ATB. LAW

Software Bill of Materials

Aktuelle Entwicklungen

20. Österreichischer IT-Rechtstag am 7. Mai 2026

RA Dr. Stefan Knotzer, LL.M.

ATB. LAW

Moderne Softwareentwicklung als komplexes Stückwerk

- Proprietärer Code dient heute vornehmlich als „Glue Code“, der Open-Source-Bibliotheken, Frameworks und APIs verbindet.
- Ein Großteil des Codes stammt von Dritten.
- Software ist zur „Black Box“ geworden: Unternehmen wissen häufig nicht, welche Komponenten in ihren Produkten enthalten sind.
- Die Modularisierung hat die Entwicklung beschleunigt, aber massive Opazität eingeführt.

Risiken moderner Softwareentwicklung

Lizenzmanagement

- OSS-Komponenten in so gut wie jeder Anwendung
- Kompatibilität von Lizenzbestimmungen
- Copyleft > viraler Effekt > „Kontamination“
- Klare Rechtezuordnung

> Sichere Rechteketten

Cyber-Security

- Schwachstellen in verbreiteten Komponenten, oft unbekannt
- Supply-Chain-Angriffe
- Abhängigkeiten

> Sichere Lieferketten

Anknüpfungspunkte

- Mehrere gute Gründe die Bestandteile einer Software genau zu dokumentieren:
- Prüfung, ob die Berechtigungen an dem Code mit der geplanten Nutzung konformgehen → **Lizenz- und Rechtemanagement**
  - Open-Source-Compliance
  - Prüfung von Software(komponenten) bei Transaktionen ein wichtiger Bestandteil der Due Diligence geworden.
- **Aktuell stehen Aspekte der Cyber-Security im Vordergrund**
  - Der CRA verlangt ausdrücklich nach entsprechender Dokumentation.
  - Operationelle Sicherheit → Lieferkettensicherheit → zwingt Unternehmen, Betriebsabläufe anzupassen sowie ihre Verträge mit Zulieferern und Abnehmern zu prüfen / aktualisieren

Agenda

- **Befundaufnahme: Software Bill of Materials (SBOM)**
  - Kompakte Informationen zu praktischen Aspekten des Einsatzes von SBOM und zur faktischen Entwicklung des Themenbereichs

- **SBOM & Cyber-Security**
  - Fokus CRA: Anwendungsbereich, Softwareprodukte, Anforderungen an PmdE, SBOM, Abhängigkeitsbewertungen, Herstellerpflichten
  - Wechselwirkung Produkthaftung,
  - Konnex Operationelle Cybersicherheit

ATB. LAW

Befundaufnahme: Software Bill of Materials (SBOM)

What is a SBOM?

- Eine SBOM oder auch „Software-Stückliste“ ist eine maschinenlesbare Aufzeichnung aller Komponenten, aus denen ein Softwareprodukt besteht, mit Angaben zu den jeweiligen Versionen und Abhängigkeiten.
- Der wesentliche Zweck einer SBOM ist die Schaffung von Transparenz in Bezug auf die Supply-Chain des Produkts bzw einer Software.
- Regelmäßig kein statisches Dokument, sondern ein dynamischer Datensatz.
- Je nach Kontext werden in der Begriffsbildung zu „SBOM“ gewisse Nuancierungen zu berücksichtigen sein. Etwa bietet der CRA eine konkrete Definition; hingegen wird bspw im Kontext von Transaktionen allenfalls auch ein weiterer Begriff Platz greifen können (SBOM als Spezial- oder Überbegriff).

Regulatorische Treiber

Die US Executive Order 14028

- Executive Order 14028 der US-Regierung (2021) als direkte Reaktion auf Cyber-Vorfälle.
- Regierung beauftragt NTIA, “Mindestelemente” für SBOM zu definieren.
- ExOrd hat bewirkt, dass Softwarehersteller, die an US-Bundesbehörden liefern möchten, eine SBOM braucht.
- “Mindestelemente” sohin Grundlage praktisch jeder Implementierung.

EU Cyber Resilience Act (CRA)

- In Europa zieht CRA nach und etabliert noch weitreichendere Anforderungen.
- Hersteller müssen eine SBOM vorhalten, Schwachstellen effektiv managen.
- CRA betrifft den gesamten Binnenmarkt.
- Zwingt Unternehmen branchenübergreifend sich mit SBOM auseinanderzusetzen.

