Leitfaden

Informationssicherheit bei vernetzbaren Medizingeräten
Umgang mit Informationen über Schwachstellen: erkennen, prüfen, melden

Motivation

Die Mitglieder des ZVEI-Fachverbands Elektromedizinische Technik empfehlen Herstellern von vernetzbaren Medizingeräten in ihren Organisationen freiwillig Maßnahmen und Prozesse zu implementieren, mit denen die schnelle, koordinierte und angemessene Behebung bekanntgewordener Schwachstellen der Informationssicherheit von Produkten – insbesondere vernetzter Medizintechnik – sichergestellt wird.

Dieser Leitfaden beschreibt die empfohlene Vorgehensweise beim Umgang mit auftretenden Schwachstellen für herstellende Unternehmen vernetzbarer Medizingeräte, wobei die Frage nach gesetzlichen Pflichten nicht im Mittelpunkt steht. Als herstellendes Unternehmen wird hier die für die produktbezogenen Aufgaben technisch verantwortliche Stelle bezeichnet, besonders hinsichtlich der Gewährleistung der Sicherheit. Diese Aufgaben kann in bestimmten Fällen neben dem Inverkehrbringer auch ein vertraglich festgelegter Dienstleister wahrnehmen.

Unabhängig von der gesetzlichen Pflicht zur Beseitigung von Gefährdungen werden hier auch Prozesse für Schwachstellen betrachtet, die allgemein die Informationssicherheit (Vertraulichkeit, Verfügbarkeit, Integrität) von anderen Daten oder Funktionen im Medizingerät selbst oder von damit bestimmungsgemäß verbundenen Geräten und verbundener Infrastruktur (im Sinne einer Netzwerkverbindung) beeinträchtigen können.

Schutzziele

Für Medizingeräte erwarten Gesetzgeber, Betreibende, Anwenderinnen und Anwender sowie Patientinnen und Patienten verschiedene Schutzeigenschaften. Derzeit liegt der Schwerpunkt in der Gesetzgebung – etwa zum Marktzugang – noch auf Gefährdungsfreiheit (im Sinne des Schutzes der Gesundheit von Personen) sowie den Leistungsmerkmalen. Anwenderinnen und Anwender und Betreibende (und auch neuere Initiativen in der Gesetzgebung) erwarten darüber hinaus eine hohe Verfügbarkeit sowie eine Robustheit und Integrität des Medizingerätes in allen während zweckbestimmter Verwendung vorhersehbaren Betriebssituationen.
Im Zusammenhang mit der Unterstützung durch Software und Vernetzung hat sich weiterhin die Informationssicherheit – als Zustand des Schutzes vor den Folgen unautorisierter/unbeabsichtigter Zugriffe auf Medizingeräte (ISO 80001-1 / ISO 81001-1, IEC 62443-4-1) als Schutzeigenschaft etabliert, da sie besonders Verfügbarkeit, Integrität und Vertraulichkeit unterstützt, aber auch zur Gefährdungsfreiheit beiträgt.

In diesem Umfeld besteht eine erhebliche Unklarheit bezüglich der sinnvollen und angemessenen Reaktion der herstellenden Unternehmen auf die immer wieder bekanntwerdenden Meldungen zu Schwachstellen in der Software vernetzter Medizingeräte: Ist die Schwachstelle auch wirklich relevant in der vorhergesehenen Betriebsumgebung? Kann die Ausnutzung der Schwachstelle wirklich – im zweckbestimmten Einsatz – Gefährdungen oder Nichtverfügbarkeit des Medizingeräts bewirken? Welches Gefährdungsszenario ist eigentlich vorhersehbar im Sinne der Risikobetrachtung? Schließlich stellt nicht jede Schwachstelle in der Software eines Medizingerätes unmittelbar eine Erhöhung des Betriebsrisikos dar.

Begriff

Die Information über bekanntgewordene Schwachstellen der IT-Sicherheit wird im Dokument vereinfachend mit „Information“ bezeichnet.
Informationen werden den herstellenden Unternehmen durch eigene Nachforschungen, durch Meldungen von Anwenderinnen und Anwendern oder aber durch Meldungen Dritter bekannt. Diese Dritten können Behörden und unabhängige Sachverständige sein.

