09.02.2020.

[11] N. N.: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. U.S. Department of Health and Human Services, Food and Drug Administration, 02.10.2014, im Internet: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices-0, abgerufen am 09.02.2020.

[12] N. N.: Postmarket Management of Cybersecurity in Medical Devices. U.S. Department of Health and Human Services, Food and Drug Administration, 28.12.2016, im Internet: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices, abgerufen am 09.02.2020.

[13] N. N.: Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. National Institute of Standards and Technology, April 16, 2018, im Internet: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, abgerufen am 09.02.2020.

[14] Wilson, A.; Gerstl, S.: Security für Medizingeräte: Wie Sie die Herausforderungen meistern. Embedded Software Engineering, 12.06.2018, im Internet: https://www.embedded-software-engineering.de/security-fuer-medizingeraete-wie-sie-die-herausforderungen-meistern-a-723298/, abgerufen am: 09.02.2020.

[15] N. N.: NIST Special Publication 800-37 Revision 2 – Risk Management Framework for Information Systems and Organizations, December 2018, im Internet: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final, abgerufen am 09.02.2020.

[16] N. N.: NIST Special Publication 800-53 Revision 4 – Security and Privacy Controls for Federal Information Systems and Organizations, April 2013, im Internet: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf, abgerufen am 09.02.2020.

Autor

Dipl.-Ing. Dipl.-Ing. oec. Stefan Trapp, Jahrgang 1968, studierte Wirtschaftsingenieurwesen im hochschulübergreifenden Studiengang von Universität, HAW und TU Hamburg und ist außerdem Absolvent des Diplom-Studienganges Elektro- und Informationstechnik der Fern-Universität in Hagen. Er ist in der Philips Healthcare Business Category Diagnostic X-Ray (DXR) als Department of Defense Manager verantwortlich für die Implementierung US DoD RMF-konformer Prozesse und Produkte. Herr Trapp ist außerdem freiberuflich tätig und externer Doktorand bei Professor Joachim Warschat im Lehrgebiet Technologie- und Innovationsmanagement an der FernUniversität Hagen und am Fraunhofer IAO in Stuttgart.

Stichworte

ATO, Authorization to Operate, Cyberangriff, Cybersecurity, Cybersecurity-Management, Department of Defense, DoD, DXR, EU-MDR, FDA, Informationssicherheit, IT-Sicherheitsmanagement, Medizinprodukt, Medizintechnik, Philips Healthcare, Risikomanagement, Risk Management Framework, RMF, Security by Design, US DoD, US-Verteidigungsministerium