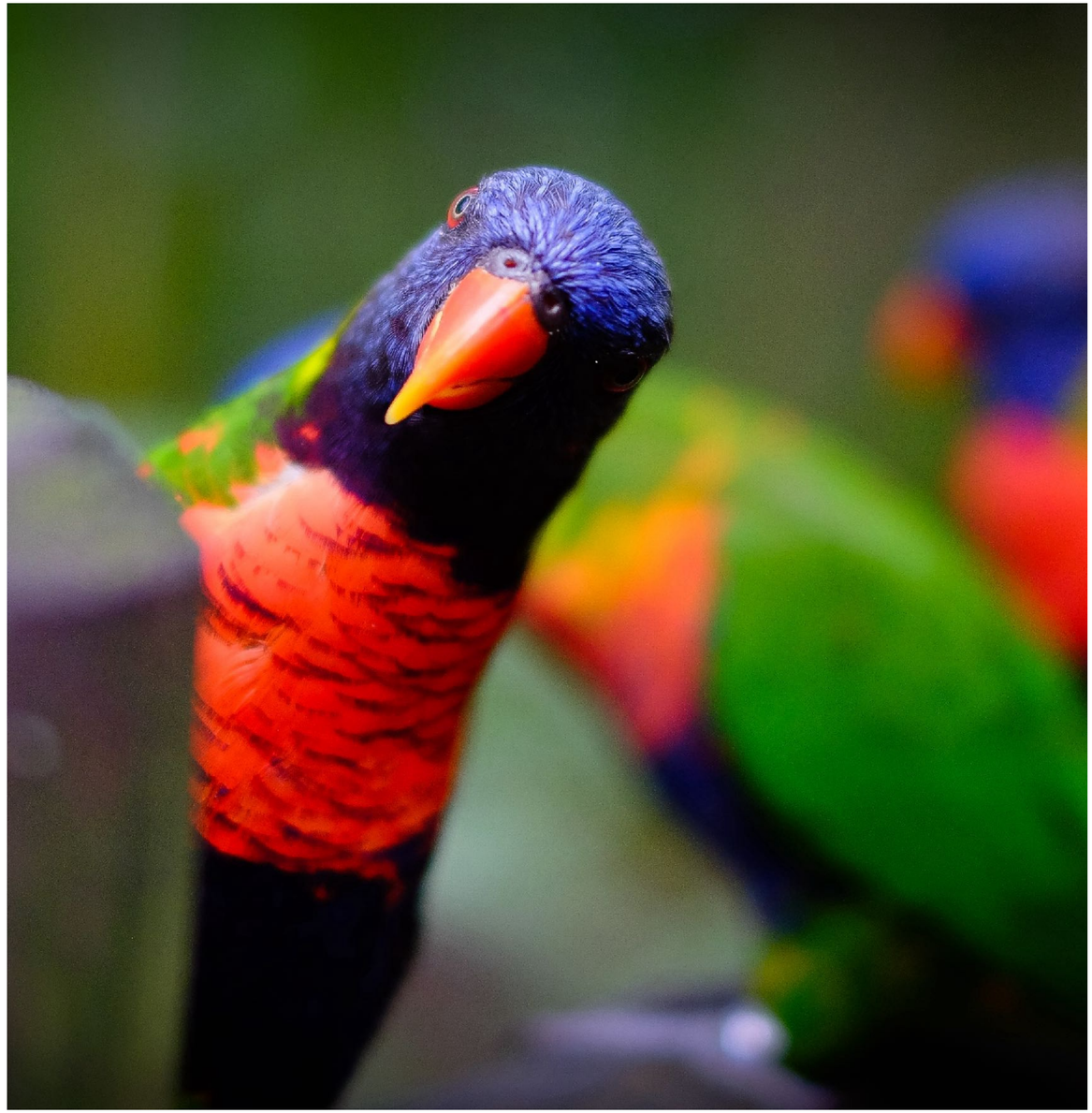
Software Bill of Materials

Inhaltsliste für Software

Sebastian Hempel • 16.05.2024

Fragen?



any questions? - (Matthias Ripp) - CC BY

Sebastian Hempel

IT CONSULTING HEMPEL

- selbständiger Software-Entwickler seit 2003
- Java, Puppet
- Linux und OpenSource

https://it-hempel.de

@sepp@chaos.social

Das Ganze ist nur so sicher wie jedes seiner Teile.

Sebastian Hempel (in Anlehnung an Aristoteles)

