Die Software-Bill-of-Materials (SBOM)

Compliance, Standards & Best Practices

© Unsplash/ Johan van Wambeke, CC0-Lizenz

In der Fertigung ist die Stückliste Standard. Sie gibt Auskunft über Bauteile und schafft Transparenz in der Supply Chain. In der Softwareentwicklung ist das anders. Hier gleicht die Zusammensetzung der Code-Komponenten oft einer Blackbox – mit spürbaren Folgen für die Sicherheit.

© Nicole Segerer

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

Ein Beispiel

Eine Boeing 747-8 besteht aus rund 6 Millionen einzelnen Bauteilen. Zahlreiche Lieferketten sind für die Teilkomponenten und Baugruppen involviert. Boeing selbst stellt dabei nur sehr wenig in Eigenfertigung her und überlässt den Großteil des Flugzeugbaus Dienstleistern und Partnern. Damit kann sich der Hersteller u. a. auf die Qualitätssicherung konzentrieren. Fällt ein Bauteil aus, gilt es den verantwortlichen Hersteller entlang der Supply Chain ausfindig zu machen, die Komponente zu reparieren, den Zulieferer zu wechseln oder die Sicherheitsanforderungen anzuheben. Die Luftfahrindustrie verfügt daher nicht ohne Grund seit Jahrzehnten über entsprechende Prozesse und kann auf ein hohes Maß an Transparenz und Rückverfolgbarkeit in der Lieferkette vertrauen. Warum der Vergleich mit einem Flugzeug?

Betrachtet man die Lieferkette, so unterscheidet sich ein Softwareprodukt nicht wesentlich von einer Boeing. Es gibt kaum eine Anwendung, die von Grund auf „neu“ geschrieben wird. Vor allem bei Programmierroutinen greifen Entwickler gerne auf bereits vorhandene Codezeilen zurück, bedienen sich in Open Source-Repositories im Netz oder kaufen Komponenten von Drittanbietern. Tatsächlich bestehen kommerzielle Anwendungen heute aus bis zu 90 % aus Open-Source-Software (OSS). Dieses Multi-Sourcing in der Softwareentwicklung ist durchaus sinnvoll. Das Problem: Es gibt keine wirklich ausgereiften Prozesse, um die Tausenden von Komponenten zurückzuverfolgen.

Blinde Flecken im Software-Code

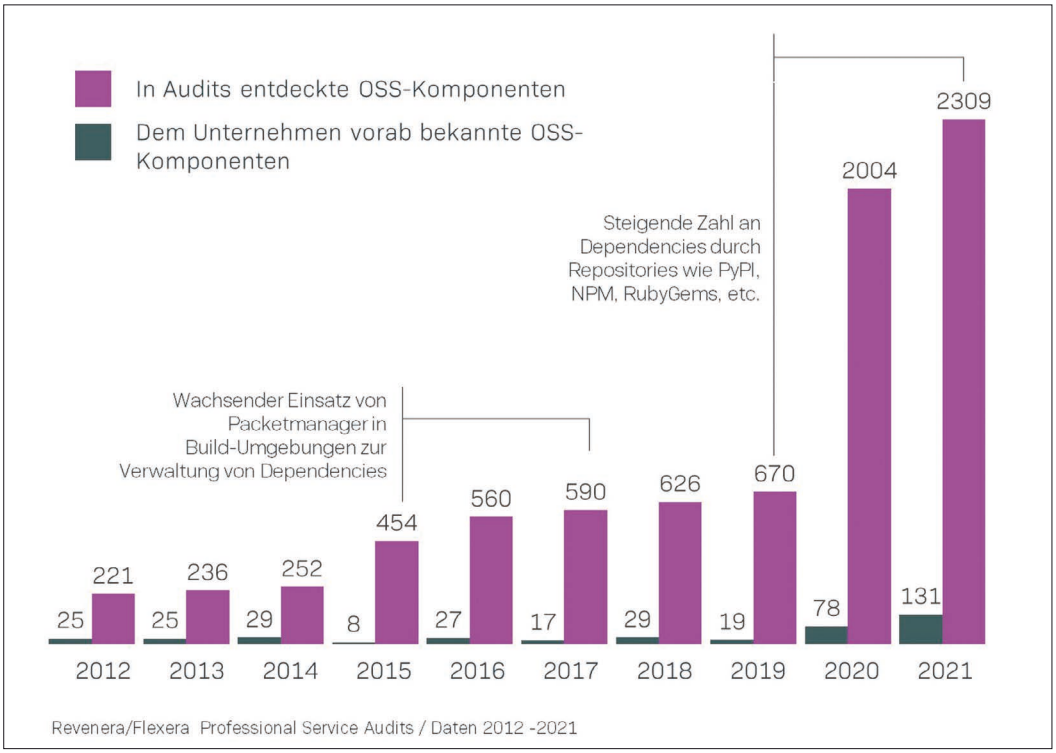
Während niemand bei Boeing willkürlich nach einer Mutter oder Schraube greift, die nicht von einem zertifizierten Zulieferer stammt, gibt es in der Softwareindustrie kein vergleichbares Überprüfungsverfahren. Entwickler entscheiden oft im Alleingang, welche Code-Komponente sie verwenden. Dabei folgen sie nicht immer festen Regeln. Zudem bleibt die Dokumentation einschließlich Herkunft, Lizenzbestimmung und Schwachstellen außen vor.

