Software Bill of Material (SBOM)
Grundlagen, Einschätzungen, Ausblicke

Die Software Bill of Material (SBOM) enthält Informationen über verwendete Software-Komponenten und kann als ein wichtiger Baustein des Software-Supply-Managements verstanden werden. Sie kann dabei helfen, Transparenz über eingesetzte Softwarekomponenten zu erlangen und die Cybersicherheit entlang der Lieferkette zu verbessern. Der Themenkomplex SBOM wird daher seit einigen Jahren als ein mögliches Instrument zur Verbesserung der Cybersicherheit und Transparenz innerhalb der (Software-) Lieferkette diskutiert. Auch regulatorisch findet die Software Bill of Material immer stärker Einzug in mögliche Vorgaben an Hersteller oder (Wieder-)Verwender von Hardware- oder Software-Produkten.

Bevor über die weitere Verwendung und Umsetzung nachgedacht wird, sollte seitens industrieller Akteure wie auch seitens des Regulierers ein einheitliches Verständnis der SBOM entwickelt werden. Dieses Papier möchte zu diesem Verständnis einen Beitrag aus Sicht der Elektro- und Digitalindustrie leisten.

Verband der Elektro- und Digitalindustrie

1. Einleitung

Hintergrund:

Das Thema SBOM gewinnt nicht nur im internen Supply-Chain-Management vieler Unternehmen an Bedeutung, sondern erhält auch durch politische Entscheidungen und regulatorische Entwicklungen größere Aufmerksamkeit. Zum einen durch den US-amerikanischen „Cyber Supply-Chain-Management and Transparency Act“ und die Executive Order 14028 „Improving the Nation's Cybersecurity“, die am 12. Mai 2021 veröffentlicht wurde. In der Executive Order wurde die Bereitstellung einer SBOM erstmals als Transparenzanforderung definiert und für bestimmte Bereiche gefordert. Im Rahmen der Executive Order wurde ein Bericht der zuständigen Telekommunikations- und Informationsbehörde NTIA[1] veröffentlicht, welcher erstmal „minimum elements“ einer SBOM beschreibt.

Das Konzept gewann weitere Bedeutung durch den am 15. September 2022 veröffentlichten Entwurfs des EU Cyber Resilience Acts – der weltweit ersten Regulierung mit horizontalen Produktanforderungen zur Cybersicherheit von Hardware und Software. Dort ist die SBOM sowohl als Teil der „Anforderungen an die Behandlung von Schwachstellen“ des Herstellers wie auch als mögliches Element der Nutzerinformationen vorgesehen.

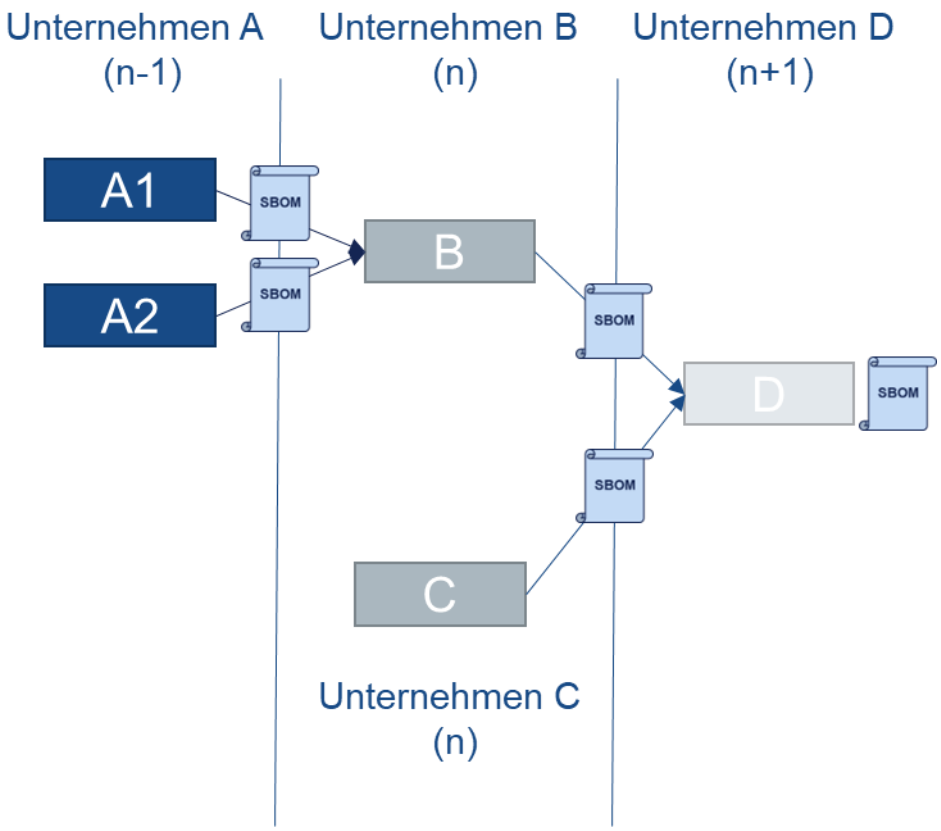
Organisatorische Problemstellungen:

