Expertenkreis CyberMed

SBOM für vernetzbare Medizingeräte

Einordnung der SBOM für die Informationssicherheit von vernetzbaren Medizingeräten

Abstract

Das folgende Dokument ist im Rahmen der Arbeit des EK CyberMed[1] entstanden und erhebt keinen normativen Anspruch. Diese Stellungnahme erläutert den Beitrag der Software Bill of Materials (SBOM) für die Informationssicherheit von vernetzten Medizingeräten.

Im Entwurf des neuen US FDA-Leitfadens zur Informationssicherheit[2] sowie des International Medical Device Regulators Forum (IMDRF)[3] ist vorgesehen, dass jeder Betreiber beim Bekanntwerden einer Schwachstelle („vulnerability“) geeignete Schutzmaßnahmen ergreifen sollte. Hierfür muss der Hersteller dem Betreiber eine SBOM zur Verfügung stellen, auf der alle Software-Komponenten aufgelistet sind. Zum Zeitpunkt der Veröffentlichung dieses Dokumentes, gibt der Teil 2 der Technischen Richtlinie TR-03183 „Cyber-Resilienz-Anforderungen“ (Version 1.0 vom 12.07.2023)[4] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) Anforderungen an eine SBOM vor. Durch die Übergabe der SBOM von allen vernetzbaren Medizingeräten an die Betreiber kann laut IMDRF WG/N73 die Informationssicherheit im Betrieb verbessert werden.

Die SBOM als produktbegleitendes Dokument zu vernetzbaren Medizingeräten kann als ein unterstützendes Element in allen Phasen des Lebenszyklus vernetzter Medizingeräte angesehen werden. Als einzelnes Dokument enthält die SBOM dabei lediglich die Bestandteile der Software und ist somit vergleichsweise statisch. Zur Etablierung effektiver Schutzmaßnahmen sollte die SBOM durch weitere produktbezogene Informationen, insbesondere der Bereitstellung von

[1] https://www.allianz-fuer-cybersicherheit.de/dok/13209480
[2] FDA-2021-D-1158, Titel: „Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions“
https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions
[3] IMDRF WG/N73 vom 1. Juli 2022 mit dem Titel: “Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity”
https://www.imdrf.org/consultations/principles-and-practices-software-bill-materials-medical-device-cybersecurity
[4] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03183/TR-03183_node.html

Schwachstellenmeldungen, von den Herstellern ergänzt und durch organisatorische Maßnahmen von Betreibern genutzt werden. Beispiele hierfür wären das Profil VEX[5] oder auch standardisierte, geräte-orientierte Nachrichten gemäß dem Standard CSAF[6]. Diese ermöglichen einen automatisierten Abgleich der SBOM mit den Schwachstellen und Mitigationsmaßnahmen.

Einführung

Derzeit bringen Gesetzgeber, unterstützt durch verschiedene Normen, für Medizingeräte die SBOM – eine strukturierte, maschinenlesbare Auflistung der im Gerät enthaltenen einzelnen Komponenten – als produktbegleitende technische Dokumentation ins Gespräch. Mit dem Begriff „Komponente“ werden in diesem Dokument Software und Software-Bibliotheken erfasst.

Nach Ansicht von Regulatoren hat die SBOM für Software im/als Medizingerät eine bedeutende Rolle als produktbegleitende Information. IMDRF und FDA schlagen vor, dem Betreiber die SBOM als standardisiertes, strukturiertes, elektronisches Dokument zum Medizingerät zur Verfügung zu stellen.

Dieses Dokument erklärt die Rolle der SBOM über die Phasen des Lebenszyklus vernetzter Medizingeräte.

Entwicklungsprozess

Innerhalb der Produkt-Entwicklung ist die SBOM als ein Element zur Dokumentation von verwendeten Komponenten und Lizenzen etabliert. Ferner wird diese von einschlägigen Werkzeugen generiert bzw. genutzt. Neben der genannten Auflistung der „obersten Integrationsebene“[7] aller (explizit) integrierten Komponenten müssen weitere Erwartungen mehrerer Regulatoren berücksichtigt werden.

