Software Composition Analysis

Cybersecurity von Medizinprodukten auf Code-Ebene

© shutterstock/Khakimullin Aleksandr

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

Der Softwareanteil in Medizinprodukten wächst und damit auch die Anforderungen an die Cybersicherheit. Der Katalog an Datenschutzbestimmungen und Dokumentationspflichten drängt Hersteller zu umfassenden Prozessen der IT-Sicherheit. Software Composition Analysis ist dabei ein Grundbaustein.

Ob Herzschrittmacher, Insulinpumpen oder CT-Systeme – sobald Medizinprodukte in ein IT-Netzwerk eingebunden sind, stellen sie im Rahmen der Cybersicherheit ein Risiko dar. Mit zunehmender Digitalisierung hat sich die Angriffsfläche in den letzten Jahren massiv vergrößert. Im Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) gehen jedes Jahr rund 35.000 Risikomeldungen [1] ein – darunter auch IT-Sicherheitsvorfälle (Bild 1).

Compliance-Katalog – eine Auswahl

Hersteller müssen einen formalen Nachweis über die Sicherheit ihrer Medizinprodukte erbringen. Von Seiten des Gesetzgebers gibt es eine ganze Reihe an Leitfäden, regulatorische Frameworks und Meldekriterien zu beachten – sowohl auf nationaler als auch internationaler Ebene.

In der EU sind die Cyberschutz-Anforderungen vor allem über die Medizinprodukteverordnung (MDR) sowie die In-vitro-Diagnostika-Verordnung (IVDR) abgedeckt. Die MDR verlangt so ausdrücklich eine „State-of-the-art"-Softwareentwicklung, die IT-Sicherheit garantiert – Datenschutz und Schutz vor unberechtigtem Zugriff miteingeschlossen. In Deutschland stellt das BSI (Bundesamt für Sicherheit in der Informationstechnik) wichtige Dokumente zu den Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte [2] zur Verfügung und verweist darüber hinaus auf branchenübergreifende Vorgaben und Standards.

Cyber Resilience Act

Cyberschutz betrifft nicht allein die Medizintechnik. MedTech-Unternehmen müssen vielmehr tief in den Compliance-Katalog eintauchen, um auch implizit geltende Regulatorien zu erfüllen. Der Cyber Resilience Act (CRA) [3] der EU beispielsweise beschränkt sich nicht auf eine Branche, sondern lässt sich als allgemeine Richtschnur für Best Practices in unterschiedlichsten Anwendungsfelder verstehen. Ähnliches gilt auch für die Richtlinie NIS2 [4], die von der EU Ende 2022 auf den Weg gebracht wurde und nun innerhalb von 21 Monaten in nationales Recht überführt werden muss.

FDA und Cybersecurity

Im globalen MedTech-Markt ist zudem der Blick über den eigenen Rechtsrahmen hinaus zentral. Die FDA (Federal Drug Administration) in den USA zum Beispiel veröffentlicht in mehreren Leitfäden sehr konkrete Anforderungen zum Thema Cybersecurity. Das neueste Dokument (Sep. 2023) [5] beinhaltet unter anderem ein Framework für die sichere Entwicklung von Medizinprodukten. Seit Dezember 2023 verpflichtet außerdem die US-Börsenaufsichtsbehörde SEC [6] Unternehmen dazu, ihre Strategie für das Risikomanagement im Geschäftsbericht offenzulegen. Cybersecurity-Fälle sind darüber hinaus innerhalb weniger Tage zu melden.

Sicherheitsdokumentation beginnt auf Codeebene

Generell gilt: Hersteller sind für die Sicherheit der Software in ihren Produkten verantwortlich. „Security by Design" integriert die Sicherheit in das Produktdesign sowie in die Produktarchitektur. „Security by Default" verlangt eine Erst-Implementierung von Lösungen auf hohem Sicherheitsniveau, das sich nur im Nachgang durch das Konfigurieren von

