Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

Software Bill of Materials

Leitfaden

2024

Danksagung

Diese Publikation wurde in der TeleTrusT-Arbeitsgruppe "Cloud Security" erarbeitet. TeleTrusT bedankt sich bei den nachstehenden Personen für ihre Mitwirkung sowie für die aktive Mitgestaltung dieses Positionspapieres.

Projektleitung
Oliver Dehning, Leiter der TeleTrusT-AG "Cloud Security"

Autorenliste (Auszug)

Bühn, Uwe - eperi
Cink, Stefan - Net at Work
Dehning, Oliver - Leiter der TeleTrusT-AG "Cloud Security"
Eidens, Dr. Fabian - Utimaco
Geißler, Yvonne - eperi
Keppeler, Dr. Lutz - Heuking RAe
Oppelland, Vincent - Haufe-Lexware
Probst, Dr. Christian W. - RMTP
Rost, Peter - secunet
Siebert, Dr.-Ing. Gunnar - Aon
Sinnwell, Thomas - consistec

Redaktion

Abou Nasser, Morad - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Mühlbauer, Dr. Holger - Bundesverband IT-Sicherheit e.V. (TeleTrusT)

In dieser Publikation werden zahlreiche Anglizismen verwendet, da sie sich in der zugrundeliegenden Fachdiskussion branchentypisch verfestigt haben.

Dieses Dokument dient als Anhaltspunkt und bietet einen Überblick. Er erhebt weder Anspruch auf Vollständigkeit noch auf die exakte Auslegung der bestehenden Rechtsvorschriften. Er darf nicht das Studium der relevanten Richtlinien, Gesetze und Verordnungen ersetzen. Desweiteren sind die Besonderheiten der jeweiligen Produkte sowie deren unterschiedliche Einsatzmöglichkeiten zu berücksichtigen. Insofern sind bei den im Dokument angesprochenen Beurteilungen und Vorgehensweisen eine Vielzahl weiterer Konstellationen denkbar.

Impressum

Herausgeber:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 400 54 310
Fax: +49 30 400 54 311
E-Mail: info@teletrust.de
https://www.teletrust.de

Inhalt

1 Zusammenfassung / Summary

Angriffe auf die IT Supply Chain haben in den letzten Jahren zugenommen und basieren auf zwei Hauptfaktoren:

1. Lieferanten und deren Komponenten genießen oft ein hohes Vertrauen und weitgehende Rechte.
2. Die Transparenz über die genaue Zusammensetzung dieser Komponenten ist häufig unzureichend.

Diese Kombination führt dazu, dass Unternehmen kaum in der Lage sind, Risiken in der IT Supply Chain proaktiv zu erkennen oder entsprechende Angriffe abzuwehren. Vielmehr müssen sie sich weitgehend auf ihre Zulieferer verlassen.

"Software Bills of Materials" (SBOM), also Software-Stücklisten, bieten hier eine Lösung, indem sie eine detaillierte Auflistung der in einem Gerät, einer Software oder einem Dienst verwendeten Software-Komponenten liefern und so die Transparenz der Supply Chain erhöhen. Dies ermöglicht es Unternehmen, potenzielle Sicherheitslücken selbst und möglichst automatisiert zu bewerten und gezielte Schutzmaßnahmen zu ergreifen.

SBOMs liefern außerdem Informationen über die Lizenzen der verwendeten Komponenten und unterstützen so den Abgleich der tatsächlichen Nutzung mit den Lizenzvorgaben. Zukünftig könnten SBOMs auch dazu beitragen, die Transparenz im Datenschutz zu erhöhen, indem sie Informationen darüber enthalten, welche Daten von welchen Systemen verarbeitet und gespeichert werden.

In Deutschland existieren derzeit keine expliziten zivilrechtlichen oder regulatorischen Vorgaben für die Erstellung und Verwendung von SBOMs. Es kann allerdings argumentiert werden, dass SBOMs Teil des "Standes der Technik" sind, wie ihn verschiedene Gesetze fordern. Zudem wird der von der Europäischen Kommission vorbereitete Cyber Resilience Act (CRA) Hersteller verpflichten, für in der EU vertriebene Produkte SBOMs bereitzustellen. In den USA wurde durch eine Executive Order vom Mai 2021 die Bereitstellung und Nutzung von SBOMs für Software, die an die U.S. Administration geliefert wird, bereits vorgeschrieben. Unternehmen sollten deshalb bereits heute Klauseln zur Verpflichtung der Lieferung und Aktualisierung von SBOMs in ihre Verträge mit Softwarelieferanten und Dienstanbietern aufnehmen.

Der TeleTrusT-Leitfaden "Software Bill of Materials" (SBOM) beschreibt auch verfügbare SBOM-Tools sowie zukünftige Anforderungen an diese Werkzeuge, um vor allem die IT-Sicherheit weiter zu verbessern.

Attacks on the IT supply chain have increased in recent years and are based on two main factors:

1. Suppliers and their components often enjoy a high level of trust and extensive rights.
2. There is often insufficient transparency about the exact composition of these components.

This combination means that companies are hardly in a position to proactively recognise risks in the IT supply chain or ward off corresponding attacks. Instead, they have to rely largely on their suppliers.
‘Software Bills of Materials (SBOMs) offer a solution here by providing a detailed list of the software components used in a device, software or service, thereby increasing the transparency of the supply chain. This enables companies to assess potential security vulnerabilities themselves, as automatically as possible, and take targeted protective measures.

SBOMs also provide information about the licences of the components used and thus support the comparison of actual usage with the licence specifications. In the future, SBOMs could also help to increase transparency in data protection by providing information on which data is processed and stored by which systems.

In Germany, there are currently no explicit civil law or regulatory requirements for the creation and use of SBOMs. However, it can be argued that SBOMs are part of the ‘state of the art' as required by various laws. In addition, the Cyber Resilience Act (CRA) being prepared by the European Commission will oblige manufacturers to provide SBOMs for products sold in the EU. In the USA, an Executive Order from May 2021 has already made the provision and use of SBOMs mandatory for software supplied to the U.S. Administration. Companies should therefore already include clauses on the obligation to provide and automate SBOMs in their contracts with software suppliers and service providers.