Mindestelemente nach NTIA

Sieben Pflichtfelder, die in jedem validen SBOM-Format enthalten sein müssen:

1. Lieferantenname: Entität, die die Komponente erstellt oder liefert.
2. Komponentenname: Der Bezeichner der Einheit (z.B. "OpenSSL").
3. Version der Komponente: Identifier der Version (z.B. "1.0.2"). Wichtig, da Schwachstellen versionsspezifisch sind.
4. Sonstige eindeutige Bezeichner: Maschinelle IDs wie PURL oder CPE.
5. Abhängigkeitsbeziehungen: Verknüpfung im Graphen (z.B. "included in").
6. Autor der SBOM-Daten: Wer hat die SBOM erstellt (Person, Organisation)?
7. Zeitstempel (Timestamp): Wann wurde die SBOM generiert?

SBOM in der Praxis

- Datenformate (SPDX & CycloneDX als Standards).
- Herausforderungen bei der Identifikation von Komponenten
- Generierung von SBOM über mehrere Phasen der Entwicklung
- Operative Workflows: Generierung von SBOM als Step in CI/CD-Pipelines
- Analyse und Operationalisierung auf Plattformen (z.B. OWASP Dependency-Track)
- Vulnerability Matching / Policy Management
- Vertrauen und Integrität von SBOM

ATB. LAW

SBOM & Cyber-Security

Cyber Resilience Act (CRA) — Übersicht

- Horizontaler Rechtsrahmen für Cyber-Security von Produkten mit digitalen Elementen
- „Security by Design“ über den gesamten Produktlebenszyklus
- Pflicht zu Schwachstellenmanagement und Sicherheitsupdates
- CE-Kennzeichnung als Marktzugangsvoraussetzung

CRA — Anwendungsbereich

- **„Produkt mit digitalen Elementen“** (Art 3 Z 1 CRA)
  ein Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die getrennt in den Verkehr gebracht werden

- Begriff: „Softwareprodukt“ und Abgrenzung
- Cloud-Dienste (SaaS) grds nicht erfasst (?) > differenzierte Beurteilung
- Begriff „Datenfernverarbeitungslösung“ iSd Art 3 Z 2 CRA

CRA — Anforderungen an PmdE

Anhang I — Teil I

Grundlegende Sicherheitsanforderungen

(Auszug)

- Keine bekannten ausnutzbaren Schwachstellen (lit. a)
- Sichere Standardkonfiguration (lit. b)
- Update-Fähigkeit für Sicherheitspatches (lit. c)
- Zugangsschutz durch Authentifizierung (lit. d)
- Verschlüsselung / Datenintegrität (lit. e, f)
- Minimale Angriffsfläche (lit. j)
- Logging sicherheitsrelevanter Ereignisse (lit. l)

Anhang I — Teil II

Schwachstellenbehandlung

(Auszug)

- **Identifikation aller Komponenten, ua durch SBOM (Z 1)** > gleich näher
- Unverzügliche Behebung durch Sicherheitsupdates (Z 2)
- Regelm Tests und Sicherheitsüberprüfungen (Z 3)
- CVD-Policy (Z 5)
- Autom Sicherheitsaktualisierungen (Z 7)
- Kostenlose Updates + Installationshinweise (Z 8)

CRA — Anforderungen an SBOM I

- ErwGr 77: „Zur Erleichterung der Schwachstellenanalyse sollten die Hersteller feststellen und dokumentieren, welche Komponenten in den Produkten mit digitalen Elementen enthalten sind, und dazu gegebenenfalls eine **Software-Stückliste aufstellen**. Über eine Software-Stückliste können denjenigen, die Software herstellen, kaufen und betreiben, Informationen bereitgestellt werden, die ihnen helfen, die Lieferkette besser zu verstehen, was zahlreiche Vorteile mit sich bringt und insbesondere Herstellern und Nutzern hilft, bekannte neu aufgetretene Schwachstellen und Cybersicherheitsrisiken zu verfolgen. Besonders wichtig ist es, dass die Hersteller sicherstellen, dass ihre Produkte mit digitalen Elementen keine anfälligen Komponenten enthalten, die von Dritten entwickelt wurden. Die Hersteller sollten nicht verpflichtet sein, die Software-Stückliste zu veröffentlichen.“