Die in jeder Integrationsebene der SBOM enthaltenen Komponenten können wiederum iterativ aufgelöst und vollständig in die SBOM einbezogen werden.

Eine transparente und unter Abwägung der Informationssicherheit begründete Auswahl der enthaltenen Sub-Komponenten ist für Betreiber und Hersteller effizient und nützlich. Je nach Vernetzung verschiedener Hardware-Komponenten kann es sinnvoll sein, auch die dort programmierten Software-Einheiten in die SBOM mit aufzunehmen.

Die SBOM dient im Entwicklungsprozess als Hilfsmittel zur Identifizierung von Komponenten, für die Schwachstelleninformationen veröffentlicht wurden.

[5] VEX = vulnerability exploitability exchange
[6] CSAF = common security advisory framework
[7] Unter der obersten Integrationsebene ist die vollständige Auflistung aller obersten Abhängigkeiten der Software eines Medizinprodukts gemeint. Die meisten Komponenten auf dieser Ebene bestehen aus weiteren Teilkomponenten, die durchaus auch von anderen Herstellern zugeliefert werden (oder auch Open Source sein) können.

Konformitätsbewertung

Im Zusammenhang mit der Einreichung zur Konformitätsbewertung können sowohl der Hersteller als auch die prüfende Stelle[8] anhand der SBOM die Aktualität der verwendeten Komponenten und deren Cybersicherheit im Medizingerät einschätzen.

Die in dem Entwurf des US FDA-Leitfadens zur Informationssicherheit formulierte Anforderung zur begleitenden Auflistung der zum Zeitpunkt der Einreichung bekannten Schwachstellen - als ergänzende Information mit Bezug für jeden Eintrag der SBOM - geht weit über die ursprüngliche Idee der SBOM hinaus. Hierdurch wird der statische Charakter der SBOM um eine variable Komponente erweitert, die getrennt durch dynamische Systeme (z.B. CSAF / VEX siehe Beschreibung weiter unten) bereitgestellt werden sollten. Bei der Einreichung von Unterlagen zur Konformitätsbewertung mit einer solchen Schwachstellen-Auflistung ist auf den jeweiligen zeitlichen Bezug hinzuweisen.

Im Hinblick auf die Gefährdungsfreiheit des Gesamtsystems „Medizingerät“ ist hierbei allerdings unbedingt zu beachten, dass die Aktualität einer Komponente nicht zwangsläufig eine Aussage über mögliche Verwundbarkeiten oder Sicherheit macht. Vorherige Versionen könnten stabiler sein; auch könnten Erweiterungen in neueren Versionen bekannt für Verwundbarkeiten sein. Eine pauschalisierte Aussage, dass nur aktuelle Software sicher (hier: gefährdungsfrei) sei, ist somit nicht korrekt. Generell besteht vielmehr die Empfehlung zur Nutzung von Versionen, die aus Systemsicht stabil und frei von Verwundbarkeiten sind. Dies gilt es während der Konformitätsbewertung zu beachten.

Beschaffung

Die SBOM kann in der Beschaffungsphase als Teil der technischen Produktbeschreibung dem anfragenden Kunden (ggf. mit Vertraulichkeitserklärung) einige Anhaltspunkte für die zu erwartenden Aufwände zur Einhaltung der sicheren, bestimmungsgemäßen Vernetzung geben. Während die Fragen nach der medizinischen Wirksamkeit und der Reduktion der Gefahren in anderen regulatorischen Einreichungen beschrieben werden, kann die SBOM den Betreiber darüber hinaus beim IT-Risikomanagement unterstützen, allerdings gelingt dies nur in Verbindung mit entsprechenden produktspezifischen Informationen.

Zum Begriff der Vernetzung ist anzumerken, dass aus der Sicht der Informationssicherheit der Austausch von Speichermedien oder die gelegentliche Vernetzung zu Wartungszwecken auch generell als „Vernetzung“ zu betrachten sind.