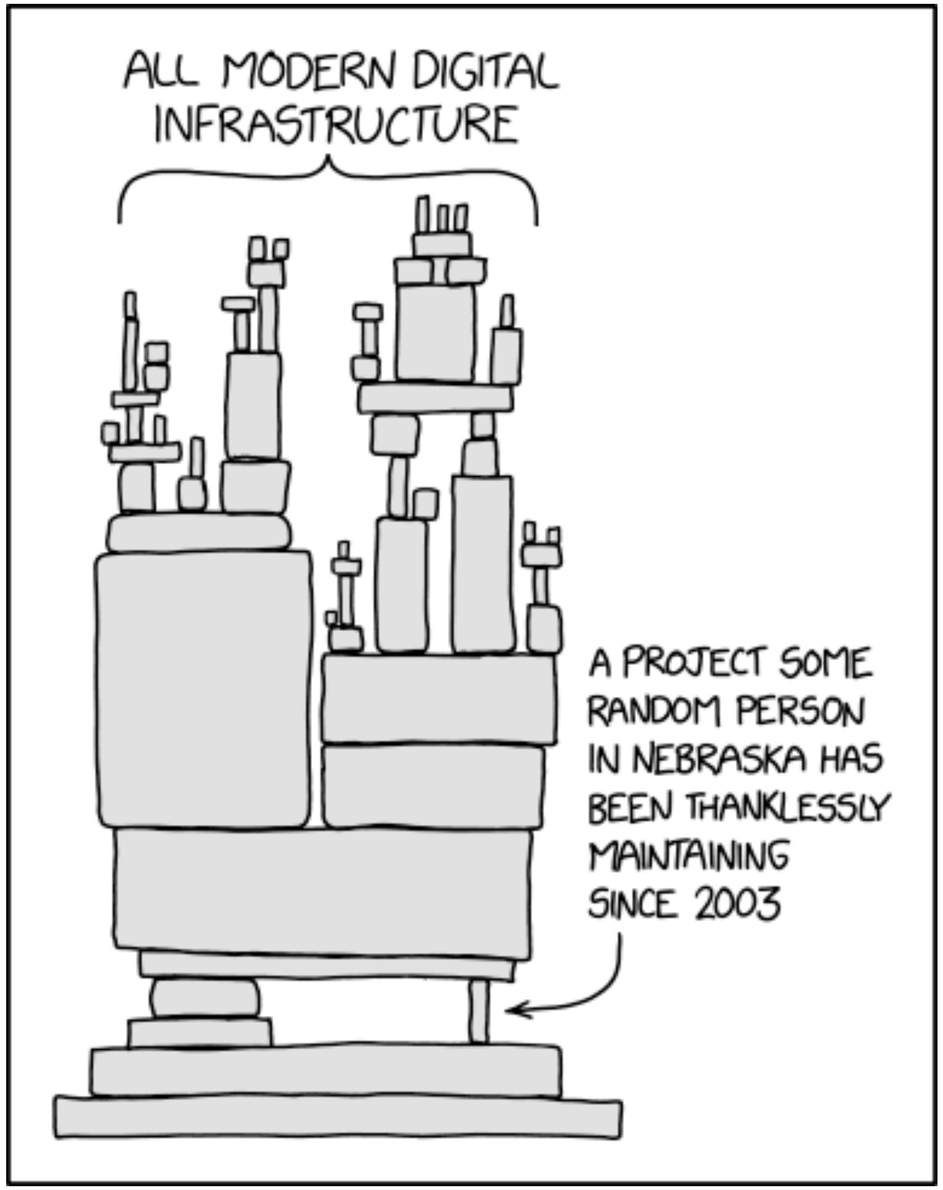
Software besteht aus mehreren Teilen

- JDK
- Framework
- Libraries
- eigene Komponenten

Software ist nie frei von Fehlern

- Bugs
- CVE (common vulnerability and exposures)

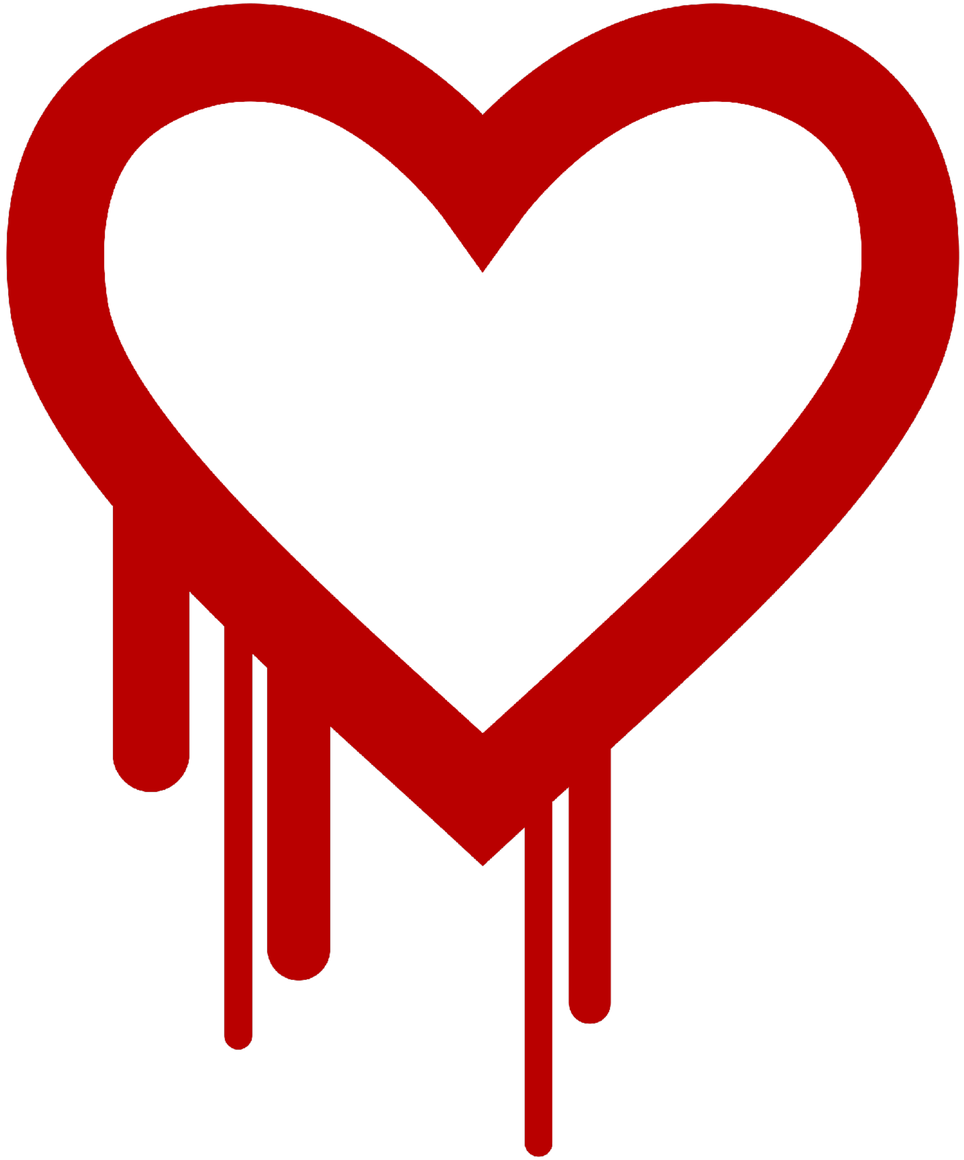
Software baut aufeinander auf



Dependency - xkcd - CC BY-NC

Berühmte Katastrophen

- Heartbleed (2014, CVE-2014-0160) - https://heartbleed.com/
- Log4Shell (2021, CVE-2021-44228)
- xz Backdoor (2024, CVE-2024-3094)



Heartbleed-Logo - Leena Snidate / Codenomicon - CC0

Es gibt einen neuen CVE

Fragen? - Beispiel Log4j

- Ist meine Software betroffen?
- Welche Software beinhaltet Log4j?
- Welche Version kommt zum Einsatz?