The TeleTrusT Guideline ‘Software Bill of Materials' (SBOM) also describes available SBOM tools as well as future requirements for these tools in order to further improve IT security in particular.

2 Einleitung und Motivation

Seit einigen Jahren wird verstärkt über Angriffe durch die IT Supply Chain berichtet. Der Erfolg dieser Angriffe beruht im Wesentlichen auf zwei Aspekten:

1. Lieferanten bzw. zugelieferte Komponenten aus der IT Supply Chain genießen einen besonderen Vertrauensstatus, meist verbunden mit weitgehenden Rechten.
2. Transparenz über die genauen Inhalte der Komponenten der Zulieferungen ist bis auf wenige Ausnahmen nicht oder allenfalls unzulänglich gegeben.

Die Kombination dieser beiden Aspekte ist fatal, denn Anwenderunternehmen haben dadurch praktisch keine eigene Möglichkeit zur proaktiven Erkennung von Risiken über die IT Supply Chain und Vorsorge vor bzw. Abwehr von entsprechenden Angriffen, sondern müssen sich fast vollständig auf den Zulieferer verlassen.

"Software Bills of Materials" (SBOMs) liefern eine Inhaltsangabe für ausgelieferte bzw. zur Diensterbringung eingesetzte Software, d.h. eine Liste der durch eine Software oder einen Dienst genutzten Software-Komponenten. Sie erhöhen damit die Transparenz der Supply Chain. Diese Transparenz kann (und sollte) vom Anwenderunternehmen für eine eigene Einschätzung möglicher Sicherheitslücken und Risiken genutzt werden und ermöglicht dadurch auch eigene gezielte Maßnahmen zum Schutz vor Angriffen, die über die Supply Chain "importierte" Sicherheitslücken ausnutzen. Hierbei ist ein möglichst hoher Automatisierungsgrad von Vorteil.

Im Leitfaden "Cloud Supply Chain Security" hat die TeleTrusT-AG "Cloud Security" bereits erste Hinweise zum Einsatz von SBOMs zur Verbesserung der IT-Sicherheit gegeben. Dieser Leitfaden geht detaillierter auf SBOMs ein, um ein umfassenderes Verständnis dieses Konzeptes zu vermitteln. Vorgestellt werden auch verfügbare Tools und Ressourcen, die bei der Umsetzung einer SBOM-Strategie unterstützen können, sowie ein Ausblick auf künftig wünschenswerte Funktionalitäten dieser Werkzeuge.

3 Was ist eine "Software Bill of Materials"?

Eine SBOM ist ein strukturiertes, maschinenlesbares Dokument, eine Datei oder eine Datenbank, das oder die eine umfassende und detaillierte Aufschlüsselung aller Komponenten und Abhängigkeiten einer Softwareanwendung enthält. Ähnlich wie eine Stückliste in der Fertigungsindustrie, listet eine SBOM alle einzelnen Bestandteile einer Software auf, einschließlich der Bibliotheken, Frameworks, Module, APIs und externen Komponenten, die zur Entwicklung und Funktionsweise der Anwendung beitragen.

Eine SBOM ist damit im Wesentlichen eine Stückliste für Software. Sie bietet eine vollständige Übersicht über die Bestandteile einer Anwendung und deren Beziehungen zueinander. Jede Komponente wird sorgfältig dokumentiert, einschließlich Versionsnummern, Lizenzinformationen und weiteren relevanten Metadaten. Diese Informationen ermöglichen eine präzise Identifikation und Verfolgung von Softwarekomponenten[1].

[1] Siehe auch
- BSI Technical Guideline TR-03183 Part 2, Section 3.1
- U.S. Executive Order 14028 on Improving the Nation’s Cybersecurity, May 12, 2021, Section 10 lit. j

4 Einsatzbereiche von SBOMs

Verbesserung der IT-Sicherheit

SBOMs ermöglichen durch den Abgleich mit Listen bekannter Schwachstellen die Identifikation von Sicherheitsrisiken, die durch eingebrachte Komponenten entstanden sind. Diese Information kann in verschiedenen Phasen des Software Life Cycles zur Verbesserung der IT-Sicherheit eingesetzt werden:

- Software-Architekten nutzen die Informationen beim Design der Software-Architektur, z.B. bei der Auswahl von einzubindenden Komponenten und Modulen.
- Programmierer nutzen die Informationen zur gezielten Vermeidung bekannter Schwachstellen in genutzten Komponenten, z.B. durch den Einbau von Work-arounds oder zusätzlich eingebrachte Prüfungen.
- IT-Administratoren nutzen die Informationen für Maßnahmen gegen die Ausnutzung bekannter Schwachstellen, z.B. durch Beschränkung von Zugriffen oder Deaktivierung einzelner Komponenten einer Software.
- CISOs nutzen die Informationen zur Risikoeinschätzung der in ihrer Organisation eingesetzten Software und Veranlassung geeigneter Maßnahmen zur Risikominimierung.

Lizenzmanagement und Compliance

Unternehmen sind verpflichtet, die Verwendung von Open Source Software oder kommerziellen Softwarelizenzen zu überwachen und sicherzustellen, dass sie den entsprechenden Lizenzbedingungen entsprechen. SBOMs liefern auch Informationen über die Softwarelizenzen genutzter Komponenten. Sie helfen dadurch beim Abgleich der tatsächlichen Nutzung mit den Lizenzbedingungen.

Künftig: Datenschutz

SBOMs haben das Potenzial, die Transparenz darüber zu erhöhen, welche Daten von wem verarbeitet und gespeichert werden. Hierfür wäre es jedoch erforderlich, dass SBOMs nicht nur Informationen über verwendete Softwaremodule enthalten, sondern auch über andere Bestandteile der IT-Lieferkette, wie beispielsweise genutzte Rechenzentren, Hardware und eingebundene Cloud-Dienste.

5 Anforderungen an SBOMs

Die Anforderungen an eine SBOM sind vielfältig und reichen von der Standardisierung bzw. Interoperabilität von Datenstrukturen über Automatisierbarkeit bis hin zur Dokumentation. Durch die Umsetzung dieser Anforderungen können Organisationen eine umfassende Transparenz über ihre Softwareumgebung erreichen. Die SBOM wird so zu einem wesentlichen Werkzeug, um die Sicherheit, Compliance und Effizienz in der Software-Lieferkette deutlich zu steigern.

