TeleTrusT-interner Workshop

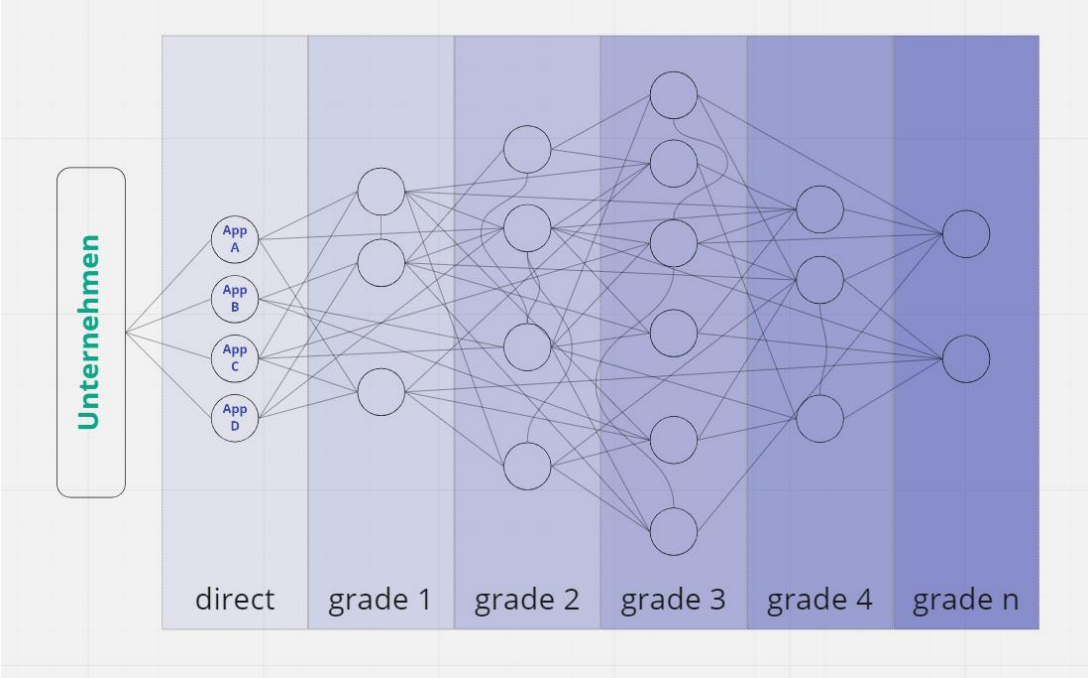
Berlin, 26. - 27.06.2024

"SBOM"

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

Sicherheitsrisiko: Mangelnde Transparenz in der IT-Lieferkette

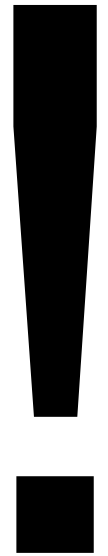
- Software und (allgemeiner) IT-Dienste bestehen aus unzählig vielen aufeinander aufbauenden Komponenten.
- Aufbau und Inhalt sind i.d.R. für Anwender vollkommen intransparent.
- Eine Bewertung der Sicherheitsrisiken aus zugelieferten IT-Komponenten und Diensten ist daher sehr schwierig bis unmöglich



Software Bill of Materials (Software-Stückliste, SBOM)

Formale und maschinenlesbare Metadaten, die ein Softwarepaket und seinen Inhalt eindeutig identifizieren

- Verständnis der Softwarezusammensetzung
- Identifikation von Abhängigkeiten
- Bewertung von Risiken
- Verfolgung von Änderungen
- Bewertung von Schwachstellen