- Herausforderung der Verwaltung eigener Assets in der Softwareentwicklung (Security Development Lifecycle, SDL)
- SBOM-Generierung: Verfügbarkeit von standardisierten Formaten und Verteilmechanismen und Aufbau von Inhalten und Tools
- Aufbereitung und Aufarbeitung der SBOM für bereits vorhandene/verkaufte Software;
- Eindeutige, reproduzierbare Identifikation von Software, insbesondere bei Open Source
- Etablierung und (schrittweise) Verbesserung von Prozessen zur SBOM-Erstellung sowie schrittweise Verbesserung (Ramp-Up) der Qualität einer SBOM
- Verfügbarkeit einer SBOM; Transparenz (auch hinsichtlich ‚veralteter‘ Software)
- Wie werden Korrekturen einer SBOM kommuniziert?
- SBOM in gesamten Supply-Chain-Security-Kette ‘anreichernd’ durchgeben; trotz der auf die Ebenen „n-1“, „n“ & „n+1“ begrenzten Reichweite jeder Stücklistengenerierung
- Verknüpfung Betroffenheit von Schwachstellen und SBOM (vgl. Kap. 6)

Ziel:

Das Ziel dieses Papiers ist ein gemeinsames Verständnis von SBOM und ihrer sinnvollen Nutzung zu entwickeln, Mindestelemente und ihren Umfang zu beschreiben sowie Optionen für die künftige Weiterentwicklung aufzuzeigen. Die Einführung einer weiteren aufwendigen Anforderung zur Informationsbereitstellung ohne Mehrwert für die umsetzenden Unternehmen sollte jedoch auf jeden Fall vermieden werden. Dieses Dokument soll auch den herstellerinternen Nutzen einer SBOM aufzeigen und die Vor- und Nachteile für einen externen Konsumenten einer SBOM aufzeigen. Dabei ist auch die Begrenztheit der Reichweite der eigenen SBOM(-Erstellung) zu berücksichtigen (vgl. die Ebenen „n-1, n, n+1 in der folgenden Grafik). Zusätzlich soll das Bewusstsein gestärkt werden, dass Zulieferer identifiziert, adressiert und sensibilisiert werden müssen sowie eine Auseinandersetzung darüber angestoßen werden, welchen Kunden welche Informationen bereitzustellen sind.

[1] https://www.ntia.gov/files/ntia/publications/sbom_minimum_elements_report.pdf



Idealerweise sollte für jeden Schritt in der Lieferkette eine Stückliste für das jeweilige Softwareprodukt oder die Komponente erstellt werden. Durch die Verwendung von vorgelagerten Stücklisten, bei der Generierung von in der Lieferkette nachgelagerten Stücklisten, sollten am Ende der Kette, trotz der begrenzten Reichweite jeder Stücklistengenerierung, alle relevanten Informationen zusammenkommen.

Beispielhaft wird dies in der obenstehenden Abbildung dargestellt: Unternehmen A stellt die Produkte A1 und A2 inklusive der SBOM bereit. Unternehmen B kombiniert A1 und A2 zu einem Produkt B. Die SBOM für Produkt B enthält daher Verweise auf die Produkte A1 und A2. Unternehmen D setzt führt einen weiteren Integrationsschritt durch und kombiniert Produkt B und Produkt C zu Produkt D.

2. Was ist eine SBOM?

Eine SBOM ist ein formaler, idealerweise maschinenlesbarer Datensatz, welcher die nachvollziehbare Inventarisierung von Software-Komponenten und deren Beziehungen enthält, die im Produkt (der Software oder Firmware) enthalten sind. Dabei wird die SBOM als rein statische Information zu der Software einer bestimmten Produktversion betrachtet:
Eine SBOM enthält Informationen über „open source“ oder proprietäre Software und könnte weithin verfügbar oder zugangsbeschränkt sein.[2] Dabei ist davon auszugehen, dass eine SBOM entsprechend ihrer weiteren Verwendung, intern oder extern, unterschiedlich detailliert ausgestaltet sein könnte (vgl. Kapitel 9).

[2] Definition: https://www.cisa.gov/sbom

3. Was sind Bestandteile einer SBOM?

Der Hauptzweck einer SBOM ist die eindeutige und unmissverständliche Identifizierung von Komponenten und ihren Beziehungen zueinander. Um dies zu erreichen, ist eine Kombination von grundlegenden Komponenteninformationen erforderlich. Die Attribute unterscheiden sich dabei darin, wie exakt sie Softwarebestandteile beschreiben – bestimmte Attribute bieten eine größere Genauigkeit. Die Aussagekraft kann durch eine größere Anzahl von Attributen in einem SBOM-Eintrag erhöht werden. Die folgenden Mindestbestandteile unterstützen viele Anwendungsfälle. Zusätzliche Attribute können für erweiterte Anwendungsfälle erforderlich sein.