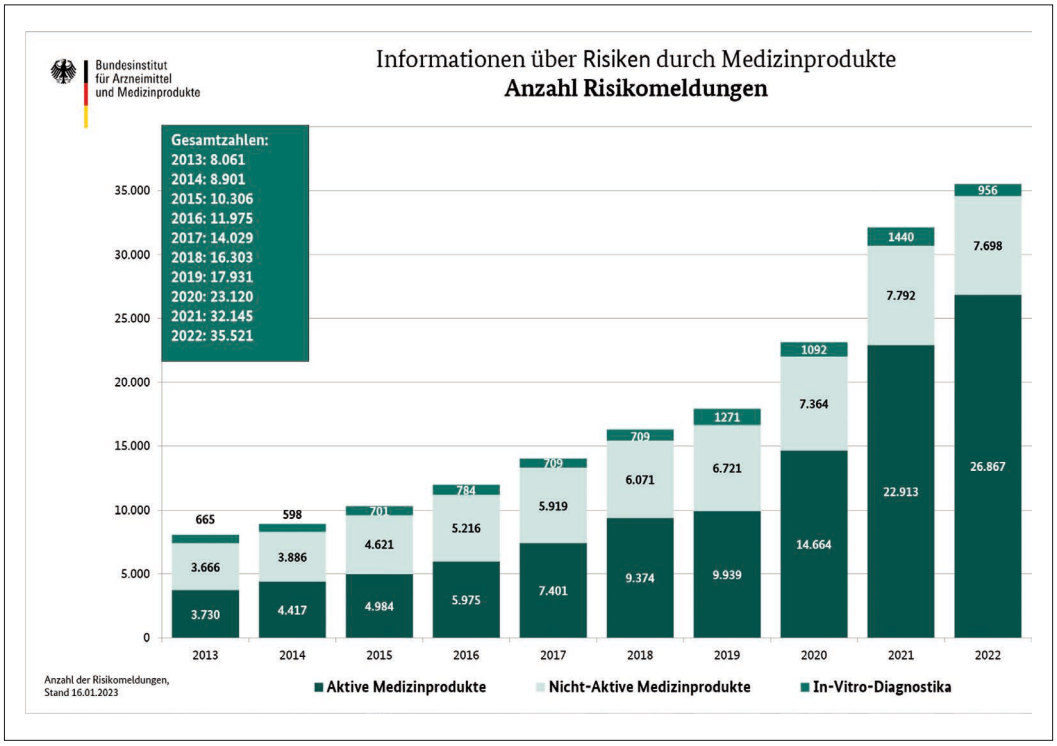

Bild 1: Kontinuierlich wachsende Zahl an Risikomeldungen (© BfArM)

Sicherheitsparametern lockern lässt. Hersteller müssen die IT-Security von Anwendungen systematisch und entlang des ganzen Software-Lebenszyklus managen. Dazu gehört es auch Anwendungen im laufenden Betrieb auf Softwareschwachstellen zu monitoren.

Dokumentation

Die Sicherheitsdokumentation beginnt bereits auf Codeebene und verlangt nach einem hohen Automatisierungsgrad. Kommerzielle Anwendungen setzen sich heute aus Tausenden von Komponenten aus unterschiedlichen Quellen zusammen. Neben proprietär entwickelten Code und dem Code von Partnern und Drittanbietern gehören dazu auch frei zugängliche Open Source-Repositories im Netz. Tatsächlich bestehen Anwendungen – auch in der Medizinelektronik – bis zu 90 % aus Open-Source-Komponenten.

Was ist Software Composition Analysis?

Angesichts des zunehmenden Umfangs von Open Source in modernen Anwendungen ist eine manuelle Überprüfung der Codebausteine nicht mehr möglich. Software Composition Analysis (SCA) hat sich daher in den letzten Jahren als bewährter Prozess etabliert, um die Analyse der Sicherheit, Lizenzkonformität und Codequalität zu automatisieren.

Als Teil eines umfangreichen Application-Security-Tests schafft SCA die Grundvoraussetzung, um unterschiedliche Anforderungen an das Risikomanagement von Software zu erfüllen und entsprechende Prozesse in Unternehmen zu implementieren.

1. Erstellen einer Software Bill of Materials (SBOM)

SBOMs sind eine Art Inventarliste, die neben Top-Level-Komponenten, Sub-Komponenten, direkte und transitive Abhängigkeiten sowie die dazugehörigen Lizenzen und Softwarschwachstellen enthält. Entwickler, Security- und Compliance-Manager erhalten so einen umfassenden Einblick in die Zusammensetzung ihrer Software.

Moderne SCA-Tools sind in der Lage, diese Stücklisten automatisiert zu erstellen. Die Lösungen aggregieren dazu Daten aus unterschiedlichen Quellen und fassen sie in einem Standardformat (z. B. SPDX, Cyclone DX) zusammen. Sicherheitsberichte wie VDR und VEX liefern eine Momentaufnahme aktueller Software Vulnerabilities und erlauben es Sicherheitsteams im Abgleich mit der SBOM, die Sicherheitslage schnell und sicher zu bewerten.

Komplette Listung

Die Auflistung der eingesetzten Code-Komponenten beschränkt sich damit nicht auf intern erstellte SBOMs, sondern deckt SBOMs von Upstream-Partner und Drittanbieter sowie Daten aus SCA-Scans, Open Source Software-Libraries und anderen Data Services ab. Dieser umfassende Abgleich erlaubt es zudem, die Gesamtqualität des Codes zu bewerten.