Eine SBOM ist somit nicht rein als eine Liste von Daten zu sehen, sondern als Ökosystem aus Prozessen, die ihre effiziente Erstellung, Verteilung und Nutzung ermöglichen.

SBOMs spielen sowohl bei der Beantwortung der folgenden Fragen im Softwareentwicklungsprozess als auch bei der Betrachtung der Risiken der aktuell genutzten Software eine entscheidende Rolle:

- Welche Komponenten sind in der Software enthalten?
  Die SBOM gibt eine umfassende Antwort darauf, welche Softwareelemente in einer Anwendung integriert sind, einschließlich aller Abhängigkeiten.
- Sind alle Softwarekomponenten auf dem neuesten Stand?
  Durch die Versionskontrolle ermöglicht die SBOM eine schnelle Überprüfung, ob alle Softwarekomponenten auf dem aktuellen Stand sind und gegebenenfalls aktualisiert werden müssen. Vor allem bei der Beantwortung der Frage, ob die eingesetzte Software von neuen CVEs betroffen ist, spielt eine SBOM eine entscheidende Rolle. Eine Antwort könnte auch sein, dass bestimmte frühere Versionen bis zum Vorliegen von aktuellen Patches noch nicht aktualisiert werden sollten, da sie für die neuen CVEs noch nicht anfällig sind.
- Welche Lizenzbedingungen gelten für die Software?
  Die SBOM liefert klare Informationen über die Lizenzierung, um sicherzustellen, dass die rechtlichen Anforderungen erfüllt sind und keine unerwünschten rechtlichen Konflikte entstehen.

5.1 Datenfelder

Eine grundlegende Anforderung an SBOMs liegt in den Datenfeldern. Diese müssen eine konsistente und einheitliche Struktur aufweisen, um Informationen über jede Softwarekomponente zu erfassen. Wichtig ist, dass die Datenfelder alle Informationen enthalten, die benötigt werden, um eine eindeutige Identifikation und Verfolgung der Komponenten über die gesamte Softwarelieferkette zu ermöglichen. Zu den grundlegenden Informationen gehören z.B. der Name des Lieferanten, der Name der Softwarekomponenten und die Versionsnummer der Komponente.

5.2 Automatisierung

SBOMs müssen in einem maschinenlesbaren Datenformat wie SPDX oder CycloneDX vorliegen, um eine automatisierte Auswertung und entsprechende Skalierung zu ermöglichen. Gleichzeitig fördert die Verwendung von interoperablen Datenformaten einen reibungsglosen Austausch der SBOMS über Unternehmensgrenzen hinweg. Der Einsatz von proprietären Datenformaten hingegen sollte vermieden werden.

5.3 Praktiken und Prozesse

Um SBOMs erfolgreich in den sicheren Entwicklungszyklus zu integrieren, sind klare Prozesse und Praktiken erforderlich. So muss z.B. festgelegt werden, in welcher Häufigkeit Aktualisierungen nötig werden, bis in welche Tiefe die transitiven Abhängigkeiten aufgelistet werden sollen oder wie die SBOM verteilt bzw. ausgeliefert werden kann. Die Beantwortung dieser Fragen kann dabei stark vom Einsatzszenario der vertriebenen Software abhängen. Auf derzeit verfügbare Tools, die funktionale und prozessuale SBOM-Mechanismen zur Verfügung stellen, geht dieser Leitfaden weiter unten ein.

6 Rechtlicher Rahmen

6.1 Allgemeine gesetzliche Anforderungen

Bislang gibt es in Deutschland weder ausdrückliche zivilrechtliche noch regulatorische Vorgaben zu SBOM. Zwar gibt es bislang auch schon Gesetze, die zu einer IT-Sicherheit nach dem "Stand der Technik"[2] verpflichten (z.B. Art 32 DSGVO, §8a Abs. 1 BSIG, § 11 Abs. 1e EnWG, § 165 TKG, § 19 Abs. 4 TDDDG). Auch andere Normen formulieren Anforderungen an die IT-Sicherheit. So gehört es gemäß § 327e Abs. 3 Nr. 2 BGB zu den objektiven Anforderungen von digitalen Produkten, dass diese die "Sicherheit" aufweisen, "die bei digitalen Produkten derselben Art üblich ist und die der Verbraucher unter Berücksichtigung der Art des digitalen Produkts erwarten kann". Weitere rechtliche Verpflichtungen ergeben sich aus branchenspezifischen Regularien, etwa MaRisk und BAIT für den Finanzsektor.

Es ist jedoch nicht zwingend, dass solche gesetzlichen Regelungen in jedem Fall zur Erstellung und Vorhaltung von SBOMs verpflichten. Die Formulierungen sind jeweils abstrakt, stehen häufig unter dem Vorbehalt der "Zumutbarkeit" oder der "Angemessenheit" und sind bisher kaum durch die Rechtsprechung konkretisiert worden. Zwar kann grundsätzlich argumentiert werden, dass SBOMs zum Stand der Technik gehören (so auch im TeleTrusT-Leitfaden zum "Stand der Technik", S. 111), ob ein Gericht aber angesichts des Angemessenheitsvorbehalts zu dem Ergebnis kommen würde, dass SBOMs für jede Software/jedes IoT-Produkt in jedem Einzelfall nach dem Stand der Technik zwingend sind, kann mangels Referenzrechtsprechung derzeit kaum vorhergesagt werden. Grob zusammengefasst lässt sich daher derzeit nur festhalten, dass je sensibler die Software und je höher die mit dem Einsatz der Software verbundenen Risiken sind, desto eher ist es unter einem der oben genannten Gesetzes rechtlich zwingend, eine SBOM zu erstellen und zu aktualisieren.

Offen bleibt damit auch, in welchem Detaillierungsgrad, in welchem Format etc. SBOMs rechtlich verpflichtend sind und ob nur der Anwender der Software bzw. der für die Datenverarbeitung Verantwortliche verpflichtet ist, SBOMs vorzuhalten, oder ob dies auch für jeden Lieferanten und Entwickler gilt.