Mindestbestandteile einer SBOM:

- **Ersteller der SBOM** (Author Name/Author of SBOM Data) der Organisation, die die SBOM erstellt
- **Name des Software-Zulieferers** (Supplier Name) der Organisation, die das Produkt bereitstellt
- **Name der Software-Komponente** (Component Name), inkl. Produktname des durch die SBOM betrachteten Produktes
- **Versionsnummer/-bezeichnung** (Version of Component) der Komponente
- **Zeitstempel** (Timestamp) der Erstellung der SBOM
- **Eindeutige Kennzeichung** (Unique Identifier) der Komponente
- **Abhängigkeiten/Beziehungen** mit weiteren Software-Komponenten (Dependency Relationship; of direct third party components,)

Die aufgeführten Mindestbestandteile entsprechen den „Baseline Component Information“ der NTIA, die bereits die wichtigsten Bestandteile umfassen.[3] Nach Ansicht des ZVEI sollte eine SBOM aus zumindest diesen Mindestbestandteile bestehen.

Weitere mögliche Bestandteile einer SBOM:[4]

- Weitere Merkmale (Other Identifiers)
- Version der SBOM (Version of SBOM)
- Referenz(en) zur Quelle von Schwachstelleninformationen (z. B. CSAF) /Verweis auf die mögliche Bezugsquellen/URL von Schwachstelleninformationen
- Lizenzinformationen (Copyright Information)
- Hash-Wert der Software-Komponente (Component Hash)
- …

Keine Bestandteile einer SBOM sind:

- Schwachstellen-Informationen, denn diese sind dynamisch, während die SBOM statisch ist.
- Andere Informationen, die nicht mittels der beschriebenen Bestandteile (ggf. maschinenlesbar) übermittelt werden können. Solche Informationen sollte der Hersteller extern bereitstellen.
- Sensitive Informationen, wie z. B. Links zu Build-Systemen oder Namen (E-Mail-Adressen) von Entwicklern

[3] https://www.ntia.gov/files/ntia/publications/sbom_minimum_elements_report.pdf
SBOM at a Glance (ntia.gov)

[4] Bei den aufgeführten weiteren Bestandteilen handelt es sich um zusätzliche Informationen, deren Berücksichtigung bei der Erstellung einer SBOM aus Sicht des ZVEI sinnvoll sein könnte.

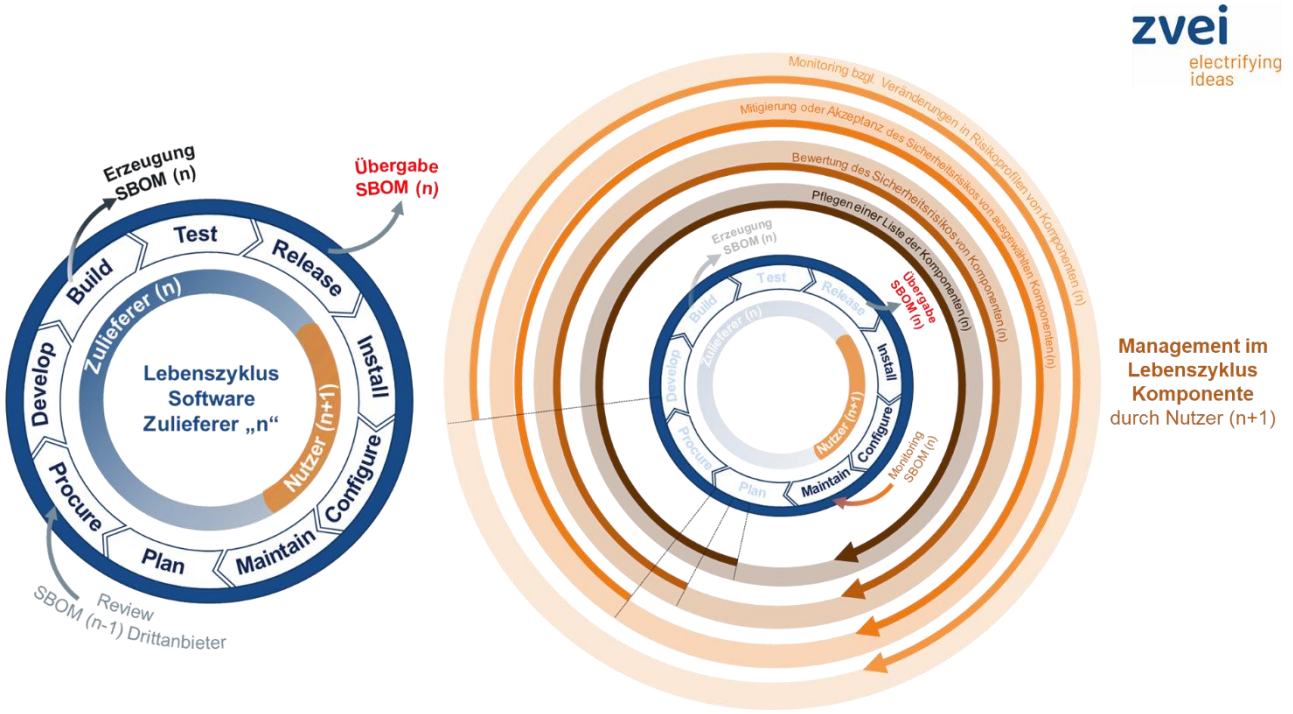
4. Wofür und wie kann eine SBOM genutzt werden?