Die SBOM enthält sensible Details zum Aufbau eines Produktes und damit geistiges Eigentum des Herstellers, welches im Missbrauchsfall auch potentiellen Angreifern hilfreich sein kann. Alle Beteiligten haben damit verantwortungsvoll umzugehen. Dazu könnten Aspekte sicherer Übertragungswege, gesicherter Ablage und der Zugriffskontrolle beim Betreiber gehören.

Die konkreten Auswirkungen einer Schwachstelle (einer in der SBOM gelisteten Komponente) auf die Sicherheit und zweckbestimmte Funktion des Medizingerätes, kann nur der Hersteller in weiteren Dokumenten (‚VEX‘ oder Security Advisory, siehe Beschreibung weiter unten) feststellen. Diese Dokumente ergänzen die SBOM, die alleine keine hinreichenden Angaben in Bezug auf eine Schwachstellen-Risikobewertung enthält.

[8] Benannte Stelle, Aufsichtsbehörde

Inbetriebnahme, Änderungen und Außerbetriebnahme

Die wirksame Nutzung der SBOM kann grundsätzlich nur auf der Grundlage einer detaillierten und aktuellen Geräteverwaltung[9] des Betreibers funktionieren. Insbesondere müssen für vernetzbare Medizingeräte oder vernetzte Geräte, auf denen Software installiert und betrieben wird, welche als Medizingerät klassifiziert wurden, für jedes einzelne Gerät die Software-Konfiguration, -Produkte, entsprechende Versionen, Standort und eine Geräte-Identifikation aktuell gehalten werden, um genau zu erkennen, welches konkrete Medizingerät wirklich betroffen ist. Updates, Upgrades sowie Außerbetriebnahmen müssen nachvollziehbar dokumentiert und die jeweils entsprechenden SBOM(s) vorgehalten werden, ggf. auch in unterschiedlichen Versionen.

Angesichts einer Vielzahl von vernetzbaren Medizingeräten in typischen klinischen IT-Netzen besteht die Erwartung, dass die SBOM-Dokumente in einem einheitlichen Format, vor allem maschinenlesbar, um eine automatisierte oder softwareunterstützte Auswertung zu ermöglichen, übermittelt werden.

Oft unbeachtet bleibt das Fehlen einer eindeutigen, über der Zeit stabilen, Identifikation von Software- und Hardwarekomponenten, was besonders bei atypischen / unbekannten Komponenten leicht dazu führt, dass Schwachstellen-Meldungen nicht zugeordnet und erkannt werden können[10]. Für hinreichend weit verbreitete Komponenten werden CPE IDs[11] vergeben. Diese sind jedoch nicht immer eindeutig, vor allem wenn mehrere Komponenten mit verschiedenen CPE IDs im selben Produkt enthalten sind.

Die Nutzungsdauer von Medizingeräten ist meist deutlich länger, als manche externe Sub-Komponenten gewartet werden. Daher kann eine SBOM den Herstellern dabei helfen, relevante Änderungen von externer Sub-Komponenten den betroffenen Medizingeräten zuzuordnen und entsprechende Risiko-Analysen zu initiieren (siehe MDCG 2019-16).

[9] IT Asset Management

[10] Gerade bei proprietären Produkten ist die Informationsgewinnung über mögliche Verwundbarkeiten schwierig. Dabei sind Hersteller der Medizinprodukte auf die Informationsweitergabe durch ihre Vertragspartner oder Entwickler angewiesen. Zwar können bei kritischen Komponenten, Entwicklungsprozesse und Unternehmen auditiert werden. Dies kann aber nur begrenzt Aufschluss zu der Umsetzung bei einem realen Vorfall geben.

[11] common platform enumeration IDs

Regulärer Betrieb

Dieser Abschnitt beschreibt die Rolle der SBOM in der zweckbestimmten, vernetzten Anwendung, soweit noch Wartungspflichten[12] des Herstellers für das Medizingerät bestehen (siehe dazu Abbildung 1[13]). Idealerweise wird ein Betreiber im Fall des Bekanntwerdens einer Schwachstelle einer auf der SBOM gelisteten Komponente in die Lage versetzt, unverzüglich Abwehrmaßnahmen für die betroffenen Medizingeräte zu ergreifen.