Fragen Antworten Fragezeichen - Peggy_Marco - Pixabay Content License

Es gibt einen neuen CVE

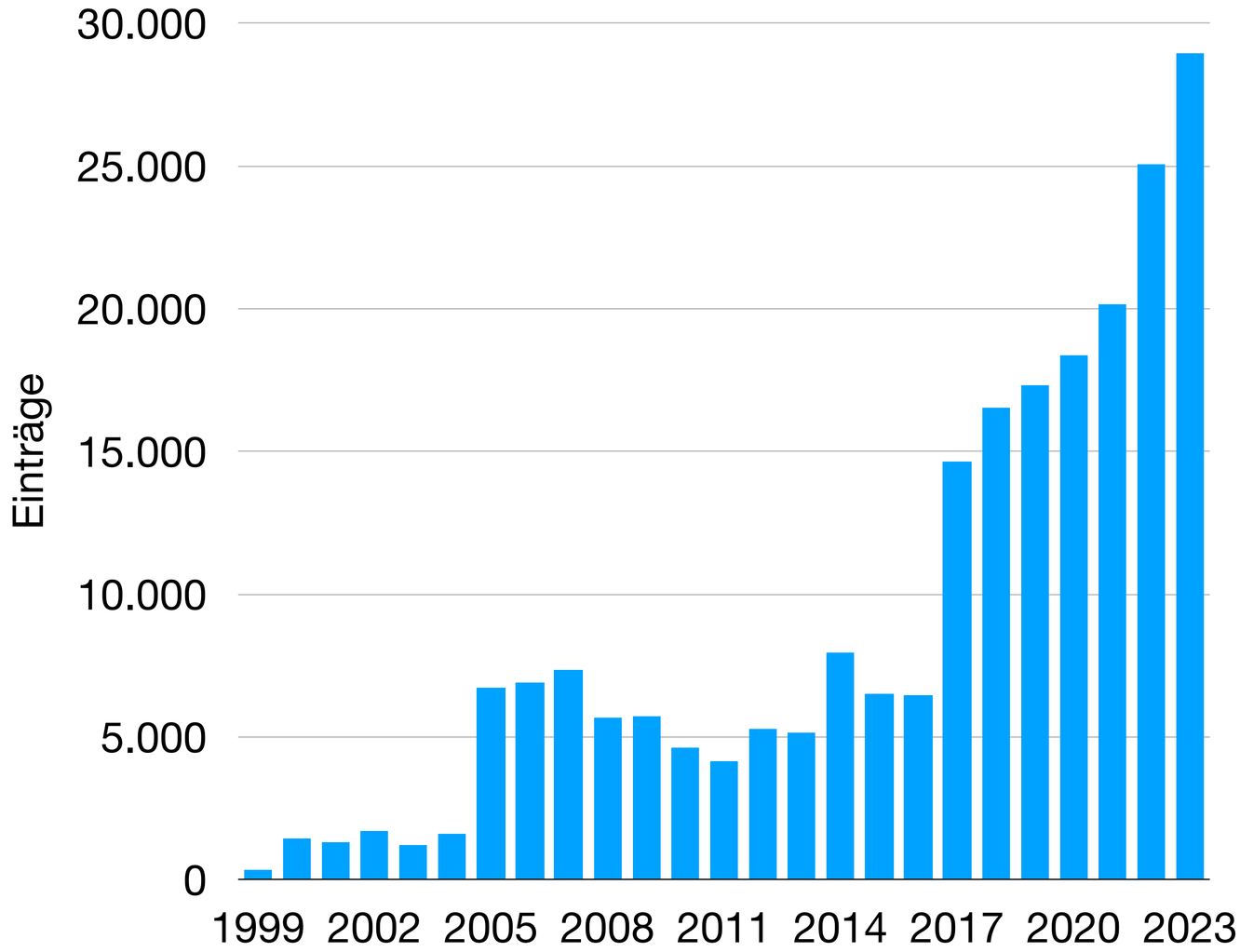
Probleme

- keine schnellen Antworten auf die Fragen
- Es vergeht wertvolle Zeit bis zur Behebung des Problems

Keine Panik Taste - TheDigitalArtist - Pixabay Content License

CVE Einträge pro Jahr

- komplexere Software
- mehr Angriffe
- mehr Untersuchung
- mehr Beachtung



https://www.cve.org/About/Metrics

Supply Chain

- Begriff aus der Logistik
- Woher kommen meine Komponenten?
- Problematisch in Bezug auf OpenSource

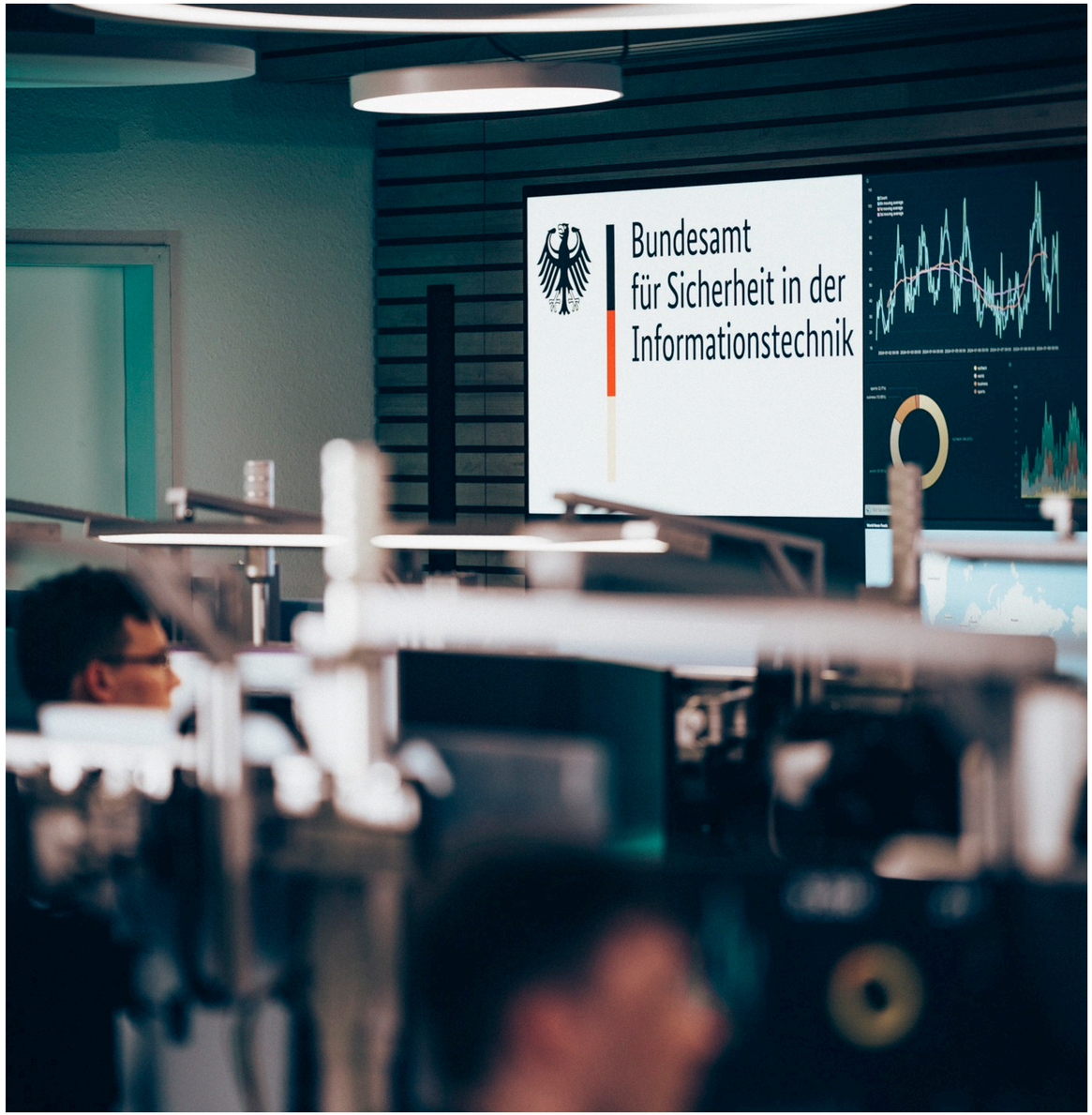
Port Loading Container - makabera - Pixabay Content License