Als Baustein …

… in der Softwareentwicklung, im Security Development Lifecycle (SDL), (vgl. “Zulieferer n” in Grafik)
- für Open-Source-Compliance-Management (Management von Lizenzinformationen) & Dependency-Management (end of life of libraries)
- im Vulnerability-Management: Verbindung und Verknüpfung SBOM und Schwachstellenmanagement;

… im Supply-Chain-Management (vgl. “Nutzer n+1” in Grafik)
- zur Identifikation und Inventarisierung verwendeter Komponenten und Unterkomponenten; Herausforderung Änderung der SBOM im Produktlebenszyklus

Durch SBOM verknüpfte Lebenszyklen:



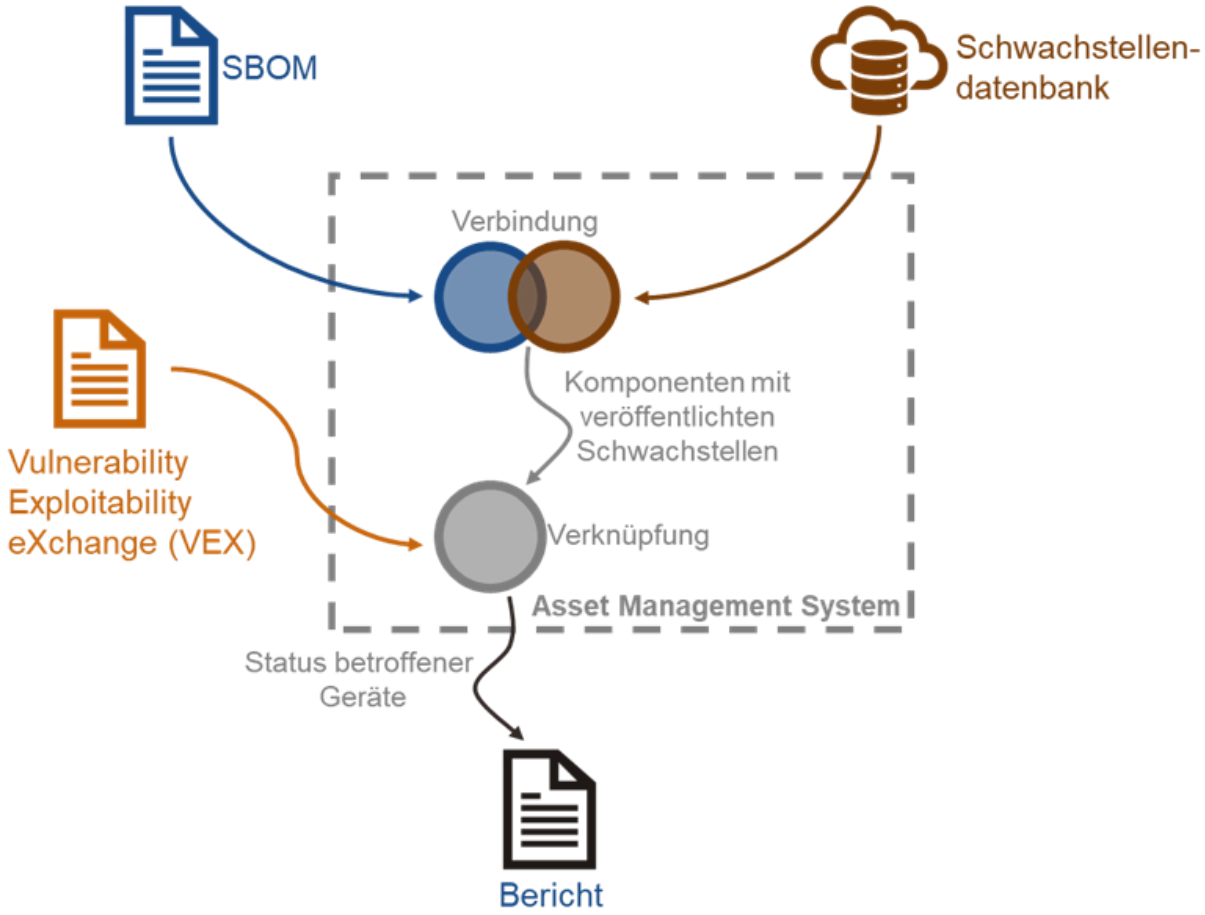
Mittels SBOM können auf verschiedenen Ebenen Software-Komponenten identifiziert und inventarisiert werden. Die jeweilige einzelne SBOM hilft dabei als Datensatz in der Kommunikation zwischen dem jeweiligen Zulieferer einer einzelnen Softwarekomponente und dem Nutzer der entsprechenden Komponente. Der Nutzer setzt diese Komponente meist zusammen mit weiteren Softwarekomponenten ein.