Vor dem Hintergrund dieser erheblichen Rechtsunsicherheit ist die aktuelle EU-Gesetzgebung zu begrüßen, die dies insbesondere durch den CRA ändern wird (siehe unter 6.1.1). Soweit die neue EU-Gesetzgebung noch nicht in Kraft getreten oder nicht anwendbar ist, sollten Vertragsklauseln in die Verträge mit Softwarelieferanten aufgenommen werden, um die Verpflichtung zur Lieferung von SBOMs festzulegen (siehe 6.2).

6.1.1 Cyber Resilience Act

Seitens der Europäischen Kommission ist die "Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen", der sogenannte "Cyber Resilience Act" ("CRA"), in Vorbereitung. Ziel des Rechtsaktes ist eine sektorübergreifende Regulierung von Produkten mit digitalen Elementen, also z.B. IoT-Geräte und Apps/Softwareapplikationen. Es handelt sich also um Produktsicherheitsrecht, das für alle vernetzten Produkte gilt, die in Europa hergestellt, nach Europa importiert oder in Europa vertrieben werden. Der CRA gilt sowohl im B2B- als auch im B2C-Bereich. Während in einem ersten Entwurf des CRA der Bereich des Cloud Computing noch vom Anwendungsbereich ausgenommen war (vgl. Erwägungsgrund 9 im Kommissionsentwurf), ist dieser Ausschluss in den aktuellen Entwürfen nicht mehr enthalten. Dies bedeutet, dass das Cloud-Backend einer App oder eines anderen Produkts mit digitalen Elementen unter den CRA fällt. Lediglich die rein interne IT eines Unternehmens oder einer Behörde, die nicht als Bestandteil eines "Produkts" an Dritte vermarktet wird, ist vom Anwendungsbereich des CRA ausgenommen. Darüber hinaus gibt es Bereichsausnahmen für einzelne Branchen, die bereits intensiver reguliert sind (z.B. Automotive und Medizinprodukte).

Hersteller sind gemäß Art. 10 Nr. 1 CRA in Verbindung mit Anhang I Nr. 2. (1) CRA verpflichtet, eine Software-Stückliste ("Software Bill of Materials", SBOM) zu erstellen. SBOM wird definiert als "*formale Aufzeichnung der Einzelheiten und Lieferkettenbeziehungen der Komponenten, die in den Softwareelementen eines Produkts mit digitalen Elementen enthalten sind*" (Art 3 Abs. 37 CRA). Weitere Konkretisierungen hinsichtlich des Formats und der Elemente der SBOM werden voraussichtlich von der Kommission im Wege von Durchführungsrechtsakten festgelegt.

Ein Importeur ist verpflichtet, nur solche Produkte mit digitalen Elementen in die EU einzuführen, die über eine SBOM verfügen (Art. 13 Nr. 1 i.V.m. Anhang I Nr. 2. (1) MRL). Der Verkäufer muss z.B. sicherstellen, dass das Produkt mit digitalen Elementen mit einer CE-Kennzeichnung versehen ist (die nur angebracht werden darf, wenn für das Produkt

[2] Siehe hierzu die TeleTrusT-Handreichung zum "Stand der Technik" (2023): https://www.teletrust.de/fileadmin/user_upload/2023-05_TeleTrusT-Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DE.pdf

SBOM vorliegen). Darüber hinaus darf der Verkäufer ein Produkt mit digitalen Elementen nicht verkaufen, wenn er Grund zu der Annahme hat, dass keine SBOMs mitgeliefert werden; eine positive Nachforschungspflicht des Verkäufers besteht jedoch nicht (Art. 14 Abs. 12 (b) und Abs. 3 CRA).

Verstöße gegen diese Pflichten können mit hohen Geldbußen von bis zu 15 Mio. EUR geahndet werden (Art. 53 CRA).

Der Cyber Resilience Act wird voraussichtlich noch 2024 in Kraft treten. Ab dem Zeitpunkt des Inkrafttretens gilt eine Übergangsfrist von 24 Monaten für die Pflicht zur Erstellung eines SBOM (Art. 55 CRA). Nach Ablauf dieser Übergangsfrist gilt der Rechtsakt unmittelbar in allen Mitgliedsstaaten.

6.1.2 KRITIS-Gesetzgebung

Grundsätzlich gelten für die Betreiber von Anlagen der Kritischen Infrastruktur noch höhere Anforderungen an die IT-Sicherheit gemäß BSIG i.v. mit den Branchenspezifischen Sicherheitsstandards (B3S). Gleichwohl enthält weder der Gesetzeswortlaut des BSIG noch ein B3S-Standard die explizite Verpflichtung zum Einsatz von SBOMs.

6.1.3 DORA, EBA-Guidelines und andere behördliche Vorgaben der Bankregulierung

Für den Finanz- und Versicherungssektor gibt es außerhalb des KRITIS-Bereichs bislang bereits relativ detaillierte gesetzliche und regulatorische Vorgaben zur IT-Sicherheit. Der Digital Operational Resilience Act (DORA) enthält umfangreiche organisatorische Verpflichtungen zur Stärkung der digitalen operationalen Resilienz der genannten Sektoren. Spezifische Vorgaben zu SBOMs sind im Text des DORA gleichwohl nicht enthalten. Gleiches gilt für die Leitlinien der Europäischen Bankenaufsichtsbehörde ("EBA") zum Management von IKT- und Sicherheitsrisiken. Diese enthalten zwar detaillierte Anforderungen, die Banken bei der Auslagerung von IT-Dienstleistungen gegenüber ihren Dienstleistern stellen müssen, jedoch keine Verpflichtungen zu SBOMs. Auch die entsprechenden Vorgaben der BaFin (insbesondere MaRisk und BAIT), gehen zwar von allen in diesem Abschnitt verwendeten Standards am detailliertesten auf "Softwarekomponenten" und selbst betriebene oder entwickelte IT-Systeme ein (BA IT, Abs. 2 Nr. 1.2 lit. f), jedoch wiederum nicht auf SBOMs.