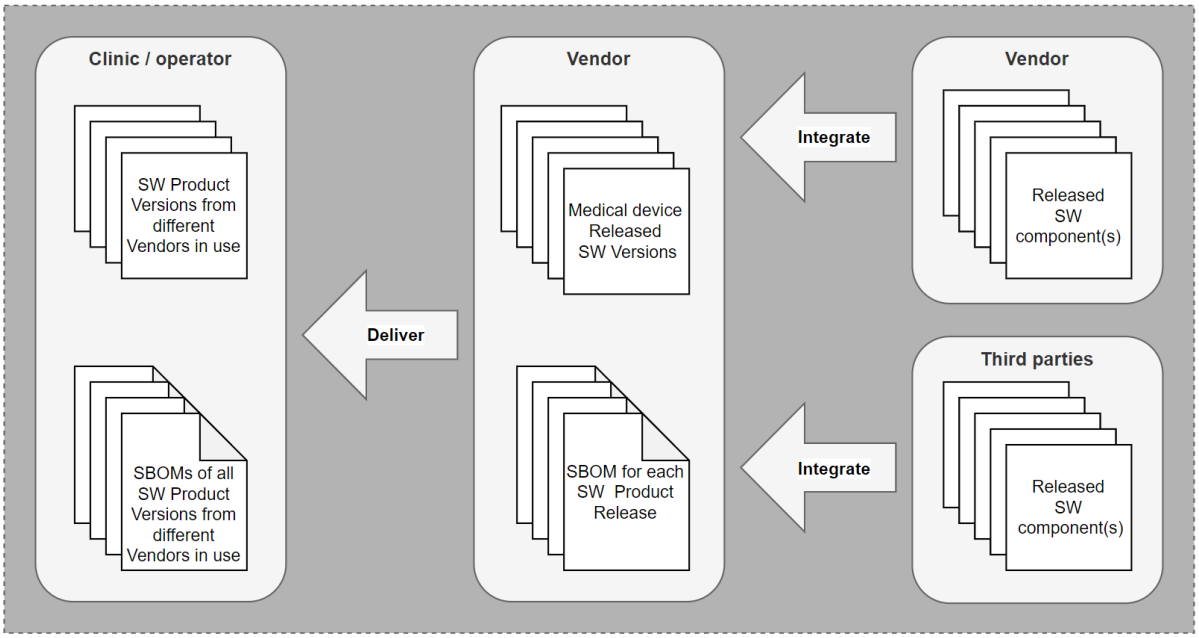

Abbildung 1: Entstehung, Übermittlung und Nutzung der SBOM

Es besteht allerdings das Problem, dass durch die bloße Auflistung einer Komponente mit einer danach bekanntgewordenen Schwachstelle die konkreten Auswirkungen auf die Funktion und die Patientensicherheit vollkommen unklar sind. Es kann sein, dass die angreifbaren Funktionen der Komponente vom Medizingerät gar nicht genutzt werden. Darüber hinaus kann es sein, dass die Architektur und Realisierung oder die Art der Netzintegration des Medizingerätes beim Betreiber einen möglichen Angriff verhindern und dessen Auswirkung abfangen würden.

Es lässt sich also festhalten, dass im regulären Betrieb der durch die SBOM alarmierte Betreiber die eventuell verfügbaren internen Schutzmaßnahmen (Patches für die betreffende Komponente im Medizingerät) nicht einrichten darf und wirksame externe Schutzmaßnahmen nicht einrichten kann, da in beiden Fällen eine konkrete herstellerseitige Information fehlt.

Der Hersteller, der unabhängig vom SBOM-Dokument eine Schwachstelle für seine Medizingeräte meldet, ist, soweit die Allgemeinen Anforderungen der Medical Device Regulation (MDR) bezüglich der Medizingerätezulassung betroffen sind, hingegen zur Veröffentlichung entsprechender Maßnahmen („mitigations“) an den Betreiber verpflichtet[14].