Rechtlicher Hintergrund

Hammer Books Law - succo - Pixabay Content License

BSI

SBOM Richtlinie
TR-03183-2
04.08.2023



Nationales IT-Lagezentrum - BSI/Bernd Lammel/bundesfoto

BSI SBOM-Richtlinie

- TR-03182 „Cyber-Resilienz-Anforderungen“
- Empfehlung zur Gestaltung von SBOMs
- Verweis auf Cyber Resilience Act
- CISA (cybersecurity & infrastructure security agency)

NIS-2-Richtlinie

EU Richtlinie 2022/2555

Inkrafttreten: 16.01.2023

Anwendung: 18.10.2024

European Union Parlament - Dusan_Cvetanovic - Pixabay Content License

NIS-2-Richtlinie

- Network and Information Security (NIS)
- Regelt Cyber- und Informationssicherheit von Unternehmen in 18 Sektoren
  - Cyber-Risikomanagement
  - Sicherheit in der Lieferkette
  - …
- Richtlinie, muss in nationales Recht umgesetzt werden
- Referentenentwurf des BMI vom Juli 2023

Cyber Resilience Act (CRA)

Einigung im Trilog

European Union Parlament - Dusan_Cvetanovic - Pixabay Content License

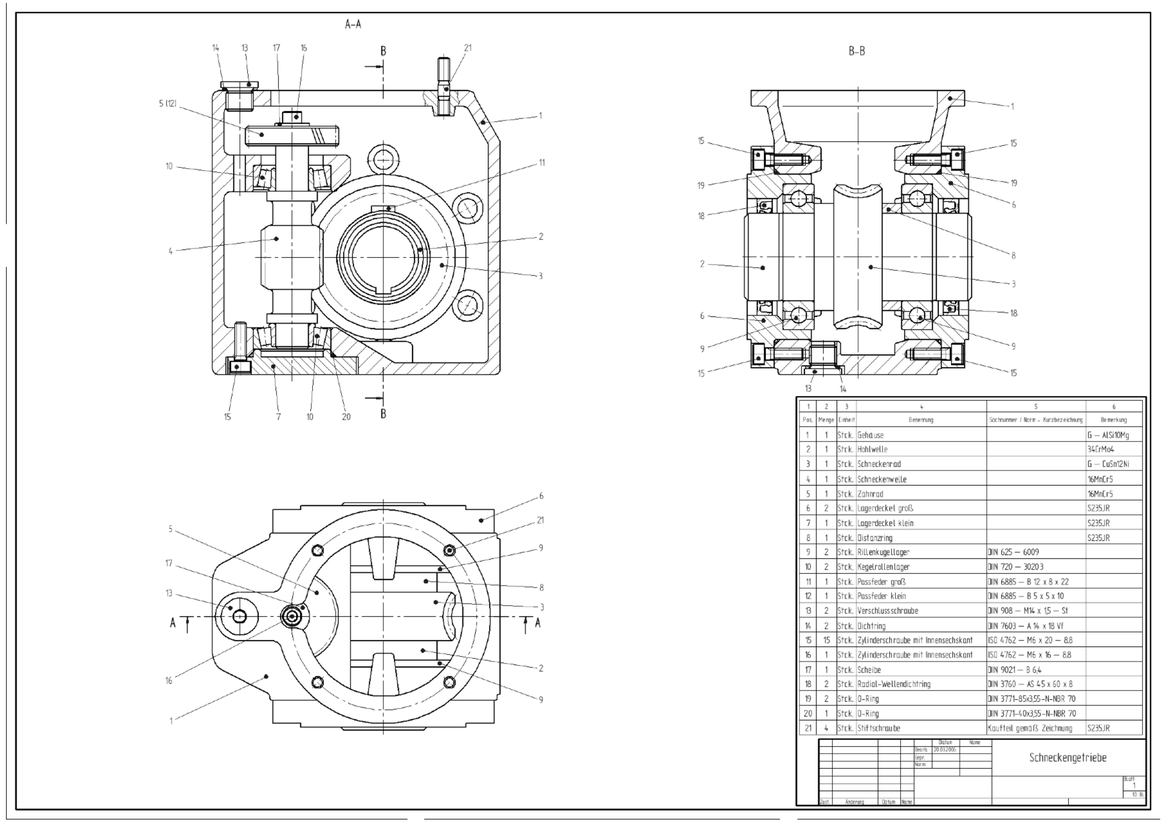
Cyber Resilience Act

„Der Cyber Resilience Act (CRA) zielt darauf ab, Verbraucher und Unternehmen zu schützen, die Produkte oder Software mit einer digitalen Komponente kaufen oder verwenden.“

- Meldung über Schwachstellen
- Lieferung von Security Updates
- Sonderbehandlung von OpenSource Komponenten
- SBOMs sind verpflichtend

Was ist eine SBOM?

Formate und Inhalte



Pos.	Menge	Einheit	Benennung	Sachnummer / Norm – Kurzbezeichnung	Bemerkung
1	1	Stck.	Gehäuse		G — AlSi10Mg
2	1	Stck.	Hohlwelle		34CrMo4
3	1	Stck.	Schneckenrad		G — CuSn12Ni
4	1	Stck.	Schneckenwelle		16MnCr5
5	1	Stck.	Zahnrad		16MnCr5
6	2	Stck.	Lagerdeckel groß		S235JR
7	1	Stck.	Lagerdeckel klein		S235JR
8	1	Stck.	Distanzring		S235JR
9	2	Stck.	Rillenkugellager	DIN 625 — 6009	
10	2	Stck.	Kegelrollenlager	DIN 720 — 30203	
11	1	Stck.	Passfeder groß	DIN 6885 — B 12 x 8 x 22	
12	1	Stck.	Passfeder klein	DIN 6885 — B 5 x 5 x 10	
13	2	Stck.	Verschlussschraube	DIN 908 — M14 x 1,5 — St	
14	2	Stck.	Dichtring	DIN 7603 — A 14 x 18 VI	
15	15	Stck.	Zylinderschraube mit Innensechskant	ISO 4762 — M6 x 20 — 8.8	
16	1	Stck.	Zylinderschraube mit Innensechskant	ISO 4762 — M6 x 16 — 8.8	
17	1	Stck.	Scheibe	DIN 9021 — 6.64	
18	2	Stck.	Radial-Wellendichtring	DIN 3760 — AS 45 x 60 x 8	
19	2	Stck.	O-Ring	DIN 3771-B5x355-N-NBR 70	
20	1	Stck.	O-Ring	DIN 3771-40x335-N-NBR 70	
21	4	Stck.	Stiftschraube	Kauffeil gemäß Zeichnung	S235JR

Was ist eine SBOM?