6.1.4 Gesetzliche Regelung in den USA

Die U.S. Administration hat durch eine Executive Order im Mai 2021, die später durch das U.S. Department of Commerce und das U.S. National Institute of Standards and Technology (NIST) konkretisiert wurde, die Bereitstellung und Verwendung von SBOMs durch Lieferanten der U.S. Administration vorgeschrieben. Jeder Lieferant von Software, die an die U.S. Administration geliefert oder von dieser genutzt wird, muss danach SBOMs bei der Entwicklung einsetzen und mit der Software bereitstellen.

6.2 Vertragliche Regelungen

Typische Vertragsmuster und viele gängige Standardbedingungen von Softwareanbietern enthalten bislang keine expliziten Regelungen zu SBOMs. Vertragliche Klauseln zur Einbeziehung von Open-Source-Komponenten in Anlagen (z.B. in Softwareentwicklungsverträgen oder in Softwarelizenzverträgen) sind jedoch bereits relativ häufig anzutreffen. Solche Klauseln sind in den letzten ca. 20 Jahren entstanden, da sich in juristischen Kreisen ein zunehmendes Bewusstsein im Bereich Open Source Compliance durchgesetzt hat. Ziel dieser Klauseln ist es, die Verpflichtungen aus Open-Source-Lizenzen zu erfassen und zu erfüllen (daher z.B. häufig Vorgaben zur genauen Bezeichnung der Lizenzen). Das Thema IT-Sicherheit spielt dabei eher eine untergeordnete Rolle (weshalb z.B. die Versionsnummer der Open-Source-Komponente häufig nicht angegeben wird).

Da auch deutsche und europäische Gesetzgeber (außerhalb des CRA) keine verpflichtende Regelung zur Mitlieferung von SBOM geschaffen haben, sollten entsprechende Verpflichtungen durch individuelle Klauseln in einem Vertrag aufgenommen werden. Eine solche Klausel sollte Regelungen zu folgenden Aspekten enthalten:

- Ausdrückliche Verpflichtung zur Lieferung von vollständigen SBOMs (inklusive Definition von SBOM und Regeln dazu, was "vollständig" bedeutet (z.B. mindestens "first level dependencies")

- Verpflichtung zur Aktualisierung der SBOM (ggf. Detailregelung zum Turnus der Aktualisierung)
- Festlegung eines Datenformats und der erforderlichen Metainformationen für jede Softwarekomponente (ggf. durch einen Verweis auf einen bestehenden Standard)
- Bei Softwareentwicklung bzw. Implementierung/Customizing sollte die Lieferung von SBOMs zur Voraussetzung der Abnahme und zum Gegenstand der Abnahme gemacht werden.

6.3 Datenschutz

Datenschutz kann bei einer SBOM eine Rolle spielen, wenn die Software oder verwendete Komponenten personenbezogene Daten verarbeiten oder speichern. In diesem Fall sollten Anbieter und Nutzer von SBOMs erwägen, auch die Aufnahme von Informationen über die Datenschutzmaßnahmen und -risiken der Software durchzuführen oder zu fordern, wie z.B.:

- Welche Art von personenbezogenen Daten können von der Software erhoben, verarbeitet oder gespeichert werden?
- Wie werden diese Daten geschützt, verschlüsselt oder anonymisiert?
- Wo und wie lange werden diese Daten aufbewahrt oder gelöscht?
- Wer hat Zugriff auf diese Daten und zu welchem Zweck?
- Wie werden die Datenübertragungen zwischen den Komponenten der Software oder zu externen Diensten gesichert?
- Welche Datenschutzrechte und -pflichten haben die Nutzer oder Betroffenen der Software?

6.4 Anforderungen aus Normen

Als Ergänzung zur ISO 27001:2022 (Informationssicherheit, Cybersicherheit und Datenschutz - Informationssicherheitsmanagementsysteme - Anforderungen) greift die ISO 27002:2022 die Sicherheitsmaßnahmen aus Anhang A der ISO 27001 auf und spezifiziert diese.

Es gibt hier zwar keine expliziten Anforderungen an den Einsatz von SBOMs, die Abschnitte zum Management der Informationssicherheit in IKT-Lieferketten (Control 5.21) und Management von technischen Schwachstellen (Control 8.8) fordern aber Methoden, um die Herkunft auch von Softwarekomponenten in der Lieferkette zu verfolgen sowie zur Meldung von Schwachstellen.

6.5 Anforderungen aus sonstigen Dokumenten

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat Anfang August 2023 Teil 2 der Technischen Richtlinie TR-03183 "Cyber-Resilienz-Anforderungen" veröffentlicht. In dem Dokument sind formelle und fachliche Vorgaben für Software-Stücklisten (SBOMs) enthalten, die Softwareherstellern als Empfehlung zur Gestaltung von SBOMs zur Erhöhung der Sicherheit in der Software-Lieferkette dienen sollen.

7 SBOM-Datenformate

Um Informationen, die in SBOMs gespeichert sind, automatisch auswerten und nutzen zu können, müssen SBOMs in einem maschinenlesbaren Format vorliegen. In diesem Kontext haben sich drei Formate etabliert, wovon zwei, nämlich SPDX und Cyclone DX, aus Sicht der IT-Sicherheit besonders sinnvoll erscheinen.

7.1 SPDX

SPDX steht für "Software Package Data Exchange" und ist ein Projekt der Linux Foundation, das 2010 ins Leben gerufen wurde. Ursprünglich konzentrierte sich das SPDX-Projekt auf die Lösung von Problemen im Zusammenhang mit der Einhaltung von Open-Source-Lizenzen. Im Laufe der Jahre wurde es weiterentwickelt, um den Sicherheitsherausforderungen in der Lieferkette gerecht zu werden. Viele Unternehmen und Projekte in der Softwarebranche haben die SPDX-Spezifikation übernommen.

