Cybersicherheit von medizintechnischen Geräten

Die Software-Bill-of-Materials (SBOM)

Die MedTech-Industrie steht im Spannungsfeld zwischen hohem Innovationsdruck und wachsendem gesetzlichen Regelwerk. Das betrifft auch die Cybersicherheit der Medizin-Geräte. Kein Wunder, dass die Software-Bill-of-Materials (SBOM) im Pflichtenheft von Herstellern mittlerweile einen festen Platz einnimmt.

© Unsplash/ BoliviaInteligente; CC0-Lizenz

Das Gesundheitswesen ist ein lohnendes Ziel für Cyberattacken, vernetzte medizinische Geräte sind ein häufiges Einfallstor für Ransomware-Angriffe und Datendiebstahl. Ein Großteil der Sicherheitsvorfälle ist dabei auf bekannte Schwachstellen in der Software bzw. Sicherheitslücken auf Codeebene zurückzuführen. Deren Zahl nimmt kontinuierlich zu: So zählten Analysten von Revenera 2022 durchschnittlich 282 Schwachstellen pro Audit, ein Anstieg von 217 Prozent im Vergleich zum Vorjahr. Von den aufgedeckten Schwachstellen stellten 27 Prozent ein „hohes" CVSS-Risiko dar (Common Vulnerability Scoring System) - und damit eine unmittelbare Bedrohung für IT-Sicherheit und Cyberschutz.

© Nicole Segerer

Autorin:
Nicole Segerer
SVP & General Manager
Revenera
www.revenera.de

Wachsende Compliance für Softwareentwicklung

Entsprechend stark haben sich Gesetzgeber, Industrie-Verbände und Aufsichtsbehörden in den letzten Jahren für höhere Sicherheitsvorkehrungen in der Softwareentwicklung eingesetzt. Die FDA (The Food and Drug Administration) zum Beispiel arbeitet seit Jahren an einem verbindlichen Regelwerk, um Medizinprodukte vor Cyberangriffen zu sichern und die Transparenz entlang der Software Supply Chain zu erhöhen. Mit ihrem neueste Entwurf zur Cybersecurity in Medical Devices führt die US-Behörde unter anderem ein neues Konzept des Secure Product Development Framework (SPDF) ein. Ähnliche Initiativen finden sich in der EU. Sowohl MDR als auch IVDR haben die Cybersicherheit von Medizinprodukten auf der Checkliste. Mit dem ersten Verordnungsentwurf des EU Cyber Resilience Act (CRA) sollen Software-Hersteller zudem noch stärker in die Pflicht genommen werden. Das betrifft zum einen die Bereitstellung von Sicherheitsupdates, zum anderen einen Einblick darüber, welche Produkte von bekannten Schwachstellen überhaupt betroffen sind.

Wissenslücken entlang der Software Supply Chain

Wie aber lässt sich eine solche durchgehende Transparenz auf Code-Ebene sicherstellen? Die Software Supply Chain ist komplex. Es gibt kaum eine Anwendung, die von Grund auf „neu" geschrieben wird. Vielmehr greifen Entwicklerteams auf Tausende von Komponenten aus unterschiedlichen Quellen zurück – angefangen bei proprietärem Code über eingekauften Code von Partnern und Drittanbietern bis hin zu Open Source-Repositories im Netz. So bestehen kommerzielle Anwendungen heute aus bis zu 90 % aus Open-Source-Software (OSS).

Eine lückenlose und einheitliche Dokumentation über die einzelnen Software-„Bestandteile" – wie sie etwa in der Automotive oder Lebensmittelindustrie vorgeschrieben ist – liegt dabei nur selten vor.

Tatsächlich klafft zwischen den in Audits entdeckten und den von Unternehmen dokumentierten OSS-Komponenten eine wachsende Kluft. Das macht es sehr schwierig, die Codebausteine zurückzuverfolgen und dringende Fragen hinsichtlich ihrer Sicherheit und Compliance zu beantworten.

- Wer hat den Code geschrieben?
- In welchen Anwendungen und Geräten wird dieser eingesetzt?
- An welche Lizenzvorgaben ist die Nutzung gebunden?