Kein Wunder also, dass 83 % der in Software-Audits aufgedeckten Compliance- und Sicherheits-Risiken den Unternehmen nicht einmal bekannt sind. In einer Studie zu undokumentierten OSS wertete Revenera mehr als 2,6 Milliarden Codezeilen aus und identifizierte insgesamt 230.000 kritische Fälle. Durchschnittlich stießen die Analysten alle 11.500 Codezeilen auf einen Compliance-Verstoß oder eine Sicherheitsschwachstelle. Um beim Vergleich mit Boeing zu bleiben: Würde man in einem Flugzeug auf ähnlich viele kritische Vorfälle stoßen, würde wohl kaum noch jemand fliegen.

Software-Bill-of-Materials (SBOM)

Software ist nie 100 Prozent sicher. Umso wichtiger ist, dass sobald Schwachstellen bekannt werden, Unternehmen schnell und zielsicher diese beheben und patchen können. Ohne lückenlose Dokumentation, lässt sich jedoch nicht

zurückverfolgen, welche Anwendungen überhaupt betroffen sind. Genau hier soll die Software-Bill-of-Materials (SBOM) Klarheit schaffen. SBOMs sind eine Art Inventarliste, in der nicht nur alle in einer Software eingesetzten Code-Komponenten – einschließlich Lizenzierung, Versionen und Herkunft – festgehalten sind. 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. Die detaillierte Auflistung soll Sicherheitsteam und Compliance Managern helfen, den Überblick zu bewahren und schneller zu reagieren. Die SBOM kann, muss dabei nicht zwingend öffentlich sein. Softwareanbieter können die Stückliste beispielsweise über einen geschützten Kanal an Kunden weitergeben, um die Intellectual Property (IP) ihrer Produkte zu schützen.



Open Source Report 2022 © Revenera

Mindestangaben der SBOM

Bei der Erstellung einer Software-Stückliste beginnen Unternehmen in der Regel mit einer einfachen Liste der Primärkomponenten. Dieser erste Basisdatensatz enthält die wichtigsten Informationen, die sich dann Schritt für Schritt mit zusätzlichen Daten zu den eingebundenen (Dritt-)Komponenten anreichern lassen. Die Detailtiefe ist bei mehrstufigen und weit verzweigten SBOMs durchaus komplex. Dabei ist es nicht unbedingt entscheidend, ob eine Subkomponente funktionskritisch für eine Anwendung ist. Viel wichtiger ist, dass in der Komponente eine kritische Schwachstelle stecken könnte.

Grundsätzlich ist die SBOM beliebig erweiterbar. Allerdings gibt es gewisse Mindestangaben, die sie erfüllen MUSS. Das BSI (Bundesamt für Sicherheit in der Informationstechnik) veröffentlichte hier im August 2023 erstmals klare Vorgaben. Eine der Richtlinie konforme SBOM muss demnach für jede zum Lieferumfang gehörende Komponente alle direkten sowie transitiven Abhängigkeiten bis einschließlich der ersten Komponente durchführen. Bei den anzugebenden Informationen unterscheidet das BSI zwischen den notwendigen Datenfeldern zur SBOM sowie zu den Komponenten (siehe Tabelle).

Notwendige Datenfelder zur SBOM	
Ersteller der SBOM	„Uniform Resource Identifier (URI)“, einschließlich E-Mail-Adresse
Zeitstempel	Datum und Uhrzeit der Erstellung
Notwendige Datenfelder zu jeder Komponente	
Ersteller der Komponente	„Uniform Resource Identifier (URI)“, einschließlich E-Mail-Adresse
Komponentenname	Ursprünglich vom Ersteller zugewiesene Bezeichnung
Version der Komponente	Vom Ersteller benutzte Bezeichner, um Änderungen in der Software-Komponente zu einer zuvor erstellten Version zu signalisieren.
Abhängigkeiten von anderen Komponenten	Aufzählung aller Komponenten, von denen diese Komponente unmittelbar abhängig ist
Lizenz	Effektive Lizenz der Komponente (SPDX-License-Identifier)
Hashwert der ausführbaren Komponente	Kryptografisch sichere Prüfsumme (Hashwert) der Komponente

Regulatorische Vorgaben und Standards

Ähnlich wie die Stückliste in der Fertigung entwickelt sich die SBOM zu einem festen Bestandteil des Anforderungskatalogs in Kaufverträgen und Request for Information (RFIs). Auch auf Seiten des Gesetzgebers rückt die Software-Stückliste in den Mittelpunkt. Der von der EU vorgelegte Entwurf des Cyber Resilience Act (CRA) macht die SBOM zur Pflicht. Entwickler sind demnach unmittelbar für Cyberattacken haftbar, wenn diese auf Sicherheitslücken im Code zurückzuführen sind. Auch Branchenverbände wie die GENIVI Alliance und die Automotive Grade Linux (AGL) sprechen sich für die verbindliche Einführung der SBOM aus.