- Stückliste aller Komponenten einer Software
- maschinenlesbar
- Angabe pro Komponente
  - Name
  - Version
  - Lizenz
- enthält direkte und transitive Abhängigkeiten

Was ist eine SBOM?

- weiteres Artefakt meiner Software
- „Beipackzettel“ bei Auslieferung
- SBOM pro Software Version / Build
- SBOM Central

Was ist eine SBOM?

Beispiel

```
<component type="library"
  bom-ref="pkg:maven/de.ithempel.sbom/sbom@1.0-SNAPSHOT?type=jar">
  <group>de.ithempel.sbom</group>
  <name>sbom</name>
  <version>1.0-SNAPSHOT</version>
  <licenses/>
  <purl>pkg:maven/de.ithempel.sbom/sbom@1.0-SNAPSHOT?type=jar</purl>
</component>
```

Was ist eine SBOM?

Beispiel

```
<component type="library" bom-ref="pkg:maven/org.apache.logging.log4j/log4j-api@2.23.1?type=jar">
  <publisher>The Apache Software Foundation</publisher>
  <group>org.apache.logging.log4j</group>
  <name>log4j-api</name>
  <version>2.23.1</version>
  <description>The Apache Log4j API</description>
  <scope>required</scope>
  <hashes>
    <hash alg="MD5">bee2e2dcbeeb983bdb6b71c9c3476b6a</hash>
    <hash alg="SHA-1">9c15c29c526d9c6783049c0a77722693c66706e1</hash>
    <hash alg="SHA-256">92ec1fd36ab3bc09de6198d2d7c0914685c0f7127ea931acc32fd2ecdd82ea89</hash>
  </hashes>
  <licenses>
    <license>
      <id>Apache-2.0</id>
      <url>https://www.apache.org/licenses/LICENSE-2.0</url>
    </license>
  </licenses>
  <purl>pkg:maven/org.apache.logging.log4j/log4j-api@2.23.1?type=jar</purl>
  <externalReferences><reference type="website"><url>https://logging.apache.org/log4j/2.x/log4j/log4j-api/</url></reference><reference
type="build-system"><url>https://github.com/apache/logging-log4j2/actions</url></reference><reference type="distribution"><url>https://
logging.apache.org/logging-parent/latest/#distribution</url></reference><reference type="distribution-intake"><url>https://
repository.apache.org/service/local/staging/deploy/maven2</url></reference><reference type="issue-tracker"><url>https://github.com/apache/
logging-log4j2/issues</url></reference><reference type="mailing-list"><url>https://lists.apache.org/list.html?log4j-
user@logging.apache.org</url></reference><reference type="vcs"><url>https://github.com/apache/logging-log4j2</url></reference></
externalReferences>
```

SBOM Formate

Cyclone DX

- OWASP
- XML oder JSON
- Option für CVEs
- https://cyclonedx.org/
- guter Java Support

Cyclone DX - OWASP Foundation

SBOM Formate

SPDX (Software Package Data Exchange)

- Linux Foundation
- JSON, YAML, XML, xls
- ISO / IEC 5962:2021
  - https://spdx.dev/
- SPDX Export von GitHub

SPDX - Linux Foundation

Erstellen einer SBOM

Ansätze in Java Ökosystem

Kaffee Stift Notizbuch - Engin_Akyurt - Pixabay Content License

Stückliste von was?

- Design SBOM
- Source SBOM
- **Build SBOM** (pom.xml, build.gradle)
- **Analyzed SBOM** / 3rd party SBOM (JAR)
- **Deployed SBOM** (Docker Image)
- Runtime SBOM / Dynamic SBOM

Build SBOM

Maven / Gradle

- Ermittlung aller Abhängigkeiten des Projekts
- Nutzung vorhandener Informationen
- weiterer Build-Schritt
- weiteres Artefakt

Hausbau Neubau Einfamilienhaus - 2211438 - Pixabay Content License

CycloneDX Maven Plugin

OWASP Foundation

- Erstellt SBOM pro pom.xml
- Option zur Aggregation mehrere SBOMs eines multi-module Builds
- CycloneDX Format der OWASP
- Artefakt Upload in Repository