Im Sinne der Reduktion von Gefährdungsrisiken sowie der Erhaltung der zweckbestimmten Funktion gibt es durchaus Fälle, bei denen bekannte Schwachstellen weniger durch technische Maßnahmen im Produkt, als vielmehr durch Kommunikation, Dokumentation und organisatorische Maßnahmen beim Betreiber wirksam behandelt werden können. Grundsätzlich sind beide Formen dieser (d. h. technischen wie auch organisatorischen) korrigierenden Maßnahmen als gleichwertig anzusehen und sollten Inhalt entsprechender Warnmeldungen („Advisories“) der herstellenden Unternehmen sein.

Grundsätzlich gilt: Nur durch Transparenz und eine professionelle Einschätzung der Bedrohungslage nach geltenden Standards (CVSS, RUBRIC, in Beziehung zur Gefährdungsanalyse gemäß ISO 14971) wird auch die Anwendungs-/Betriebsseite in die Lage versetzt, eine fundierte Risikoanalyse und Risk Mitigation aufstellen zu können [MITRE-RUBRIC]. Risk Mitigation ist hier die Risikoabschwächung als Begrenzung oder Reduzierung der Eintrittswahrscheinlichkeit oder Auswirkung des zur Schwachstelle gehörigen schädlichen Szenarios.

Probleme

Anwendende, Sicherheitsforschende („Researcher“) und Behörden berichten von verzögerter, fehlender oder unzureichender Reaktion der herstellenden Unternehmen vernetzter Medizingeräte auf Informationen zu Schwachstellen. Herstellende Unternehmen berichten von rechtlichen und technischen Unklarheiten sowie organisatorischen Aufwänden bei der Annahme, Bewertung und Behandlung von Informationen. Konkret sind oder waren bei herstellenden Unternehmen beim Umgang mit Informationen zu Schwachstellen die folgenden Probleme zu beobachten:

- Fehlende oder unklare Kontaktstellen zur Annahme von Schwachstellen-Meldungen von Dritten, z. B. Sicherheitsforschenden. Dritte finden bei herstellenden Unternehmen kein Portal oder keinen Kontakt für Meldungen.
- Fehlende oder unklare Prozesse zur internen Ermittlung und Erkennung von relevanten Informationen über Schwachstellen. Meldungen aus dem Feld können oft nicht systematisch daraufhin untersucht und klassifiziert werden, ob die Abweichung ursächlich mit einer Schwachstelle verbunden ist. Schwachstellen-Informationen werden nicht als solche gekennzeichnet, weil Datenbanken und die Prozesse zur Einreichung sowie Abarbeitung von Produktmeldungen oft für die Behandlung von Gefährdungen („Safety“) optimiert sind. Mangels klarer Prozesse werden dabei Meldungen zu Informationssicherheit oft pauschal als „nicht-gefährdungsrelevant“ abgewiesen und nicht genau analysiert.
- Fehlende oder späte Rückmeldungen an Sicherheitsforschende (soweit bekannt), wenn sie nicht gerade Behörden oder Kundinnen und Kunden sind.
- Fehlende „Coordinated Vulnerability Disclosure“-Prozesse („CVD“) bei Zulieferern und Auftragnehmern („3rd-party manufacturer“), oft verbunden mit unvollständigen Konfigurationsdaten zu Software von Dritten.
- Unsystematisches Vorgehen bei der Ermittlung der von der Schwachstelle betroffenen Produkte (Typen). Der spätere Zugriff auf die Entwicklungsakten muss die Ermittlung aller Softwareversionen der Anwendung, jedoch auch der Versionen der verwendeten Software von Dritten, einschließlich der Software für Plattformen (Treiber, Datenbanken, Betriebssystemen etc.) ermöglichen.
- Aufwände und Verzögerungen bei der Ermittlung der von der Schwachstelle betroffenen Geräte (Instanzen) im Feld - insbesondere bei Altgeräten. Die Zuordnung von ausgelieferten Produkten und den darauf installierten Softwareversionen wird möglicherweise nicht systematisch unterstützt.
- Fehlende Benachrichtigung an Kunden. Es ist unklar, welche Art von Schwachstellen tatsächlich zu einer Information der Kunden führen sollten. Dazu müsste eine Risikobewertung aus Sicht der Informationssicherheit neben den Schutzzielen der Gefährdungsfreiheit und der wesentlichen Funktionen auch die Informationssicherheit sonstiger Funktionen und Daten berücksichtigen.
- Fehlende Abschlussbewertungen zur internen sowie zur externen Verwendung. Keine abschließende Dokumentation der Behandlung der konkreten Schwachstellen-Information.
- Fehlende Benachrichtigung („advisory“, „security bulletin“) der Öffentlichkeit.