Die SPDX-Spezifikation umfasst verschiedene Abschnitte und Felder eines SPDX-Dokuments, die wiederum in Profilen (um bestimme Use-Cases abzudecken) gebündelt sind:

- Informationen zur Dokumentenerstellung, wie Ersteller, Entstehungsinformationen und Vorwärts-/Rückwärtskompatibilität.
- Paketinformationen, die Details zum "Paket" enthalten, wie Urheber, Herkunftsort, Download-URL und Lizenzinformationen.
- Dateiinformationen, einschließlich Urheberrechten, Lizenz der Datei, Prüfsummen und Mitwirkende.
- Snippets für Inhalte, die aus anderen Quellen übernommen wurden.
- Beziehungen, die die Verbindung zwischen SPDX-Dokumenten beschreiben.

SPDX unterstützt Ausgabeformate wie JSON, YAML und XML. Am 9. September 2021 wurde SPDX als öffentlicher Standard (ISO/IEC 5962:2021) bei der Internationalen Organisation für Normung (ISO) veröffentlicht. Die aktuelle Version von SPDX, 3.0 wurde im April 2024 offiziell veröffentlicht. In der Version 3.0 wurden spezielle Ausprägungen von SPDX, sogenannte Profile, erweitert und hinzugefügt. Diese umfassen die Profile für Security, Licensing, AI, Datasets, and Software-Build-Prozesse.

7.2 Cyclone DX

CycloneDX ist ein leichtgewichtiger SBOM-Standard, der für den Anwendungssicherheitskontext und die Analyse von Lieferkettenkomponenten entwickelt wurde. Es unterstützt auch die Überprüfung der Lizenzeinhaltung und wurde 2017 in der Open Web Application Security Project (OWASP) Community initiiert.

CycloneDX bietet Schemata für XML und JSON und definiert ein Format zur Beschreibung einfacher und komplexer Softwarekomponentenzusammenstellungen. Es ist flexibel und leicht anpassbar, mit Implementierungen für gängige Build-Systeme. Die Spezifikation fördert die Verwendung von ökosystemspezifischen Namenskonventionen und unterstützt verschiedene Standards wie SPDX-Lizenz-IDs, Ausdrücke, Stamm- und externe Referenzen. CycloneDX unterstützt auch die Paket-URL-Spezifikation und die Zuordnung von Komponenten zu Common Platform Enumerations (CPEs), die in Common Vulnerabilities and Exposures (CVE) Systemen verwendet werden.

Das CycloneDX-Objektmodell beschreibt verschiedene Komponenten, darunter BOM-Metadaten, Komponenteninformationen, Informationen über Dienste, Abhängigkeitsbeziehungen, Kompositionen, Schwachstellen und Erweiterungen.

7.3 SWID

SWID ist ein vom National Institute of Standards and Technology (NIST) in den USA implementierter Standard, der 2009 veröffentlicht und 2015 überarbeitet wurde. SWID wurde entwickelt, um Unternehmen eine transparente Möglichkeit zu bieten, die auf ihren verwalteten Geräten installierte Software zu verfolgen. Die Nutzung von SWID erfolgt vorwiegend im Bereich Lizenzmanagement.

8 SBOM-Tools

SBOM-Tools lassen sich allgemein den folgenden funktionalen Gruppen zuordnen, wobei viele der SBOM-Tools mehrere Gruppen mit ihren Funktionen abdecken:

- Werkzeuge zum Erstellen von SBOMs während des Build-Prozesses,
- Analyse von Quellcode und Binärdateien zur Generierung von SBOMs,
- Bearbeitung bestehender SBOMs,
- Anzeige, Vergleich, Import und Validierung von SBOMs,
- Zusammenführung und Übersetzung von SBOM-Inhalten von einem Format oder Dateityp in ein anderes,
- Unterstützung der Integration von SBOMs in andere Tools über APIs und Bibliotheken,
- Integration mit existierenden Tools wie Schwachstellen-Scannern und Anwendungssicherheitstest-Tools,
- Erstellung von Berichten und Analysen zur Aufdeckung potenzieller Sicherheitsrisiken.

SBOMs lassen sich in Abhängigkeit des Zeitpunkts ihrer Erstellung in verschiedene Klassen unterteilen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterscheidet in der Technischen Richtlinie 03183 die folgenden Klassen:

- Design SBOM: Wird in der Entwurfsphase erstellt und enthält Informationen über geplante Komponenten.
- Source SBOM: Dokumentiert den Quellcode und seine Abhängigkeiten während der Entwicklungsphase.
- Build SBOM: Wird während des Build-Prozesses erstellt und enthält detaillierte Informationen über alle Komponenten und deren Versionen.
- Analyzed SBOM: Umfasst Ergebnisse aus Analysen und Prüfungen des Build-Artefakts.
- Deployed SBOM: Dokumentiert die tatsächlich in der Produktionsumgebung bereitgestellten Komponenten.
- Runtime SBOM: Enthält Informationen, über die zur Laufzeit verwendeten und geladenen Komponenten.

Bei der Auswahl eines geeigneten SBOM-Tools sind neben den zu unterstützenden Dateiformaten und dem gewünschten Funktionsumfang auch die Unterscheidung der verschiedenen Klassen zu berücksichtigen.

Im nachfolgenden eine unvollständige Liste von SBOM-Tools, die naturgemäß nur einen Überblick über zum Zeitpunkt der Drucklegung verfügbare Werkzeuge geben kann. Sie dient zur Orientierung, welche SBOM-Tools es im Wesentlichen derzeit gibt und in welchem Bereich sie eingesetzt werden können. Womöglich wird eine Einordnung der Funktionen vorgenommen. Eine genauere Analyse der SBOM-Tools und Auswahl muss immer im Hinblick auf den Anwendungsfall und die individuelle Entwicklungsumgebung erfolgen.