SBOM: Einsatzbereiche

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Verbesserung der IT-Sicherheit
  - Identifikation von Sicherheitsrisiken durch den Abgleich mit Listen bekannter Schwachstellen
  - Nutzung in verschiedenen Phasen des Software-Life-Cycles:
    - beim Design der Software-Architektur,
    - zur gezielten Vermeidung bekannter Schwachstellen in genutzten Komponenten,
    - für Maßnahmen gegen die Ausnutzung bekannter Schwachstellen,
    - zur Risikoeinschätzung und Veranlassung geeigneter Maßnahmen zur Risikominimierung.
- Lizenzmanagement und Compliance
  - Überwachung der Verwendung von Open-Source-Software oder kommerziellen Softwarelizenzen
  - Abgleich der tatsächlichen Nutzung mit Lizenzbedingungen
- Künftig : Datenschutz
  - SBOMs könnten Transparenz schaffen: welche Daten werden von wem verarbeitet und gespeichert
  - Dazu müssten SBOMs auch Informationen über andere Bestandteile der IT-Lieferkette enthalten, außerhalb von Software:
    - Genutzte Hardware, Cloud-APIs, Identity-Services, …

SBOM: Rechtlicher Rahmen

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- U.S. Executive Order 14028 on Improving the Nation’s Cybersecurity
  - Klare Forderung nach SBOM
  - Vorschrift für Lieferanten an U.S. Behörden
- Allgemeine rechtliche Anforderungen
  - Bisher keine ausdrückliche Verpflichtung zu SBOM in Deutschland
  - Allerdings Berücksichtigung „Stand der Technik“ (z.B. DSGVO, BSIG, TKG)
- EU Cyber Resilience Act (CRA)
  - Sektorübergreifende Regulierung von Produkten mit digitalen Elementen
    - inklusive Cloud Backend
  - Nur rein interne IT nicht betroffen
  - Verpflichtet Hersteller (und Importeure) zur Bereitstellung von SBOMs
  - Konkretisierung hinsichtlich Format und Elementen steht noch aus
    - TR-03183 „Cyber-Resilienz-Anforderungen“ des BSI mit formellen und fachlichen Vorgaben für Software-Stücklisten
  - CRA tritt voraussichtlich 2024 in Kraft, Umsetzung innerhalb 24 Monaten
- Empfehlung: Aufnahme von SBOMs in IT Liefer- und Serviceverträge

SBOM-Tools

- 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 in ein anderes,
- Unterstützung der Integration von SBOM 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.
- Beispiele (Auszug):
  - Syft: Tool zum Integrieren in die CI/CD Pipeline, mit dem Ziel SBOMs für Container zu erstellen
  - Dependency-Track: Open Source SBOM Analyse Plattform zum Integrieren in die CI/CD Pipeline
  - SOOS : breit aufgestelltes professionelles Tool, integriert SBOMs als einen Teil eines Dashboards für den Software Development Life Cycle
  - Snyk: Lösung für die Software Composition Analysis, Erstellung und Analyse von SBOMs
  - Cybeats SBOM Studio: SBOM Management Software

Weiterführende Entwicklungen

- Erweiterte Cloud-Integration
  - Nicht nur lokal gebundene Software sondern auch Abhängigkeiten von Cloud-APIs, Authentisierungsdiensten, Datenbanken etc. beschreiben
- Hardware- und Netzwerkkomponenten
  - Hardware Bill of Materials (HBOM)
  - Informationen über Hersteller, Modell, Firmware-Versionen und bekannte Schwach-stellen
- Automatisierte Updates und Patch-Management
  - Integration von SBOMs in das Patch-Management um auf neue Bedrohungen automatisiert und schnell zu reagieren
- Erweiterte Sicherheitsmetriken
  - z.B. Risikoniveau von Schwachstellen, Compliance mit Sicherheitsstandards
  - Ermöglicht quantitative Bewertung der Sicherheit von Softwareprodukten
  - Einfluss auf die Bewertung der Gesamtlage und Ableitung von Maßnahmen
- Integration von KI und maschinellem Lernen
  - Erkennung von Muster und Anomalien in SBOMs, die auf mögliche Sicherheitsrisiken hinweisen
- Datenschutz
  - Verbesserung der Transparenz, welche Daten von wem verarbeitet und gespeichert werden