Technische Richtlinie TR-03183

Die SBOM gehören zu den Empfehlungen in vielen gesetzlichen Cybersecurity-Frameworks – unter anderem im Cyber Resilience Act der EU und der Executive Order (EO) in den USA. In Deutschland hat das BSI im letzten Jahr mit Teil 2 der Technischen Richtlinie TR-03183 [7] erstmals Vorgaben für die SBOM vorgelegt. Darüber hinaus hält die

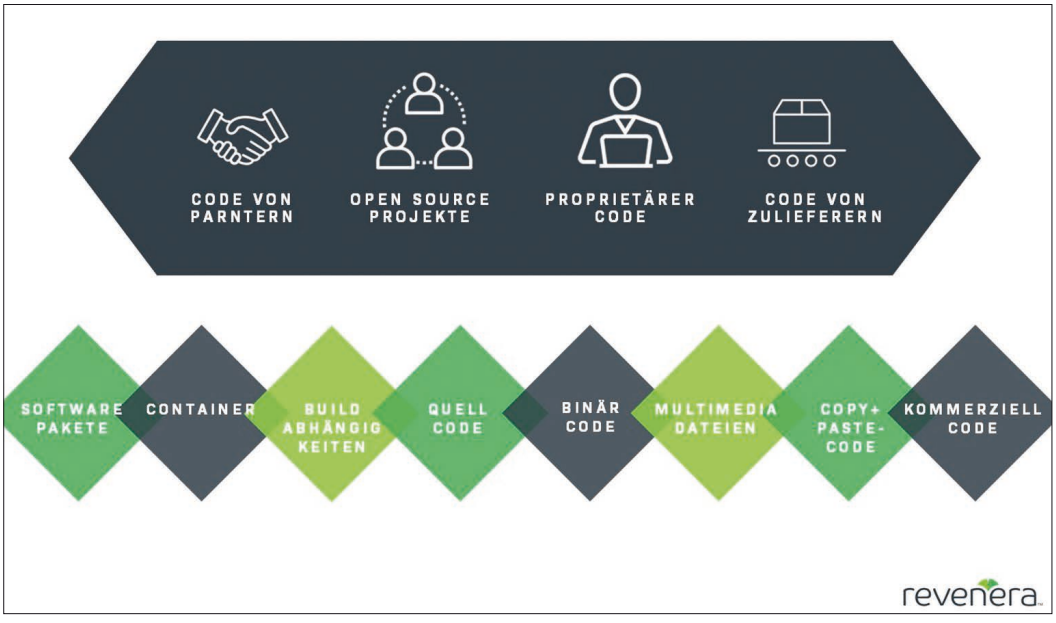

Bild 2: Software Supply Chain (© Revenera)

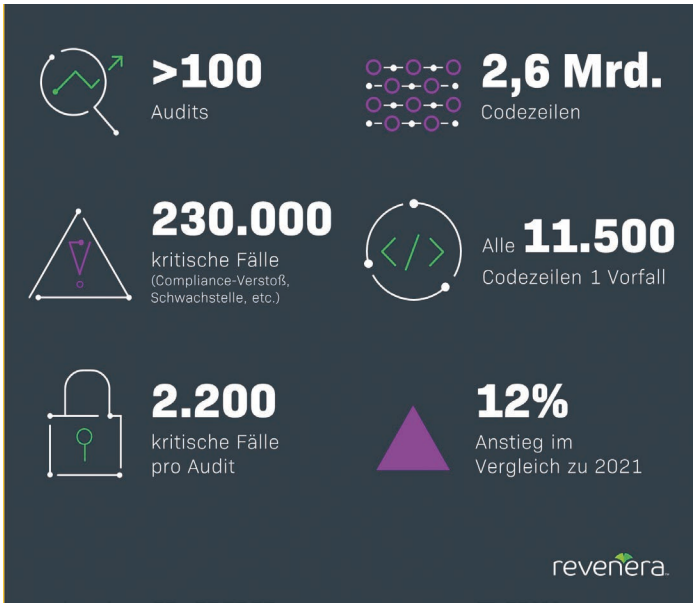

Bild 3: Ergebnisse des Statusreport 2022 zu Open Source Software (© Revenera)

SBOM vermehrt Einzug in Service Level Agreements zwischen Softwareherstellern und Kunden.

2. Open Source Tracking

SCA konzentriert sich auf die Nachverfolgung und Dokumentation aller Open Source-Komponenten sowie ihre modifizierten Varianten. Das erhöht die Transparenz entlang der Software Supply Chain und stellt wichtige Informationen bereit, um den Umfang undokumentierter Open Source Software (OSS) in Unternehmen zu erfassen und potenzielle Compliance- und Sicherheits-Risiken zu identifizieren.