CRA — Anforderungen an SBOM II

- **Art 3 Z 39**: *„Software-Stückliste“ eine formale Aufzeichnung der **Einzelheiten** und **Lieferkettenbeziehungen** der Komponenten, die in den Softwareelementen eines Produkts mit digitalen Elementen enthalten sind*;

- **Anhang I Teil 2 Z 1**: *„Schwachstellen und Komponenten der Produkte mit digitalen Elementen ermitteln und dokumentieren, u. a. durch Erstellung einer Software-Stückliste in einem gängigen maschinenlesbaren Format, aus der **zumindest die obersten Abhängigkeiten** der Produkte hervorgehen“*

- EU-Kommission ermächtigt, Inhalt und Format per **Durchführungsrechtsakt** festzulegen (ErwGr 118, Art 13 Abs 24). Erwartbar, dass auf etablierte Formate wie SPDX oder CycloneDX zurückgegriffen wird → Interoperabilität.

CRA — Anforderungen an SBOM III

- Mindestens die **obersten Abhängigkeiten**: die direkt im Produkt verbauten Softwaremodule; optional können tiefer verschachtelte Abhängigkeiten ebenfalls aufgeführt werden, was aber (noch) nicht zwingend ist.
- SBOM = Teil der **technischen Dokumentation** des Produkts (s Art 31, Anhang VII); muss ggf auf Verlangen den Marktaufsichtsbehörden vorgelegt werden können.
- **ABER**: keine Verpflichtung, SBOM gegenüber Kunden proaktiv offenzulegen.
  - Begründung: Sicherheit; Betriebsgeheimnisschutz
  - Vgl aber Anhang II Z 9.

→ **Merke**: **SBOM dient primär interner Transparenz & behördlicher Kontrolle.**

CRA — Abhängigkeitsbewertungen

Abhängigkeitsbewertungen

- Art 13 Abs 25: „Um die Abhängigkeit […] von Softwarekomponenten und insbesondere von Komponenten, die als freie und quelloffene Software gelten, zu bewerten, kann die **ADCO** beschließen, für bestimmte Kategorien von Produkten mit digitalen Elementen eine unionsweite Bewertung der Abhängigkeit durchzuführen. Zu diesem Zweck können die Marktüberwachungsbehörden die Hersteller solcher Kategorien von Produkten mit digitalen Elementen auffordern, die entsprechenden Software-Stücklisten gemäß Anhang I Teil II Nummer 1 vorzulegen. Auf der Grundlage dieser Informationen können die Marktüberwachungsbehörden der ADCO anonymisierte und aggregierte Informationen über Softwareabhängigkeiten zur Verfügung stellen. Die ADCO legt der gemäß Artikel 14 der Richtlinie (EU) 2022/2555 eingesetzten Kooperationsgruppe einen Bericht über die Ergebnisse der Abhängigkeitsbewertung vor. “ (vgl auch ErwGr 22)

CRA — Herstellerpflichten I

Regelungsadressaten > „Wirtschaftsakteure“ > „Hersteller“

Art 13 CRA (iVm Anhang I)

- Konformität gewährleisten: Produkte müssen bei Inverkehrbringen Anhang I Teil 1 entsprechen (Abs 1)
- Bewertung der Cybersicherheitsrisiken (Abs 2, 3, 4)
- Sorgfältiger Umgang mit Komponenten Dritter, insb auch FOSS (Abs 5)
- Dokumentation aller relevanten Cybersicherheitsaspekte (Abs 7)

CRA — Herstellerpflichten II

- Schwachstellenmanagement während Unterstützungszeitraum (mind. 5 Jahre; Abs 3, 6, 8 f)
- Technische Dokumentation (Abs 12 f; Art 31, Anhang VII [Z8: ggf: SBOM])
- Konformitätsbewertung + EU-Konformitätserklärung + CE-Kennzeichnung (Art 28–30)
- 24h-Meldepflicht an ENISA/CSIRT bei aktiv ausgenutzten Schwachstellen (Art 14)
- Zusammenarbeit mit Marktüberwachungsbehörde (Abs 22 ff)