- Syft (https://github.com/anchore/syft) ist ein Tool zum Integrieren in die CI/CD Pipeline, mit dem Ziel SBOMs für Container zu erstellen.
  - Kann gepaart werden mit Grype (https://github.com/anchore/grype) als Vulnerability Scanner für Container.
  - Professionell unterstützt von Anchore SBOM Management Solutions (https://anchore.com/sbom/).
- Dependency Track von OWASP (https://dependencytrack.org/) ist eine Open Source SBOM Analyse Plattform zum Integrieren in die CI/CD Pipeline
  - Das Open Source Tool hat eine große Community, die viele Integrationen für andere Dienste bereitstellt und den Funktionsumfang stark erweitert.
  - https://github.com/DependencyTrack/hyades ist ein assoziiertes Projekt, welches Dependency Track in einfacher zu verwaltende Services aufteilt.
- SOOS (https://soos.io/) ist ein breit aufgestelltes professionelles Tool, das SBOMs erstellen, überwachen und verwalten kann. Es integriert SBOMs als einen Teil eines Dashboards für den Software Development Life Cycle.
- Rezilion SCA Dynamic SBOM (https://www.rezilion.com/platform/sca-dynamic-sbom/) ist eine weitreichende Lösung, die unter anderem die Erstellung von SBOMs sowie Analyse und Berichterstellung abdeckt.
- Gitlab CI hat eine direkte Integration, welche die Handhabung von SBOMs erleichtert.
- Gitlab selbst arbeitet an einer nativen Integration von Vulnerability Scanning und SBOM Erstellung (https://gitlab.com/groups/gitlab-org/-/epics/7886).

- Revenera SBOM Insights (https://www.revenera.com/software-composition-analysis/products/sbom-insights) ist eine SBOM Management Lösung und Teil der Revenera-Software-Composition-Analysis-Lösung.
- Snyk Open Source ist eine Lösung für die Software Composition Analysis, die unter anderem die Erstellung und Analyse von SBOMs anbietet:
  - https://snyk.io/de/product/open-source-security-management/
  - https://snyk.io/de/blog/creating-sboms-snyk-cli/
  - https://snyk.io/de/code-checker/sbom-security/
- Mend SCA (https://www.mend.io/sca/): Erstellung, Verwaltung, und Export von SBOMs.
- Cybeats SBOM Studio (https://www.cybeats.com/sbom-studio) ist eine SBOM Management Software.

9 Weiterführende Entwicklungen

"Software Bill of Materials" (SBOMs) sind ein entscheidender Schritt zur Verbesserung der Transparenz und Sicherheit in der IT-Lieferkette. Die aktuell verfügbaren Werkzeuge konzentrieren sich jedoch auf Software im engeren Sinne und berücksichtigen die erweiterten Anforderungen durch die Nutzung von Cloud Services, sei es als SaaS, über Cloud APIs oder durch die dynamische Einbindung gehosteter Softwarebibliotheken, bisher nur unzureichend oder gar nicht. Auch Bedrohungen durch Schwachstellen in der eingesetzten Hardware oder Netzwerkkomponenten werden durch SBOMs nicht berücksichtigt. Zukünftige Erweiterungen könnten deshalb folgende Aspekte umfassen:

- **Erweiterte Cloud-Integration**: SBOMs sollten die dynamische Natur von Cloud-Services berücksichtigen, indem sie nicht nur die direkt genutzte Software, sondern auch die zugrundeliegenden Authentifizierungsmechanismen, Datenflussbeschreibungen und Abhängigkeiten von tieferliegenden Cloud-Diensten dokumentieren. Solche Informationen wären essenziell, um Sicherheitsrisiken besser zu verstehen und gezielte Maßnahmen zur Absicherung der Cloud-Umgebungen zu ergreifen. Dies könnte u.a. durch die Integration von Cloud Service Maps befördert werden, die eine visuelle Darstellung der Service-Abhängigkeiten bieten.
- **Hardware- und Netzwerkkomponenten**: Die Einbeziehung von Hardware- und Netzwerkkomponenten in SBOMs ist essenziell, um ein vollständiges Bild der Sicherheitslage zu erhalten. Dies könnte durch die Erstellung von Hardware Bills of Materials (HBOMs) erfolgen, die Informationen über Hersteller, Modell, Firmware-Versionen und bekannte Schwachstellen enthalten. Dies ist besonders wichtig, weil Sicherheitslücken in der Hardware schwerwiegende und oft schwer behebbare Angriffsvektoren darstellen. Durch die Integration von HBOMs in das Sicherheitsmanagement könnten Unternehmen schneller auf Bedrohungen reagieren und ihre Abwehrmechanismen entsprechend anpassen.
- **Automatisierte Updates und Patch Management**: SBOMs bieten detaillierte Informationen über die Komponenten und Abhängigkeiten einer Software. Diese Informationen sind entscheidend für effektives Patch-Management, da sie es ermöglichen, genau zu identifizieren, welche Komponenten aktualisiert werden müssen. Im Patch-Management sollten daher Informationen aus SBOMs integriert werden, um auf neue Bedrohungen automatisiert und schnell reagieren zu können.
- **Erweiterte Sicherheitsmetriken**: Neben der Auflistung von Komponenten könnten SBOMs auch erweiterte Sicherheitsmetriken enthalten, wie z.B. das Risikoniveau von Schwachstellen oder die Compliance mit Sicherheitsstandards. Dies würde es ermöglichen, die Sicherheit von Softwareprodukten quantitativ zu bewerten und diese Bewertung in die Bewertung der Gesamtlage und Ableitung von Maßnahmen einfließen zu lassen.
- **Integration von KI und maschinellem Lernen**: Künstliche Intelligenz und maschinelles Lernen könnten genutzt werden, um Muster und Anomalien in SBOMs zu erkennen, die auf potenzielle Sicherheitsrisiken hinweisen. Dies würde eine proaktive Sicherheitsüberwachung ermöglichen.
- **Datenschutz**: SBOMs haben das Potenzial, die Transparenz darüber zu erhöhen, welche Daten von wem verarbeitet und gespeichert werden. Hierfür wäre es jedoch erforderlich, dass SBOM-Werkzeuge nicht nur Informationen über verwendete Softwaremodule enthalten, sondern auch über andere Bestandteile der IT-Lieferkette, wie beispielsweise genutzte Rechenzentren, ggf. deren Standorte, Hardware und eingebundene Cloud-Dienste.

Diese Erweiterungen würden SBOMs zu einem noch mächtigeren Werkzeug in der Bekämpfung von Sicherheitsrisiken in der IT-Lieferkette machen. Sie würden nicht nur die Sichtbarkeit erhöhen, sondern auch die Reaktionsfähigkeit auf Bedrohungen verbessern und dadurch einen umfassenderen Schutz ermöglichen.