- Fehlende oder ungenaue Meldungen an Behörden sowie Erfassung von „security updates“ als Produktaktualisierungen.
- Unsicherheit beim herstellenden Unternehmen in der Kommunikation mit Sicherheitsforschenden: Keine vertrauenswürdige Behandlung der Kommunikation, fehlende Rückmeldungen, keine Würdigung der Arbeiten der Sicherheitsforschenden.

Aktivitäten zur Behandlung von Informationen über Schwachstellen

Dieser Abschnitt enthält informative Hinweise zu einem Prozess zur umfassenden Behandlung von Meldungen über Schwachstellen.
Ausgangspunkt ist die vierte Empfehlung im ZVEI-Leitfaden „Medizintechnik braucht Cybersicherheit“: „Herstellende Unternehmen von Medizinprodukten sollten deshalb den regelmäßigen Austausch mit Anwendern zum Thema Cybersicherheit suchen. Die Erkenntnisse sollten in die Produktentwicklung und die Produktpflege zurückfließen“. Aus den sehr detailliert begründeten CERT-Richtlinien (SEI CMU, 2018) werden dazu diese Schritte empfohlen:

- Einrichtung und Bekanntmachung einer Kontaktstelle zur Annahme von Meldungen und umgekehrt zur Publikation von Informationen zu Produkten, Schwachstellen, Einschränkungen und Maßnahmen,
- zeitgerechte Antwort an den Berichtenden, Aufbau einer vertrauensvollen Zusammenarbeit,
- interne Identifikation einer Schwachstelle: Zusammenfassung der Berichte über zusammengehörige Szenarien, mit Bewertung der Quellen und des Zielprodukts, sowie eines Scores zu Schweregrad und Wahrscheinlichkeit (z. B. CVSS, CWSS, Medical RUBRIC inklusive Auswirkung auf “Safety” und den klinischen Arbeitsablauf),
- Priorisierung der Schwachstelle und Ressourcenplanung zur angemessenen Behandlung,
- systematische Ermittlung aller betroffenen Produkte in Entwicklung / Produktion und Wartung,
- Veröffentlichung einer produktbezogenen Information an Betreibende und Kundschaft,
- systematische Ermittlung der betroffenen Geräte-Instanzen im Feld,
- zeitnahe Benachrichtigung der Kundinnen und Kunden (eventuell der zuständigen Behörde und je nach Zweckbestimmung auch der Nutzerinnen und Nutzer / Patientinnen und Patienten) im Hinblick auf erkannte Gefährdungen und eventuell resultierende Einschränkungen der zweckbestimmten Funktion, zusammen mit Anweisungen zu externen Maßnahmen („compensating controls“),
- umfassende Gefährdungsanalyse (Threat / Risk Analysis) auf der Basis der aktualisierten vorhersehbaren Bedienung, gefolgt von einer Bewertung der Schwachstelle im Hinblick auf die Gesamtheit der Schutzziele, Ermittlung aller relevanten Angriffsszenarien und aller betroffenen Softwareelemente des Gesamt-Systems, Entwurf, Implementierung und Validierung einer Lösung im Rahmen der produktbezogenen Prozesse für die betroffene Software oder Dokumentation, Verteilung der Lösung im Feld. Dies beinhaltet eine Entscheidung, ob im Hinblick auf die vorgesehene Einsatzumgebung und die zweckbestimmte Verwendung als Lösung eine technische Implementierung, eine Änderung der Bedienungsanleitung, eine Information zu externen (auch: organisatorische) Maßnahmen oder eine Kombination dieser Maßnahmen, effektiv und sinnvoll ist.
- abschließende Publikation der Schwachstelle und der verfügbaren Lösungen, Verwendung einer externen Identifikation der Schwachstelle, beispielsweise als CVE bei MITRE oder den dafür autorisierten „CNA“; sowie Publikation einer Zusammenfassung der Schwachstelle und ihrer Lösung („vulnerability disclosure document“), zusammen mit einer öffentlichen Wertschätzung der Beiträge der beteiligten Sicherheitsforschenden („hall of fame“) [MITRE-CVE].

