PRESSEMITTEILUNG / PUBLIKATIONSANKÜNDIGUNG

Bundesverband IT-Sicherheit e.V. (TeleTrusT) veröffentlicht Leitfaden "Software Bill of Materials"

Berlin, 27.08.2024 - "Software Bills of Materials" (SBOMs) sind ein relativ neues Werkzeug in der IT-Sicherheit. Die Einsatzmöglichkeiten werden sich in den kommenden Jahren deutlich erweitern. Der jetzt veröffentlichte TeleTrusT-Leitfaden "Software Bill of Materials" beschreibt verfügbare SBOM-Tools sowie zukünftige Anforderungen an diese Werkzeuge.

https://www.teletrust.de/publikationen/broschueren/cloud-security/

"Software Bill of Materials" 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. Lieferanten und deren Komponenten genießen oft ein hohes Vertrauen und weitgehende Rechte. 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, potentielle 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.

Oliver Dehning, Leiter der TeleTrusT-AG "Cloud Security": "Software Bills of Materials (SBOMs) sorgen für Transparenz in der IT Supply Chain. Ohne sie ist eine angemessene Einschätzung von Risiken aus IT-Diensten praktisch unmöglich. Unternehmen sollten deshalb die Bereitstellung von SBOMs konsequent von ihren IT-Lieferanten fordern und auf allen Ebenen der IT im Rahmen von Sicherheitsüberwachung und Risikomanagement nutzen. Der jetzt veröffentlichte neue TeleTrusT-Leitfaden soll dabei unterstützen."

Bundesverband IT-Sicherheit e.V. (TeleTrusT), Dr. Holger Mühlbauer, Geschäftsführer, Chausseestraße 17, 10115 Berlin, Tel.: +49 30 40054310, holger.muehlbauer@teletrust.de
https://www.teletrust.de