10 Empfehlungen

SBOMs sind ein relativ neues Werkzeug der IT-Sicherheit. Der Einsatz von SBOMs ist daher eher am Beginn seiner Entwicklung. Entsprechend werden sich die Einsatzmöglichkeiten in den kommenden Jahren noch deutlich erweitern.

Die Empfehlungen gelten für alle Bereiche, die mit SBOMs in Berührung kommen (Anwender, Softwareentwickler und Entwickler von SBOM-Werkzeugen). SBOM-Werkzeuge und die von ihnen genutzten Datenquellen müssen, wie jede Software, regelmäßig aktualisiert werden. Ebenso sollten die relevanten Prozesse bei Entwicklern und Anwendern wiederkehrend überprüft und um für die Nutzung und Erzeugung von SBOMs relevanten Schritte erweitert werden. Dies betrifft auch Rahmenwerke zur sicheren Softwareentwicklung und Rahmenwerke für Informationssicherheit und Compliance. Des Weiteren müssen Mitarbeiter in relevanten Abteilungen wie Entwicklung, Einkauf, IT und Compliance in der Anwendung der relevanten Werkzeuge geschult werden. Generell sollten Formate und Werkzeuge wie die hier beschriebenen genutzt werden, um eine weitere Nutzung der SBOMs zu vereinfachen.

Gerade im Bereich der Softwareentwicklung sollten SBOMs in bestehende Prozesse integriert werden. Hier sind insbesondere Abläufe der kontinuierlichen Integration und kontinuierlichen Auslieferung geeignet, in die eine automatische Überprüfung auf bekannte Sicherheitslücken in genutzten Softwarebausteinen eingebaut werden sollte. Auch für die Pflege der hierzu erforderlichen Liste der verwendeten Bausteine, zum Schwachstellenmanagement und zur Überwachung der Einhaltung von Lizenzen stehen die hier beschriebenen und weitere Werkzeuge zur Verfügung.

Im Rahmen vertraglicher Verpflichtungen, gerade in stark regulierten Bereichen, sollten Nutzer und Kunden über hierbei festgestellte Schwachstellen mit einer Bewertung und Status der Behebung so schnell als möglich informiert werden. Es sollten insbesondere jeweils detaillierte und aktuelle SBOMs in den hier beschriebenen Standardformaten, mit entsprechenden Anmerkungen zu der jeweiligen Version bereitgestellt werden.

Für Entwickler und Nutzer von Anwendungen erleichtert ein solches Vorgehen eine schnelle Identifizierung betroffener Komponenten bei Sicherheitsvorfällen, was eine schnellere und gezielte Abhilfe erleichtert.

Anwender von Software sollten verstärkt beginnen, von Entwicklern und Betreibern die Bereitstellung von SBOMs in Standardformaten zu fordern. Dies sollte in Zukunft ein wesentlicher Faktor in der Lieferantenauswahl und -bewertung sein. Relevante Abteilungen wie IT und Compliance sollten bereits jetzt in der Anwendung der relevanten Werkzeuge geschult und eingebunden werden.

Wenn SBOMs zur Verfügung gestellt werden, sollten diese regelmäßig gegen Schwachstellendatenbanken abgeglichen werden (siehe auch die Technische Richtlinie TR-03191 Common Security Advisory Framework (CSAF)[3]). So können SBOMs dann auch effektiv zur Verbesserung der IT-Sicherheit beitragen. SBOMs können dann auch bei Anwendern zur Überprüfung von Softwarelizenzierungsanforderungen und zur Erstellung von Prüfpfaden für Konformitätsprüfungen genutzt werden und um betroffene Komponenten bei Sicherheitsvorfällen schnell zu identifizieren und so eine schnellere Abhilfe zu schaffen.

Um die gewünschten Effekte zu erzielen, müssen Entwickler von SBOM-Werkzeugen insbesondere auf Benutzerfreundlichkeit und die Integration in CI/CD-Pipelines und Entwicklungsumgebungen achten. Des Weiteren sollten Werkzeuge mehrere SBOM-Formate, mehrere Plattformen und eine breite Palette von Programmiersprachen und Ökosystemen unterstützen.

SBOMs lösen nicht alle Probleme der IT-Sicherheit, sie liefern aber einen großen Beitrag zur Transparenz in der IT-Lieferkette. SBOMs sind Basis für verbesserte Einschätzung von Bedrohungen und Risiken in der IT-Lieferkette und für weitergehende Maßnahmen zur Verbesserung der IT-Sicherheit. Die Bereitstellung und Nutzung von SBOMs wird bereits jetzt oder in naher Zukunft vom Gesetzgeber in bestimmten Bereichen gefordert. Unabhängig von der gesetzlichen Situation sollten Anwender von Lieferanten die Bereitstellung von SBOMs fordern und Anbieter sollten SBOMs für alle ihre Kunden bereitstellen.

Wir empfehlen, sich rasch mit den Anforderungen auseinander zu setzen, um SBOMs in der Praxis einzusetzen.

[3] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03191/BSI-TR-03191.pdf?__blob=publicationFile&v=5

Glossar

AG	Arbeitsgruppe
BOM	Bill of Materials (Stückliste)
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz
CRA	Cyber Resilience Act
CSAF	Common Security Advisory Framework
DSGVO	EU Datenschutzgrundverordnung (Engl.: GDPR)
DORA	Digital Operational Resilience Act
ENISA	European Union Agency for Cybersecurity
EnWG	EnergiewirtschaftsgesetzHBOM Hardware Bill of Materials
ISO	International Organization for Standardization
KI	Künstliche Intelligenz
MRL	EU Maschinenrichtlinie 2006/42/EG
NTIA	National Telecommunications and Information Administration (Agentur des U.S. Department of Commerce)
OWASP	Open Web Application Security Project
SBOM	Software Bill of Materials
SPDX	Software Package Data Exchange
SWID	Software Identification Tag
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz
TKG	Telekommunikationsgesetz

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Fachleute, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Personenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie der Vertrauenszeichen "IT Security made in Germany" und "IT Security made in EU". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Telefon: +49 30 4005 4306
E-Mail: holger.muehlbauer@teletrust.de
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.