Software-Bill-of-Materials (SBOM)

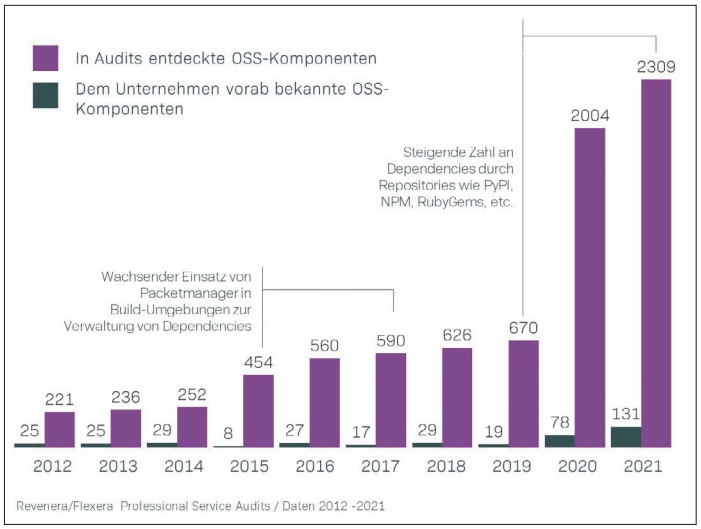
In diesem Zusammenhang entwickelt sich die Software-Bill-of-Materials (SBOM) zum Kernelement von Compliance-Programmen. Sie ist mittlerweile in Kaufverträgen und Request for Information (RFIs) zu finden und wird im Rahmen der Pre-Market-Submission verlangt. Die detaillierte Auflistung aller in einer Software eingesetzten Code-Komponenten soll helfen, den Überblick zu bewahren. Sicherheitsteam können so schneller überprüfen, ob eine Anwendung von neu veröffentlichten Sicherheitslücken und Exploits betroffen ist. Die SBOM gibt dabei nicht nur Aufschluss über die jeweiligen Codebasen, einschließlich Lizenzierung, Versionen und Herkunft. Auch die Beziehungen innerhalb der Softwarelieferkette werden offengelegt. Aufgeführt finden sich Pakete und Abhängigkeiten, Binärdateien ohne Manifest-Dateien, Multimedia-Dateien, Bilder/Icons, Codecs und Copy/Paste-Codes sowie die von den Entwicklern genutzten Source Libraries und Drittanbieter-Bibliotheken.

Minimalkriterien für SBOMs

Die SBOM beginnt in der Regel als eine einfache Liste der Top-Level-Komponenten. Dieser erste Basissatz an Daten kann bereits wichtige Informationen enthalten, die sich schnell an Stakeholder (z. B. IT-Sicherheit) weitergegeben lassen. Danach lässt sich die Liste Schritt für Schritt mit zusätzlichen Daten anreichern, einschließlich den jeweiligen Subkomponenten. Die Detailtiefe ist bei mehrstufigen und weit verzweigten SBOMs durchaus komplex. Sie ist aber notwendig. Denn selbst wenn eine Subkomponente für die Funktionalität einer Anwendung oder eines Geräts nur eine geringfügige Rolle spielt, kann in ihr doch eine kritische Schwachstelle stecken.

Was wird in einer SBOM aufgelistet

Welche Daten genau in welchem Umfang in einer SBOM aufgelistet sind, hängt von der Anwendung ab und wo sie zum Einsatz kommt. In der sicherheitskritischen Medizintechnik sind die Anforderungen naturgemäß hoch. Die FDA legt in ihren Leitlinien zum Beispiel großen Wert auf die Erstellung einer SBOM und betrachtet Änderungen an ihr als Teil der Design History File (21 CFR 820.30) und des Device Master Record (21 820.181). Hinsichtlich des Formats können Her-



Open Source Report 2022 © Revenera

steller auf gängige Branchen-Standards zurückgreifen – vorausgesetzt, diese decken die folgenden Datenfelder ab:

- das Gerät/System/Asset, in der/denen sich die Softwarekomponente befindet,
- der Name der Softwarekomponente,
- die Version der Softwarekomponente,
- der Hersteller/Autor der Softwarekomponente,
- der Grad des Supports hinsichtlich Überwachung und Wartung seitens des Herstellers der Softwarekomponente,
- das Datum, an dem der Support für die Softwarekomponente endet, und
- alle bekannten Schwachstellen.

Best Practices und Standards

Auch wenn diese Liste auf den ersten Blick sehr geradlinig erscheint, sind Herausforderungen vorprogrammiert. Informationen zu Software-Komponenten werden entlang der Software Supply Chain von verschiedenen Stakeholdern auf unterschiedliche Art und Weise weitergegeben. Die Angaben stimmen oft nicht überein, weisen Lücken auf oder sind schlichtweg nicht recherchierbar. In den letzten Jahren haben sich jedoch einige Best Practices und Standards etabliert, die bei der Erstellung von SBMOs helfen.