Abschließend sei darauf hingewiesen, dass diese Liste reaktiver Maßnahmen lediglich die „post-market security“ beschreibt und sowohl durch begleitende Maßnahmen („Vigilanz“) zu Gefährdungsfreiheit („safety“) als auch durch präventive Maßnahmen – etwa durch technische Maßnahmen im Produkt sowie durch regelmäßig an die aktuelle Informationssicherheit angepasste Testszenarien – unterstützt werden muss.

Prozesselemente

Offene und zielgerichtete Kommunikation über Schwachstellen, verbundene Risiken und resultierende Aktivitäten ist eine wirksame, aktive Maßnahme zur Risikominimierung. Ein zentraler Bestandteil dieser Kommunikation ist die Entgegennahme von Informationen von außerhalb der Organisation des herstellenden Unternehmens. Der hohe Stellenwert der Kommunikation im Umgang mit Informationen über Schwachstellen ist nachfolgend ersichtlich.

	Communicate	Analyse	Implement
Publish a coordinated vulnerability disclosure process	■		
Establish a public portal for accepting reports and for publishing product notifications, research receipts, vulnerability information, restrictions, and compensating controls	■		
Timely contact the researcher and provide a more detailed response, negotiate a non-disclosure grace time,	■		
Identify related vulnerability, target products, scores (e.g., CVSS, CWSS, Medical RUBRIC) [MITRE-RUBRIC] Contact the researcher during vulnerability analysis for clarification on steps needed to reproduce vulnerability	■	■	
Plan internal handling (e. g. priorities, resources), identify affected products, identify scenarios / analyse impact / hazard analysis		■	
If needed for own code: assign a CVE number and use it for reporting to MITRE and CERTs	■		
Identify affected product instances in the field and notify customers (technical administration contact)		■	
Perform systematic Threat/Risk Analysis, identify solution outlines (incl. compensating controls)		■	
Design solutions, inform the researcher of the remediation timeline (when to provide a patch or other means) to support coordinated disclosure efforts	■		■
Communicate solution to customers, In the customer-facing documentation related to the disclosure (e. g. security advisory), attribute the disclosure to the researcher after receiving proper consent from the researcher.	■		
Publish disclosure document (acknowledge researcher)	■		
Implement, document, deploy solution			■
List the researcher in an on-line recognition site, after receiving proper consent from the researcher, follow up (internal report)	■		

Referenzen

Allianz für Cybersicherheit, BSI, Bonn, https://www.allianz-fuer-cybersicherheit.de/

BSI CS132 Empfehlung: Hersteller – Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte, www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_132.pdf, BSI, Bonn, 2018

ISO/IEC 30111:2019, Information technology — Security techniques — Vulnerability handling processes, ISO, Geneva, 2019

IEC/ISO 62443-4-1 (DIN, EN, VDE 0802-4-1) IT-Sicherheit für industrielle Automatisierungssysteme; Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung

MITRE-CVE, "Common Vulnerabilities and Exposures," [Online]. Available: https://cve.mitre.org/

MITRE-RUBRIC, “Rubric For Applying CVSS To Medical Devices” [Online]. https://www.mitre.org/publications/technical-papers/rubric-for-applying-cvss-to-medical-devices
NL MoJS, National Cyber Security Centre: Coordinated Vulnerability Disclosure, www.enisa.europa.eu/news/member-states/WEB_115207_BrochureNCSC_EN_A4.pdf, Dutch MoJS, The Hague, 2018

SEI, The CERT Guide to Coordinated Vulnerability Disclosure, SEI, CMU, Pittsburgh, PA, 2017, resources.sei.cmu.edu/asset_files/SpecialReport/ 2017_003_001_503340.pdf

ZVEI-Positionspapier: „Medizintechnik braucht Cybersicherheit“, Fachverband Elektromedizinische Technik, Frankfurt a. M., 2017

Kontakt
Hans-Peter Bursig • Fachverbandsgeschäftsführer Elektromedizinische Technik • Fachverband Elektromedizinische Technik • Mobil: +49 162 2664 915 • E-Mail: hans-peter.bursig@zvei.org

Andreas Bätzel • Referent Innovation Medizintechnik und Gesundheitsmarkt • Fachverband Elektromedizinische Technik • Tel.: +49 69 6302 388 • Mobil: +49 162 2664 929 • E-Mail: andreas.baetzel@zvei.org

ZVEI e. V. • Verband der Elektro- und Digitalindustrie • Lyoner Straße 9 • 60528 Frankfurt am Main
Lobbyregisternr.: R002101 • EU Transparenzregister ID: 94770746469-09 • www.zvei.org

Datum: 12.07.2022