Der Begriff *vulnerability* wird in den Dokumenten der IMDRF als „ausnutzbare Schwachstelle“ definiert, wobei für Medizingeräte klar zu unterscheiden ist zwischen der Ausnutzbarkeit aus Sicht der Komponente (identifiziert über die SBOM) sowie einer möglicherweise resultierenden

[12] Post market obligations
[13] Quelle: A. Lämmerzahl, Eckental
[14] Siehe hierzu EU-MDR - Anhang 1, 4., 14., 17. ff.

Ausnutzbarkeit aus Sicht des Medizingerätes, die sich keinesfalls zwingend ergibt und letztendlich nur auf der Basis einer herstellerseitigen Bewertung festgestellt werden kann.

Noch vielfältiger sind die Interpretationen des *Risiko*-Begriffs. Hier können Funktions-einschränkungen der einzelnen Komponente, des Medizingerätes, der klinischen Integration aber auch mögliche physische Gefährdungen gemeint sein.

Behebung bekannter Schwachstellen

Hierbei stehen unterschiedliche Möglichkeiten zur Verfügung:

- Patch des gesamten Medizinproduktes auf eine vom Hersteller freigegebene Version (Produkt-Patch)
- Behebung durch Patch für eine einzelne Komponente (Komponenten-Patch)
- Maßnahmen an der IT-Infrastruktur / Nutzungsumgebung (Härtung).

Allen Maßnahmen ist gemeinsam, dass sie nur unter Berücksichtigung der Effektivität und Sicherheit des Medizinproduktes angewendet werden dürfen. Die Kommunikation mit dem Hersteller ist dabei von zentraler Bedeutung.

Produkt-Patch

Idealerweise steht eine aktuellere Version oder ein Patch für das Medizingerät zur Verfügung, der vom Hersteller freigegeben wurde und die Schwachstelle behebt. Dieser sollte zeitnah und vollständig eingespielt werden.

Anmerkung: Insoweit dies externe Maßnahmen einschließt (z. B. Abschaltung von Protokollen oder Ports für jedes betroffene Produkt), ergeben sich regelmäßig Inkonsistenzen und oft auch Funktionseinschränkungen im Geräteverbund.

Komponenten-Patch

Eine häufig empfohlene Abhilfe nach dem Bekanntwerden einer Schwachstelle ist das Installieren einer für die betroffene Komponente verfügbaren Modifikation („patch“) – soweit technisch im Einzelfall möglich. Die Freigabe „bei Verfügbarkeit“ muss ein Betreiber für die einzelne Komponente entscheiden – unter angemessener Berücksichtigung resultierender Risiken bezüglich der sicheren und bestimmungsgemäßen Verwendung des Medizingerätes. Dabei ist einerseits zu beachten, dass Modifikationen durch (nicht vom Medizingeräte-Hersteller freigegebenen) Patches am Medizingerät dessen weitere Betriebsverantwortung dauerhaft und umfassend auf den Betreiber verlagern. Andererseits können die Schwachstelle und deren Folgen beim Betreiber nunmehr durch die bloße Kenntnis der SBOM als "vorhersehbar" aus der Sicht des Betreibers betrachtet werden, sodass auch bei Nichthandlung durch unterlassene Schutzmaßnahmen beim Betreiber ebendort für etwaige Folgen eine (Mit)haftung abgeleitet werden kann. Explizit sei jedoch noch einmal darauf hingewiesen, dass ein Betreiber auf Basis einer SBOM in der Regel nicht automatisch die Auswirkungen einer Schwachstelle ableiten kann. Dafür fehlen die Informationen über die Verwendung der verwundbaren Funktionen.

Die betreiberseitigen Risiken eines Komponenten-Patches und die naheliegende Lösung, den Hersteller zur rechtzeitigen Bereitstellung von Produkt-Patches zu veranlassen, stellen den Nutzen eines Komponenten-Patches basierend auf der SBOM in Frage.