SBOM & SaaS = SaaSBOM

- CRA-Anwendungsbereich grds nicht eröffnet (zumindest fraglich; siehe oben)
- NIS-2-RL / NISG 2026
  - Für SaaS-Anbieter gelten ggf. Pflichten zum Risikomanagement, inkl Supply-Chain-Sicherheit.
- Vertragliche SBOM-Pflicht
  - SBOM-Transparenz kann vertraglich geschuldet sein, insb bei regulierten Kunden (z.B. Finanzunternehmen).
- Beispiel: CycloneDX unterstützt SaaSBOM und gilt derzeit als der führende Standard für diesen Anwendungsbereich

SBOM & AI = AI-BOM

- Zusammenspiel CRA ↔ AI Act
  - KI als PmdE unterliegt beiden Regelwerken; Art 12 CRA: CRA-konforme KI-Systeme gelten hinsichtlich Cyber-Security als AI-Act-konform (Konformitätsvermutung).
- Besondere Herausforderungen einer SBOM für AI (Auswahl)
  - Vortrainierte KI-Modelle als „Komponenten“ in der SBOM?
  - Lizenzierung von Trainingsdaten als neue SBOM-Dimension; Versionierung bei kontinuierlichem Lernen
- „SBOM for AI“ bzw „AI-BOM“ bzw „ML-BOM“:
  - SPDX und CycloneDX bieten spezifische Felder für KI-Modelle: Modellarchitekturen, Trainingsdaten, Hyperparameter, Evaluierungsmetriken.
  - „A shared G7 Vision on SBOM for AI“

CRA — Way forward

- Prüfung Anwendbarkeit des CRA → gerade bei Software mitunter heikles Thema
- Pflichten erfassen – Dokumentation anpassen. SBOM erstellen samt Methoden, um diese stets aktuell zu halten > Zweck beachten > funktionsfähige Prozesse etablieren, um gegebenenfalls rasch reagieren zu können
- Zur Gewährleistung der eigenen Pflichten > Prüfung entsprechender Vereinbarungen mit den Zulieferern, um Cybersicherheit aller Komponenten sicherzustellen.
  - ➢ Entscheidend zu regeln sind dabei neben den direkt ableitbaren Pflichten, wie z.B. zur Bewertung von Cyberrisiken, zur Bereitstellung von Sicherheitsupdates oder zu Incident Response, auch die Vereinbarung von vertraglichen Kontrollbefugnissen zur Durchsetzung der Pflichten.

Wechselwirkung Produkthaftungsrecht

- **„Stand der Technik“**: CRA-Anforderungen prägen die berechtigte Erwartungshaltung der Nutzer. Nichteinhaltung als gewichtiges Indiz für Produktfehlerhaftigkeit
- **Neue ProdHaft-RL (EU) 2024/2853**: erfasst ausdrücklich Software. Sicherheitslücken = haftungsrelevante Produktfehler.
- **Beweislast** (Art 10): Verstoß gegen Sicherheitsanforderungen (zB CRA) begründet Vermutung für Produktfehler. Fehlende SBOM = Indiz für unzureichendes Risikomanagement.
- **Verschuldensunabhängige Haftung (§ 1 PHG)**: Gefährdungshaftung. Entwicklungsrisikoeinwand (§ 8 Abs 2 PHG) greift nicht bei bekannten oder fahrlässig übersehenen Schwachstellen.

Konnex Operationelle Cybersicherheit

Lieferkettenverantwortung

NIS-2-RL / NISG 2026

- NIS-2-RL (EU) 2022/2555 richtet sich an Betreiber wesentlicher und wichtiger Einrichtungen
- Österreich: Umsetzung durch NISG 2026
- Risikomanagement muss Sicherheit der Lieferkette umfassen
- Vertragliche Absicherung: Zulieferer sind einzubinden

CRA ↔ NIS-2

- CRA = Produktgesetz (Hersteller)
- NIS-2 = Betriebspflichten (Betreiber)
- Synergie: CRA-konforme Produkte reduzieren Risiko in der Lieferkette
- Schwachstellenmeldung: CRA (Art 14) an ENISA; NIS-2 (Art 23) an nat CSIRT — können kumulativ greifen
- SaaS/Cloud-Dienste: NIS-2 statt CRA?

ATB.
LAW

Rechtsanwält:innen in Kooperation
Bauernmarkt 24, Top 15 | 1010 Wien
office@atb.law | www.atb.law

RA Dr. Stefan Knotzer, LL.M.
knotzer@atb.law