So zeigt die obenstehende Abbildung auf der linken Seite die Erstellung einer SBOM aus der Sicht des Software Zulieferers “n” auf den Lebenszyklus der Software-(Komponente). Die rechte Seite hingegen zeigt die Verwendung dieser SBOM im Lebenszyklus der Nutzung der Komponenten durch den Nutzer „n+1“ und Schritte in diesem Lebenszyklus, die der Nutzer unter Zuhilfenahme der SBOM ergreift.

5. Zusammenhang SBOM mit dem Schwachstellen-management

Verknüpfung Betroffenheit von Schwachstellen und SBOM
SBOM bleiben, bis auf die Korrektur von inhaltlichen Fehlern für die Version des Produktes statisch. Eine Korrektur von inhaltlichen Fehlern in der SBOM darf nicht mit einer dynamischen Anreicherung bzw. Verknüpfung mit anderen Informationsquellen, z. B. VEX[5] (vgl. untenstehende Grafik), verwechselt werden. Eine SBOM enthält keine Schwachstelleninformationen.

SBOM sollten auch nicht mit Schwachstelleninformationen angereichert werden, da sonst jede neue Schwachstelleninformation mit einer erneuten Erstellung und Verteilung der SBOM der entsprechenden Produktversion verbunden wäre. Die SBOM sollte vielmehr der Identifikation der Betroffenheit bei Erhalt einer Schwachstelleninformation dienen.



Die Verknüpfung wird zudem hohe Aufwände und Ansprüche in der Qualitätssicherung der Schwachstellen-Meldungen und ihrer Verarbeitung stellen: Es ist zu erwarten das wesentlich mehr Schwachstellen-Negativmeldungen als Meldungen bestätigter Schwachstellen („echte Advisories“) entstehen und veröffentlicht werden. Nutzer brauchen daher Prozesse und entsprechende Tools, um diese Datenmengen verarbeiten zu können.

[5] CycloneDX - Vulnerability Exploitability eXchange (VEX)
Vulnerability Exploitability eXchange (VEX) – Use Cases (cisa.gov);
Quelle Grafik: https://www.ntia.gov/files/ntia/publications/framing_2021-04-29_002.pdf

Deswegen ist die Verwendung von Standards im Schwachstellenmanagement zur weitestgehenden Automatisierung von der Inventarisierung, über den Abgleich bekannter Schwachstellen, bis zur Bereitstellung notwendiger Informationen an den User, sehr wichtig.

So können die Schwachstelleninformationen, inklusive Informationen über Betroffenheit (Positiv-Meldung) und Nicht-Betroffenheit (Negativ-Meldung) über CSAF (Common Security Advisory Format)[6] und VEX (Vulnerability Exploitability eXchange), kommuniziert werden.

Nur wenn sowohl SBOM als auch Schwachstellen maschinenlesbar sind, ist eine automatische und damit genaue und schnelle Auswertung möglich. Auch wird damit erreicht, dass der Nutzer des Produkts darüber in Kenntnis gesetzt wird, welche öffentlich bekannten Schwachstellen tatsächlich für das Produkt relevant sind. Dies ist nicht gewährleistet, wenn nur die SBOM-Information, ohne eine vom Hersteller bewertete Schwachstelleninformation (im Kontext der Anwendung), vorliegt.

[6] Link zur CSAF-Spezifikation: https://docs.oasis-open.org/csaf/csaf/v2.0/csaf-v2.0.html
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/CSAF/CSAF_node.html

6. Grenzen der Nutzung

Die SBOM kann für die Risikoabschätzung genutzt werden, braucht für die Einschätzung aber Zusatzinformationen.

Keine unkontrollierte Herausgabe der SBOM:

Eine SBOM kann vom Endkunden ohne Zusatzinformationen nicht direkt für ein Schwachstellenmanagement verwendet werden.

Bei den Zusatzinformationen handelt es sich z. B. um die Verwendung der Funktionen der im Produkt integrierten Komponenten. Dies soll an einem Beispiel konkretisiert werden:

In einer Bibliothek zur Verschlüsselung werden unterschiedliche Algorithmen (A, B, C) unterstützt. Der Hersteller integriert die Bibliothek und verwendet nur Algorithmus C. Es wird dann eine Schwachstelle in Algorithmus A gefunden, der Fehler behoben und ein Update sowie ein Security Advisory veröffentlicht. Ohne eine Information bzgl. der Verwendung besteht auf Basis der SBOM der Verdacht, dass das Produkt von dieser Schwachstelle betroffen ist. In der Realität ist dies jedoch nicht der Fall, da die betroffene Funktionalität nicht benutzt wird.