CycloneDX Maven Plugin

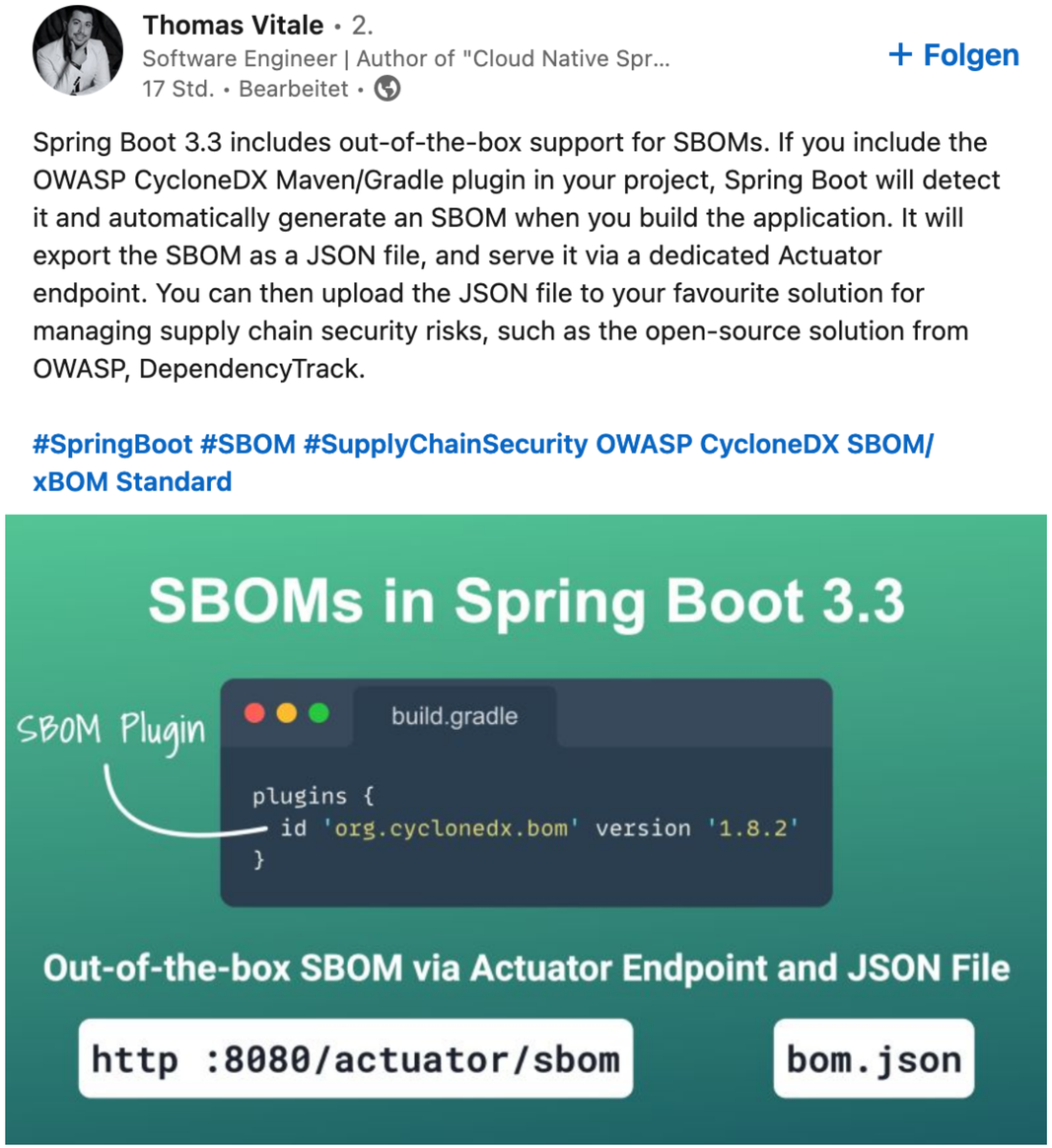
Konfiguration

```
<plugins>
  <plugin>
    <groupId>org.cyclonedx</groupId>
    <artifactId>cyclonedx-maven-plugin</artifactId>
    <version>${cyclonedx.version}</version>
    <executions>
      <execution>
        <phase>package</phase>
        <goals>
          <goal>makeAggregateBom</goal>
        </goals>
      </execution>
    </executions>
  </plugin>
```

CycloneDX Maven Pluing

Spring Boot

- Spring Boot >= 3.3
- erkennt CycloneDX Plugin
- Quelle: Thomas Vitale via LinkedIn



Thomas Vitale • 2.
Software Engineer | Author of "Cloud Native Spr...
17 Std. • Bearbeitet •

+ Folgen

Spring Boot 3.3 includes out-of-the-box support for SBOMs. If you include the OWASP CycloneDX Maven/Gradle plugin in your project, Spring Boot will detect it and automatically generate an SBOM when you build the application. It will export the SBOM as a JSON file, and serve it via a dedicated Actuator endpoint. You can then upload the JSON file to your favourite solution for managing supply chain security risks, such as the open-source solution from OWASP, DependencyTrack.

#SpringBoot #SBOM #SupplyChainSecurity OWASP CycloneDX SBOM/ xBOM Standard

SPDX Maven Plugin

Linux Foundation

- Erstellt SBOM pro pom.xml
- Lifecycle Phase verify
- SPDX Format der Linux Foundation

SPDX Maven Plugin

Konfiguration

```
<plugin>
  <groupId>org.spdx</groupId>
  <artifactId>spdx-maven-plugin</artifactId>
  <version>${spdx.version}</version>
  <executions>
    <execution>
      <phase>verify</phase>
      <goals>
        <goal>createSPDX</goal>
      </goals>
    </execution>
  </executions>
  <configuration>
    <excludeFilePatterns>
      <excludeFilePattern>*.spdx</excludeFilePattern>
    </excludeFilePatterns>
  </configuration>
</plugin>
```

Analyzed SBOM

JAR

- Ermittlung auf dem Artefakt
- Scanner benötigt Wissen über Format
- Beispiel: Syft

Labor Forschung Prüfung - PublicDomainPictures - Pixabay Content License

Syft

Artefakt Scanner

- Scanner basierend auf Artefakt
- Umfangreicher Support
- JAR

syft

Syft

Scannen eines JAR

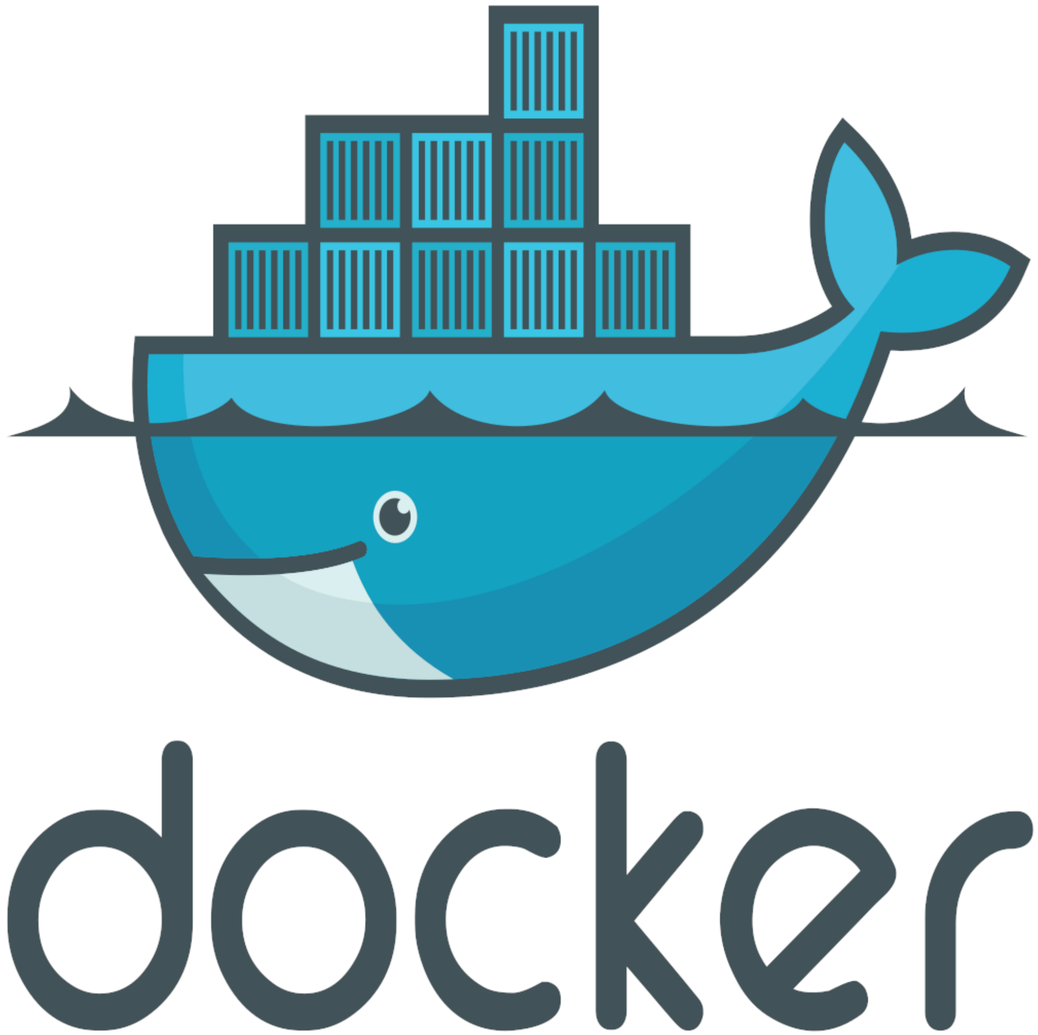
```
syft artifact.jar -o cyclonedx-xml --file bom.syft.cdx.xml
```