Hilfreich sind zum Beispiel die ISO/IEC 5230:2020 and ISO/IEC DIS 18974 Standards des von Linux ins Leben gerufene OpenChain Projects, die sich mit der Nutzung von OSS-Komponenten in Software befassen. Darüber hinaus bietet das NIST Secure Software Development Framework (SSDF) umfassende Anleitungen für Unternehmen, um das Risikomanagement von Software und software-gestützten Geräten zu verbessern. Den einen formalen Aufbau einer Software-Stückliste, der von allen Entwicklern und Herstellern einheitlich verwendet wird, gibt es leider nicht. Als anerkannte Standardformate gelten jedoch beispielsweise SPDX (z. B. von Microsoft genutzt) und CycloneDX (z. B. von Siemens genutzt).

Grundlegende Punkte

Darüber hinaus sollten Hersteller bei der Erstellung einer SBOM einige grundlegende Punkte beachten:

- Ein zentrales Kriterium der SBOM ist ihre Aufbereitung. Der Datensatz sollte maschinenlesbar, formal und hoch-strukturiert sein, um einen hohen Automatisierungsgrad sicherstellen zu können. In der Regel übernehmen dann Tools das Auslesen und Erstellen von SBOMs, scannen die Listen nach Sicherheits- und Compliance-Verstößen und gleichen diese mit dem Software-Code ab. Strukturierte Datenformate und Austauschprotokolle sind daher Grundmerkmale einer funktionalen Software-Stückliste.
- Eine SBOM allein ist nur eine lange Aufzählung an Komponenten. Relevanz und Praktikabilität für die IT-Sicherheit gewinnt sie erst, wenn sie mit entsprechenden, sicherheitsrelevanten Daten kombiniert wird. Idealerweise finden sich diese Daten in einem separaten, dazugehörigen Dokument, das eine aktuelle Momentaufnahme zeigt und sowohl entsprechende Querverweise zu den in der SBOM aufgelisteten Code-Komponenten als auch den notwendigen Kontext liefert (z. B. Vulnerability Disclosure Report (VDR) und Vulnerability Exploitability eXchange (VEX)). Als Sicherheits-Instrument lässt sich die SBOM dann auch in die Threat Intelligence integrieren, wo sie beispielsweise einen schnellen Abgleich mit Schwachstellen, Datenleaks oder Exploits im Darknet ermöglicht.
- Stücklisten sind so dynamisch wie die Software, die sie beschreiben. Eine kontinuierliche Überprüfung und Aktualisierung der SBOM ist daher wesentlich. Oft nutzen Hersteller ein neues Release, um die Stückliste auf den neuesten Stand zu bringen. Auf jeden Fall aber sollte das Update in regelmäßigen und klar abgesteckten Zeiträumen stattfinden. In manchen Fällen bestimmten auch Vertragsvereinbarungen mit Kunden sowie Compliance-Richtlinien den Zyklus.
- Das Erstellen, Managen und Überwachen von SBOMs verlangt neben Expertise und Training auch Ressourcen. Mehr und mehr Unternehmen setzen daher dezidierte Teams für diese Aufgaben ein. Das Open Source Program Office (OSPO) beispielsweise arbeitet mit anderen Abteilungen (z. B. Recht, Entwicklung, Produktmanagement, Sicherheit) zusammen, um Richtlinien für den sicherheitskonformen Umgang von Open-Source-Code zu implementieren. Ein Open Source Review Boards (OSRB) verfeinert die definierten Workflows dann in der Praxis.

Fazit

Die SBOM entwickelt sich immer mehr von der Kür zur Pflicht. Über kurz oder lang wird sie wohl in allen Branchen und Märkten zum festen Bestandteil der Softwareentwicklung und Cybersicherheit. Je früher die Hersteller beginnen, Prozesse zu definieren, Richtlinien zum Umgang mit Open Source festzulegen und ihre Softwareprodukte mit einer Auflistung aller Komponenten auszustatten, desto besser.

Wer schreibt:

Nicole Segerer blickt auf über 15 Jahre Erfahrung in den Bereichen Softwareproduktstrategie und Marketing zurück. Bei ihr dreht sich alles um die Analyse von Softwareprodukten und darum, den Mehrwert der Lösungen sowie das Kundenerlebnis zu steigern. Als SVP und General Manager von Revenera bei Revenera unterstützt sie Softwareanbieter und IoT-Hersteller bei der Umstellung auf neue digitale Geschäftsmodell und der Optimierung der Softwaremonetarisierung. ◄

SBOM Kreislauf © Revenera