Branchenübergreifende Studie

In einer branchenübergreifenden Studie [8] wertete der Softwareexperte Revenera mehr als 2,6 Milliarden Codezeilen aus. Dabei stießen die Analysten durchschnittlich alle 11.500 Codezeilen auf einen Compliance-Verstoß, eine Sicherheitsschwachstelle oder Ähnliches. 83 % der in den Audits aufgedeckten Risiken war den Unternehmen im Vorfeld der Untersuchung nicht einmal bekannt.

3. Aufdecken von Schwachstellen

Wer nicht weiß, was im eigenen Anwendungscode steckt, kann darin befindliche Sicherheitslücken kaum beheben. Besonders eindrücklich zeigte das Log4j, das sich als De-facto-Standard für Logging von Java in unzähligen Anwendungen befindet. Als im Dezember 2021 eine Schwachstelle öffentlich wurde, herrschte bei Softwareanbietern Unsicherheit: Viele konnten das Sicherheitsrisiko der Schwachstelle für ihre eigenen Produkte nicht genau oder erst nach geraumer Zeit abschätzen.

Ein Schwerpunkt von SCA liegt daher auf der Aufdeckung von Sicherheitslücken. SBOMs lassen sich mit einschlägigen Datenbanken (z. B. National Vulnerability Database, NVD) abgleichen. Sicherheitsteams überprüfen dann das Risikolevel und die Kritikalität bekannt gewordener Schwachstellen und patchen diese bei Bedarf. Vor allem aber wissen sie, ob sich die betreffende Sicherheitslücke überhaupt im Code ihrer Anwendungen steckt. Updates und Patches lassen sich so zu Beispiel zielgerichtet und nicht mehr nach dem Gießkannenprinzip verteilen.

4. Integration von OS-Scans in den Build-Prozess

Die Dokumentation und das Management von OSS-Code beginnt bei der Entwicklung von Softwarenanwendungen. In modernen DevOps- oder DevSecOps-Umgebung ist SCA daher eng mit dem sogenannten „Shift Left"-Ansatz verbunden. In der Entwicklungsphase werden Aufgaben rund um das Testen, Beheben und Nachverfolgen des Codes möglichst an den Beginn bzw. eine frühe Phase verschoben. Die vorausschauende Entwicklung steigert dann im Folgenden die Effizienz von Arbeitsabläufen.

In Bezug auf SCA bedeutet es, dass Entwickler und Sicherheitsteams OSS-Scans sowie Tests und Audits möglichst früh, proaktiv und kontinuierlich durchführen. Software Vulnerability Management und Lizenz-Compliance wird damit fester Bestandteil des Entwicklungsprozesses.

5. Richtlinien festlegen und durchsetzen

SCA untermauert interne Richtlinien auf praktischer Ebene. Entsprechend gehören zu einem SCA-Framework auch Trainings und Fortbildungen, um das Know-how rund um OS-Lizenzkonformität und -Sicherheit im gesamten Unternehmen zu verbreiten.

Um Workflows und Best Practices im Betriebsalltag tatsächlich durchzusetzen, empfiehlt es sich darüber hinaus dedizierte Teams für SCA und das Management von Open Source Software einzusetzen. Dazu gehört beispielsweise ein Open Source Program Office (OSPO) oder Open Source Review Boards (OSRBs), die eine Open Source-Strategie entwickeln, implementieren und im Austausch mit internen Entwicklerteams und externen Organisationen verfeinern.

Fazit

IT-Sicherheit und Cyberschutz sind keine einmaligen Aufgaben, die sich per Knopfdruck lösen lassen. Auch SCA läuft kontinuierlich ab und zielt darauf, Software und Medizinprodukte über den kompletten Lebenszyklus hinweg zu schützen. Den wachsenden Katalog an regulatorischen Anforderungen zu erfüllen, ist das eine. Als Strategie, die auf Codeebene beginnt, bietet SCA jedoch noch weitere Vorteile – von einer schnellen Time-to-Market über Kosteneffizienz bis zum Innovations-Boost für vernetzten Medizinprodukte.

Links

[1] Jahresbericht 2023 - Science. Network. Healthcare: https://www.bfarm.de/SharedDocs/Downloads/DE/BfArM/Publikationen/Impulsbericht-2023.pdf?__blob=publicationFile
[2] Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_132.html
[3] Cyber Resilience Act: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
[4] NIS2: https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/
[5] 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
[6] SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies: https://www.sec.gov/news/press-release/2023-139
[7] SBOM-Anforderungen: TR-03183-2 stärkt Sicherheit in der Software-Lieferkette: https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/TR-03183-2-SBOM-Anforderungen.html
[8] Revenera's 2022 Report on Software Supply Chain Compliance: https://info.revenera.com/SCA-RPT-OSS-License-Compliance-2022/?lead_source=PR

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. ◄