Diese Zusatzinformationen können nur vom Hersteller zur Verfügung gestellt werden bzw. nur von diesem kann die Auswertung durchgeführt werden. Diese Zusatzinformationen sind dabei kein Teil der SBOM, aber für ihre Nutzung essenziell. Deshalb sollten diese beiden Inhalte nur in Kombination gepflegt und herausgegeben werden bzw. diese Informationen müssen in Referenz vorliegen, um eine SBOM nutzen zu können.

Diese Zusatzinformationen sind vor allem die Bewertung und Einschätzung von Schwachstelleninformationen (CVE) durch den Hersteller zum Produkt

Prozesse zur Verwendung müssen gegeben sein:

- Hersteller müssen zunächst die Prozesse und Tools etabliert haben, damit SBOM erstellt oder empfangen, gepflegt und (automatisiert) weitergeben werden können. (Pflege der SBOM über den Lebenszyklus: Generierung, Aktualisierung, Schwachstellenmanagement, Bereitstellung der Daten).
- Prozesse zur (automatisierten) Verarbeitung müssen auch auf der Nutzer Seite vorhanden sein, um die kuratiert herausgegebene SBOM effektiv nutzen zu können.

Abschließend ist es wichtig zu betonen, dass das alleinige Vorliegen einer SBOM nicht zu einer zielführenden weiteren Nutzung derselben befähigt.

7. Welchen Mehrwert stellt die SBOM dar?

Eine SBOM hilft Herstellern ihre internen Prozesse zu organisieren und strukturieren. Daher ist vor allem die unproblematische Anknüpfung an bestehende Unternehmensprozesse im Sinne der Erhöhung der Software-Qualität wichtig.

Zu den Vorteilen gehören die Reduzierung von Kosten, Sicherheitsrisiken, Lizenz- und Compliance-Risiken. Zu den Anwendungsfällen gehören Verbesserungen in der Softwareentwicklung, im Supply-Chain-Management, im Schwachstellenmanagement, im Asset-Management, in der Beschaffung und in „High Assurance“-Prozessen.

Nachvollziehbarkeit:
Eine SBOM ist ein gemeinsamer Datensatz, um an externe oder interne Empfänger (vgl. Kapitel 2) adressatengerecht zu berichten, wie Software gebaut, ausgewählt und betrieben wird. Sie ist ein wichtiger Bestandteil des Security Development Lifecycle (SDL).

- Durch den Einsatz/Verwendung von SBOM wird eine Inventarisierung von eingesetzten Drittkomponenten geschaffen. Mit diesem Datenpool sind Aussagen für den Softwarebetreiber und dessen Eco-System über Abhängigkeiten schnell, zeitnah, und vollumfänglich möglich. Bei einem Security Vorfall oder einer neu entdeckten Schwachstelle wird so eine schnelle Reaktion mit den notwendigen Maßnahmen erst möglich.
- Softwareentwickler, die Open Source Komponenten einsetzen, werden mindestens für diese Komponenten bereits eine Datenbasis zur Verfolgung der Lizenzbedingungen besitzen.

Qualitätsverbesserung der Prozesse in der Supply-Chain:
- Um eine SBOM zu erstellen werden Supply-Chain-Prozesse definiert, umgesetzt und verbessert. Dadurch verbessert sich die Qualität sowie die Handhabbarkeit der Komplexität im Herstellungsprozess und damit der Produkte insgesamt.
- SBOM sollten genauso angesehen werden wie Software, das heißt, sie sind nie fehlerfrei. Deswegen wird es auch Updates zu SBOM geben. Idealerweise ist eine SBOM-Änderung in der Software-Historie nachvollziehbar.

Schnelligkeit:
- Möglichkeit der automatisierten Auswertung
- Potentiell von Schwachstellen betroffene Produkte können schneller identifiziert werden.
- Risikobewertung einer Anlage und Umsetzung von mitigierenden Maßnahmen kann schneller erfolgen.

Aussagefähigkeit:
- Qualifizierte Aussagen über die Betroffenheit von Schwachstellen in Produkten eines Herstellers durch Komponenten von Drittanbietern werden von SBOM unterstützt (z. B. Betroffenheit durch Log4Shell).

8. Welche SBOM-Standards gibt es und welche werden in der Praxis genutzt?

Um die Vorteile von SBOM voll auszuschöpfen, ist eine maschinelle Verarbeitung und Automatisierung erforderlich. Dies erfordert eine umfassende Interoperabilität in der gesamten Lieferkette, die wiederum standardisierte Datenformate und Identifikationsschemata erfordert.

Die folgenden drei Formate konzentrieren sich auf das Kernproblem der Identifizierung von Softwareentitäten und der Übermittlung von zugehörigen Metadaten. Sie verfügen über die erforderlichen Felder, um den Bedarf für die Mindestbestandteile einer SBOM zu decken. Es sind Werkzeuge vorhanden, um diese SBOM zu erstellen, zu konsumieren und zu transformieren.