- Scannt das Artefakt artifact.jar
- Erstellt ein SBOM im CycloneDX Format (XML)
- erkennt „eingebettete“ JARs

Deployed SBOM

Docker Image

- Ermittlung basierend auf dem Docker Image
- Scanner liest Layer
- Beispiel: Syft



Docker

Syft

Scannen eines Docker Images

```
syft scan appimage -o cyclonedx-xml --file docker.image.xml
```

- Scann das Image appimage
- Erstellt SBOM im CycloneDX Format (XML)
- erkennt Layer und deren Properties

CVE Scan

Software Composition Analysis (SCA)

Sicherheit Schutz Antivirus - pixelcreatures - Pixabay Content License

CVE Scan

Prüfung

- Prüfung auf CVEs in der SBOM
- Abgleich mit Datenbanken
  - National Vulnerability Database (NVD) des NIST
  - OpenSource Vulnerability Database (OSV) von Google
  - Datenbanken von SCA Herstellern

CVE Scan

Klassifizierung

- Ist der CVE relevant für meine Software?
  - Wird betroffene Funktionalität genutzt?
  - Gibt es Gegenmaßnahmen?
- Vulnerability Exploitability Exchange (VEX)
  - vom Hersteller als eigenes Dokument
  - Referenz auf SBOM
  - eingebettet bei SBOM-Erstellung

CVE Scan

- SBOM ist nach Erstellung statisch
- CVE Scan sollte regelmäßig durchgeführt werden

trivy

OpenSource Vulnerability Scanner

trivy

Funktionsumfang

- Command-Line Tool
- Quellen: Dateisystem, Docker Images, Code Repositories und SBOMs
- unterstützt VEX
- erkennt vulnerabilities, misconfiguration, secrets und Lizenzen