Härtung

Unter dem Gesichtspunkt der zeitnahen und sicheren Reaktion auf bekannt gewordene Schwachstellen, lässt die Kenntnis der SBOM genaugenommen nur externe Schutzmaßnahmen zu. Der Betreiber muss durch externe, technische Härtung oder durch Einschränkung der Nutzung des Medizingerätes die Auswirkungen der Angriffe auf die Schwachstelle reduzieren oder die Möglichkeit solcher Angriffe erschweren, soweit dies in Bezug auf die Zweckbestimmung des Medizingerätes möglich ist. Auch hierbei ist die Kommunikation mit dem Hersteller wichtig. Dies gilt insbesondere deshalb, weil getroffene IT-Sicherheitsmaßnahmen nicht zur Beeinträchtigung des klinischen Betriebes führen dürfen, auch wenn eine Risikobewertung der Maßnahmen keine unmittelbare Gefährdung der Effektivität und Sicherheit des Medizingerätes im netzgebundenen Betrieb erkennen lässt.

Die Betrachtung der unterschiedlichen Möglichkeiten zur Behebung bekannter Schwachstellen hat gezeigt, dass die SBOM als einzelnes Dokument sowohl bei der Abschätzung als auch bei der Behebung der Bedrohung unzureichend ist. Sie sollte durch weitere produktbezogene Informationen ergänzt werden. Hier helfen Hinweise gemäß VEX oder auch standardisierte, geräte-orientierte Nachrichten gemäß CSAF dem Betreiber deutlich mehr.

Betrieb von älteren Medizingeräten

Insoweit durch Abkündigung der Wartung und durch Ablauf gesetzlicher Pflichten der Hersteller eines vernetzten Medizingerätes keine Überwachung oder Abmilderung von Schwachstellen der Informationssicherheit des alten Medizingerätes mehr vornimmt, erhöhen sich beim Betreiber die Pflichten bezüglich der Erhaltung des sicheren Betriebs dieses Gerätes.

In dieser Situation ist die produktbegleitende SBOM ein grundsätzlich hilfreiches Instrument, um die Möglichkeit der Auswirkung einer Schwachstelle auf die sichere Funktion und Wirksamkeit, jedoch auch auf die Informationssicherheit der Vernetzung an sich, zu gewährleisten. Darauf weist auch schon IMDRF WG/N70 zu „Legacy“ hin.

Fazit

Die SBOM als produktbegleitendes Dokument zu vernetzbaren Medizingeräten kann als ein unterstützendes Element in der IT-Risikobehandlung der Betreiber von Medizingeräten angesehen werden, insbesondere, wenn für „alte Medizingeräte“ die Informationssicherheit weitgehend beim Betreiber liegt. Wichtig ist hier, dass die SBOM-Dokumente in einem einheitlichen, maschinenlesbaren Format übermittelt werden, um eine automatisierte oder softwareunterstützte Auswertung zu ermöglichen. Eine manuelle Erfassung und Verwaltung von SBOM-Dokumenten, vor allem in heterogenen Gerätelandschaften, ist effektiv nicht umzusetzen.

Die SBOM kann den Herstellern helfen, Schwachstellen in ihrem Produktportfolio zu erkennen. Des Weiteren kann diese im Rahmen der Betriebsverantwortung unterstützen, Schwachstellen-Probleme im Gerätebestand zu erkennen. Hierdurch werden mögliche technische Gegenmaßnahmen an den jeweiligen Medizingeräten im Rahmen des Betreiber-Risikomanagements eingeordnet und umgesetzt.

Betreiberseitig erfüllt die SBOM den gewünschten Zweck lediglich in Verbindung mit einer effektiven Geräteverwaltung und begleitenden Prozessen. Geräte mit potentiellen Schwachstellen können auf diese Weise – auch ohne Mitwirkung des Herstellers – schnell identifiziert werden. Die Identifikation und Härtung der betroffenen Geräte scheint der primäre Zweck der SBOM zu sein. Da die SBOM als alleiniges Dokument an sich sowohl bei der Abschätzung als auch bei der Behebung der Bedrohung unzureichend ist, sollte sie durch weitere produktbezogene Informationen und betreiberseitige Prozesse ergänzt werden.