Format	Spezifikation	Bekannte Tools
SPDX	https://spdx.github.io/spdx-spec/	https://docs.google.com/document/d/1A1jFIYihB-IyT0gv7E_KoSjLbwNGmu_wOXBs6siemXA/edit
CycloneDX	https://cyclonedx.org	https://docs.google.com/document/d/1biwYXrtoRc_LF7Pw10TO2TGIhlM6jwkDG23nc9M_RiE/edit
SWID	ISO/IEC 19770-2:2015	https://docs.google.com/document/d/1oebYvHcOhtMG8Uhnd5he0l_vhty7MsTjp6fYCOwUmwM/edit

Somit sind vor allem die folgenden drei Standards für SBOM als Formate (s. o.) für den Datenaustausch im Gespräch:

- **International Open Standard (ISO/IEC 5962:2021) - Software Package Data Exchange (SPDX)**[7]
  An open standard for communicating software bill of material information, including components, licenses, copyrights, and security references.

- **OWASP CycloneDX Software Bill of Material (SBOM) Standard**[8]
  OWASP CycloneDX is a lightweight Software Bill of Material (SBOM) standard designed for use in application security contexts and supply chain component analysis.

- **Software Identification (SWID) Tags**, *defined by the ISO/IEC 19770-2:2015 standard;*

In der internen Anwendung werden die Informationen sicher in einer Applikation oder Datenbank gespeichert und verwaltet, die Auswertungen und automatische Zuordnungen, etwa von Schwachstellen, ermöglicht. Hier wird häufig der Begriff „Software Composition Analysis“ verwendet. Komponenteninformationen in den SBOM und Schwachstelleninformationen sollten zusammen eingesetzt werden, um entlang der Supply-Chain sowohl die Abhängigkeiten von Drittkomponenten als auch die Schwachstellen in den Komponenten zu kommunizieren.

[7] https://spdx.dev/; https://github.com/spdx
[8] https://cyclonedx.org/

9. Wer erhält Zugriff auf welche Information?

Eine SBOM ist ein gemeinsamer Datensatz für das Inventar und die Beziehungen in der Lieferkette der verschiedenen Komponenten, die im Endprodukt (der Software) enthalten sind. Sie ist entlang der Supply-Chain auch zur Erfüllung und Erreichung von Security-Anforderungen hilfreich, indem sie der Nachvollziehbarkeit dient, hinsichtlich der Frage, was in einem Produkt integriert wurde. Die Umsetzung der Erstellung und Nutzung von SBOM sollte entsprechend eines Stufenmodells erfolgen. Dabei sollte die Herausgabe stets auf einer **Need-to-Know-Basis** erfolgen. Wie in Kapitel 2 angemerkt, kann dabei davon ausgegangen werden, dass SBOM entsprechend ihrer weiteren Verwendung, intern oder extern, unterschiedlich umfangreich ausgestaltet sein könnten. Eine interne SBOM, die nur unter entsprechender Vertraulichkeit intern verwendet wird, könnte umfangreicher ausfallen, als eine SBOM die extern herausgegeben wird, z. B. auch zur Einhaltung regulatorischer Anforderungen.

Stufenmodell für alle Beteiligten (Hersteller, Integratoren und Betreiber):

Ab 2025 im Kontext der voraussichtlichen Veröffentlichung des Cyber Resilience Acts ein „best effort“ bereitstellen und auf Feedback (z. B. von Kunden) reagieren sowie Fehler ausbessern:

B2C-Customer: Lediglich Informationen, die der Kunde für den bestimmungsgemäßen Gebrauch benötigt

B2B-Customer: Vertragsrechtlich ausgehandelte Informationsweitergabe abhängig von der weiteren Verwendung des Produkts und entsprechend dem Kenntnisstand und Informationsbedürfnisses des Kunden

B2G (Hersteller gegenüber Aufsichtsbehörden):

Berichtspflichten: Informationen aus SBOM können genutzt werden, um den bisher regulatorisch festgelegten Berichtspflichten nachzukommen. Es sollte allerdings stets eine Engführung auf die tatsächlich von den Aufsichtsbehörden benötigten Informationen erfolgen, sodass eine zielgerichtete Informationsweitergabe erfolgen kann. (Beispiel Schwachstellen-management: Nur Information, wenn Produkte tatsächlich betroffen sind).

Begründete Anfrage Marktüberwachungsbehörden:
Sofern regulatorisch, z. B. durch den CRA, gefordert muss ggf. anlässlich einer begründeten Anfrage einer Marktüberwachungsbehörde die SBOM herausgegeben werden.