trivy

Beispiel

```
trivy sbom target/bom.json
```

Prüfung der SBOM auf vulnerabilities

```
trivy sbom –scanners=vuln,license
```

zusätzlich Prüfung der genutzten Lizenzen

Lizenzprüfung

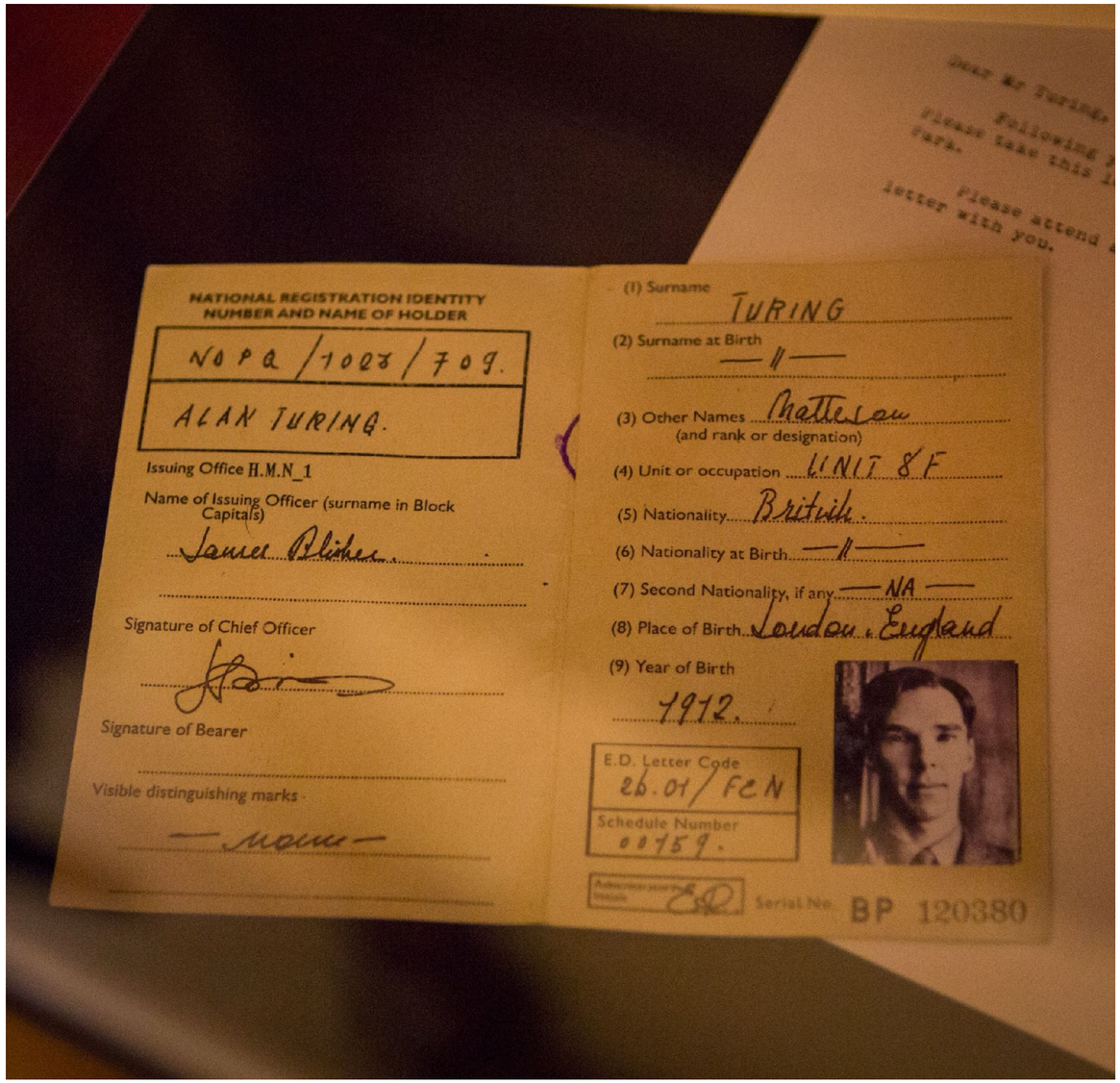
Kompatibilität der FLOSS Lizenzen

Lizenzprüfung

- Auflistung der Lizenzen der Komponenten
- Passen die Komponenten zusammen?
- Nutzung von verbotenen Lizenzen (im Enterprise Umfeld)

Identifizierung

Wie erkenne ich eine Komponente?



Identifizierung

- Standard zur eindeutigen Identifizierung einer Komponente
- Vereinheitlichung der Komponenten in SBOMs
- Wichtig zur Zuordnung von CVEs

SWID Tagging

- Software Identification (SWID) Tagging
- ISO 19770-2:2015
- Ursprünglich für Software Asset Management
- keine Verbreitung
- https://csrc.nist.gov/Projects/Software-Identification-SWID

CPE

- Common Platform Enumeration
- zentraler Ansatz / zentrales Verzeichnis
- NIST
- https://csrc.nist.gov/projects/security-content-automation-protocol/specifications/cpe

PURL

- Package URL
- Orientierung an Paketmodellen (Maven, NPM, …)
- dezentraler Ansatz
- OpenSource
- Github: package-url / purl-spec (https://github.com/package-url/purl-spec)

PURL

Beispiel

```
scheme:type/namespace/name@version?qualifiers#subpath
```

```
pkg:maven/org.apache.logging.log4j/log4j-api@2.23.1?
type=jar

pkg:gem/jruby-launcher@1.1.2?platform=java

pkg:npm/%40angular/animation@12.3.1
```

SBOM

Relevanz für (Java-)Entwickler

SBOM für (Java-)Entwickler

rechtliche Anforderungen

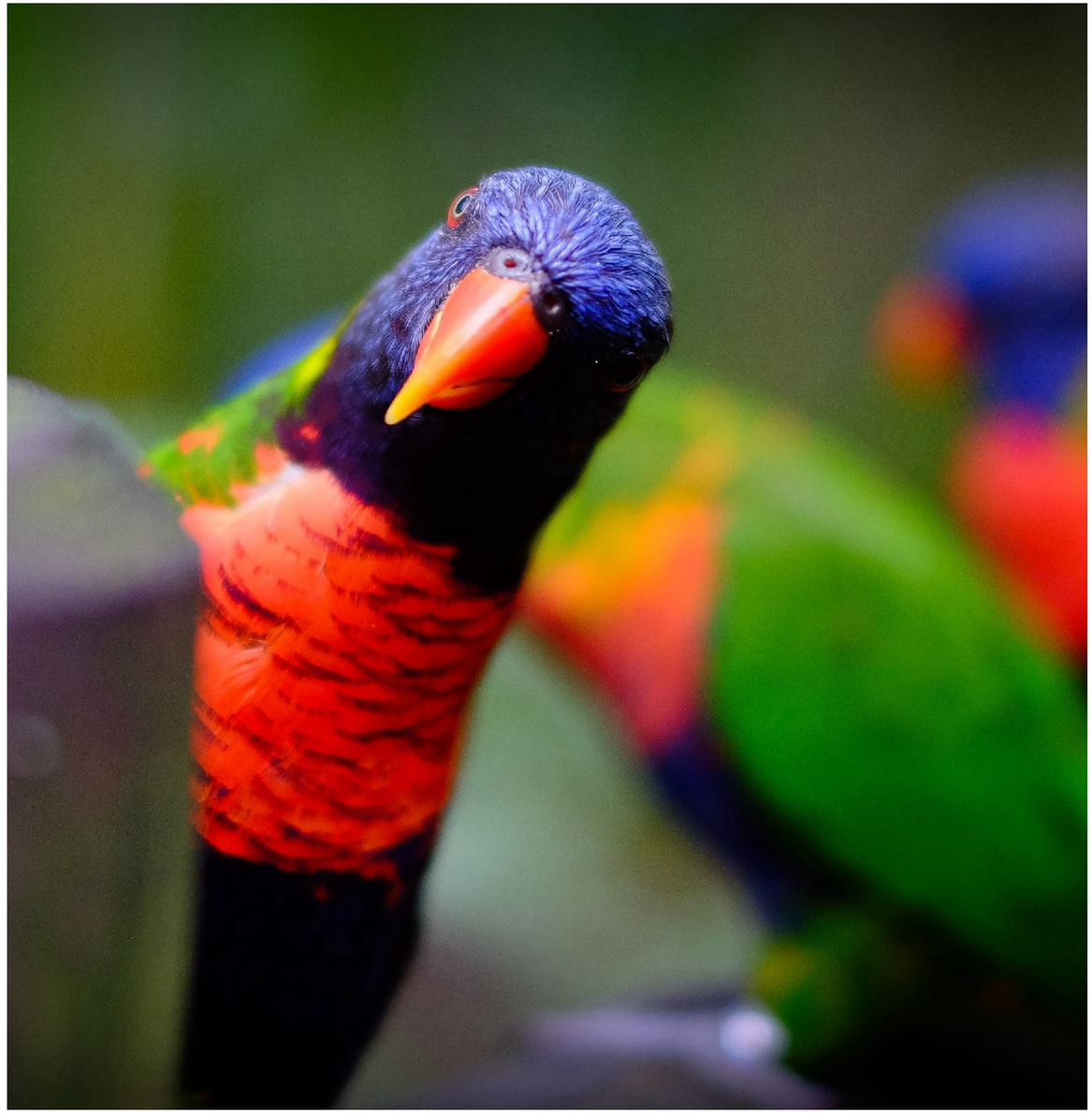
- spätestens CRA erfordert SBOMs
- getrieben von Governance in Unternehmen
- Nutzung zur Handhabung von CVEs

SBOM für (Java-)Entwickler

Unterstützung bei CVE Management

- Teil des Konfigurationsmanagements
  - Übersicht aller Komponenten
  - Schnelle Ermittlung von CVEs
  - Einschätzung der Gefahr

Fragen?



any questions? - (Matthias Ripp) - CC BY