Noch kein Standard für SBOM-Erstellung

Trotz aller Initiativen: Noch fehlt es an dem einen Standard für die Erstellung von SBOMs. Verschiedene Stakeholder geben Informationen auf unterschiedliche Art und Weise entlang der Lieferkette weiter. Das reißt Lücken in die Dokumentation und macht sie fehleranfällig. Zu den vom BSI anerkannten Formaten gehören SPDX in der Version 2.3 oder höher sowie CycloneDX in der Version 1.4 oder höher. Doch Vorsicht: Auch hier ist die Wahl von jeweiligen Präferenzen abhängig. So wird SPDX beispielweise von Microsoft genutzt, während Siemens auf das CycloneDX-Format setzt.

Best Practices

Unternehmen sollten darüber hinaus beim Erstellen einer SBOM einigen grundlegenden Best Practices folgen:

- **Aufbereitung:** Für einen hohen Automatisierungsgrad sollte der Datensatz einer SBOM maschinenlesbar sein und über strukturierte Datenformate und Austauschprotokolle verfügen. Tools können dann das Auslesen und Erstellen der Stückliste übernehmen, die Listen nach Sicherheits- und Compliance-Verstößen scannen und diese mit dem Software-Code abgleichen. Die Automatisierung ist notwendig, um der Fülle an SBOM-Informationen sowie den unterschiedlichen Strukturen von SBOMs Herr zu werden.
- **Mehrwert für die IT-Sicherheit:** SBOMs an sich enthalten keine Aussage zu Schwachstellen oder deren Ausnutzbarkeit. Dafür bedarf es eines Abgleichs mit CVE(Common Vulnerabilites and Exposures)-Informationen oder Security Advisories. Auch eine Analyse oder der Einsatz eines Software Composition Analysis-Tool entfällt durch die SBOM nicht. Vielmehr sollten SBOMs mit Ergebnissen von Analysen und Sicherheitsupdates kombiniert werden. Vulnerability Disclosure Reports (VDR) oder Vulnerability Exploitability eXchange (VEX) liefern eine aktuelle Momentaufnahme der Sicherheitslage und verweisen auf die in der SBOM aufgelisteten Code-Komponenten.
- **Kontinuierliche Aktualisierung:** Ein Update der SBOM muss in regelmäßigen und klar abgesteckten Zeiträumen stattfinden, wenn sie nicht an Bedeutung verlieren will. Hersteller nutzen oft ein neues Release als Gelegenheit zur Überprüfung und Aktualisierung. In manchen Fällen bestimmen auch Vertragsvereinbarungen mit Kunden sowie Compliance-Richtlinien den Zyklus.
- **Dedizierte Teams:** Die Komplexität des Software Supply Chain Managements setzt klar definierte Prozesse und neue Rollen und Verantwortlichkeiten im Unternehmen voraus. Im Open Source Program Office (OSPO) arbeiten beispielsweise verschiedene Abteilungen (z. B. Recht, Entwicklung, Produktmanagement, Sicherheit) zusammen, um Richtlinien für den sicherheitskonformen Umgang von Open-Source- und Dritt-Code zu implementieren. Die praktische Realisierung und Durchsetzung ist dann die Aufgabe des Open Source Review Boards (OSRB). OpenChain Project

Für Unternehmen auf der Suche nach definierten Prozessen, Frameworks und Trainings-Material rund um die SBOM bietet das von Linux ins Leben gerufene OpenChain Project eine gute Anlaufstelle. Der Zusammenschluss aus über 1.000 Unternehmen ist verantwortlich für die Standards ISO/IEC 5230:2020 und ISO/IEC DIS 18974, die sich mit der Nutzung und Dokumentation von OSS befassen. Umfassende Guidelines finden sich zudem auf den Webseiten der US-Behörde National Telecommunications and Information Administration (NTIA) sowie der Cybersecurity and Infrastructure Security Agency (CISA).

Über die Autorin:

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 bei Revenera unterstützt sie Softwareanbieter und IoT-Hersteller bei der Umstellung auf neue digitale Geschäftsmodell und der Optimierung der Softwaremonetarisierung. ◄

Links:

National Telecommunications and Information Administration (NTIA)
https://www.ntia.gov/page/software-bill-materials

Cybersecurity and Infrastructure Security Agency (CISA)
https://www.cisa.gov/sbom

SBOM Kreislauf © Revenera