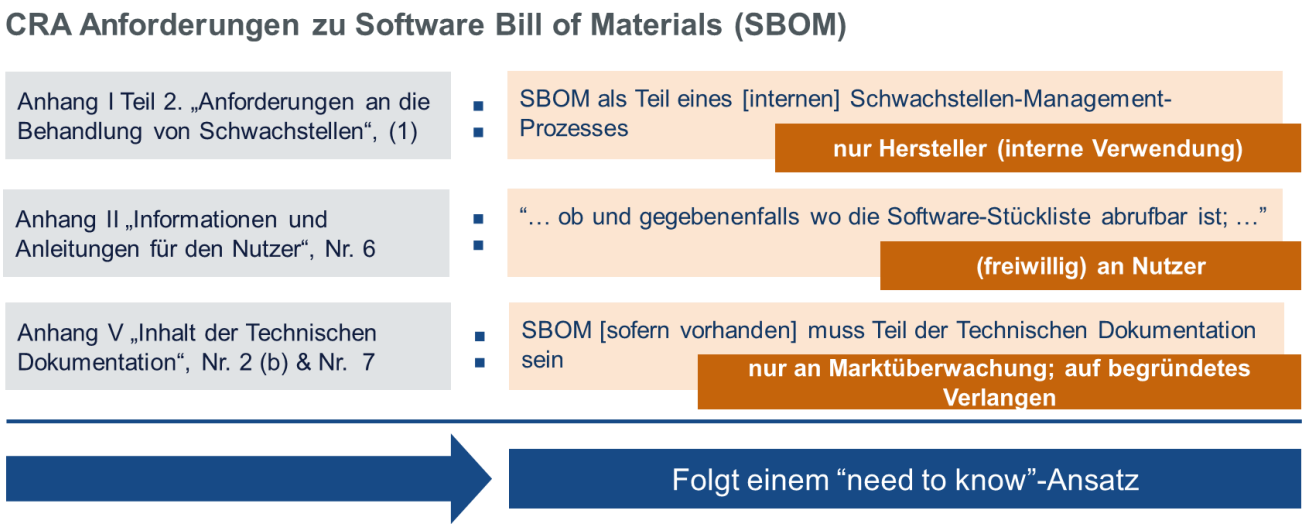
Mit der Zeit wird sich durch die zunehmende Verwendung von SBOM, der Etablierung von Prozessen und der Nutzung entsprechender Tools die Software-Qualität, verstanden als Qualität der Software an sich, Qualität der Prozesse und Qualität der SBOM, verbessern. Eine standardisierte Nutzung und der Fokus auf einige wenige Standards zur Etablierung ihrer Nutzung zwischen Unternehmen ist wichtig.

10. SBOM als Grundlage/Bestandteil einer Konformitätserklärung

Anforderungen zur Verwendung einer SBOM finden sich derzeit nur im Entwurf des EU Cyber Resilience Acts vom 15.09.2022.

Der Entwurf des EU CRA fordert eine SBOM (derzeit ohne Angabe von Details) als Bestandteil der herstellereigenen technischen Dokumentation. In der Kundendokumentation muss lediglich angegeben werden, ob eine SBOM zur Verfügung gestellt wird und wie diese ggf. angefragt werden kann.

Nach Ansicht des ZVEI sollten dabei die in Kapitel 3 beschrieben „Mindestbestandteile“ einer SBOM zur Erfüllung der im Entwurf des CRA gestellten Anforderungen enthalten sein.



Anhang 1 Teil 2:
Zur Erfüllung der Anforderungen aus dem CRA zur Etablierung eines Schwachstellenmanagement-Prozesses, welcher die Erstellung von SBOM beinhaltet, können die in diesem Papier beschriebenen Elemente eine Hilfe bieten.

Anhang II, Nr. 6:
Im Rahmen eines Security Advisories könnten auf freiwilliger Basis Informationen aus der internen SBOM herausgegeben werden.

Anhang V, Nr. 2 (b) und Nr. 7:
Der CRA verlangt eine Technische Dokumentation für jedes Produkt. Sofern es sich um ein Produkt handelt, für das im Rahmen des Schwachstellenmanagement-Prozesses eine SBOM erstellt wurde, muss die SBOM ebenfalls in die Technische Dokumentation aufgenommen werden. Im Einzelfall muss die technische Dokumentation auf eine berechtigte Anfrage der zuständigen Marktüberwachungsbehörde an diese herausgegeben werden.

11. ZVEI-Empfehlungen

- SBOM als wichtiges Mittel für den Informationsfluss zwischen den Stakeholdern entlang der Supply-Chain, die regulatorische Ebene sollte den freien Fluss von Informationen unterstützen
- SBOM ist wesentlich für ein effizientes Schwachstellenmanagement (Monitoring/Scanning).
- SBOM sollte sinnvollerweise im Kontext der Software betrachtet werden: Veränderungen in der realen Software sollten zeitgleich in der SBOM abgebildet werden, damit die SBOM immer den aktuellen Softwarestand widerspiegelt.
- SBOM sollten vom Hersteller die direkt eingesetzten Drittkomponenten enthalten, nicht deren Abhängigkeiten (Level n-1), um der in Kapitel 1 beschrieben Betrachtungstiefe Rechnung zu tragen.

Kontakt
Marcel Hug • Manager Cyber Security & Strategy • Abteilung Digital- und Innovationspolitik •
Tel.: +49 69 6302 432 • Mobil: +49 162 2664 941 • E-Mail: Marcel.Hug@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: 14.04.2023