dataport

Stefan **Schumacher:**

Open-Source-Software und BSI-Grundschutz



Mi., 1. Okt. 2025, 14:30–14:45 Uhr
Speakers Corner am Dataport Stand

SMART COUNTRY CONVENTION

Grundlage

- BSI Grundschutz (APP6A3) verlangt sichere Quellen für Software
- in der Regel ein Wartungsvertrag o.ä.
- für Open-Source-Software selten verfügbar
- Prozess für die Bewertung von Open-Source-Software und Quellen entwickelt

Prozess

1. Software kommt mit Wartungsvertrag
2. Software kommt ohne Wartungsvertrag
   - 2.1 Quellenrichtlinie anwenden
   - 2.2 Checkliste durchiterieren
   - 2.3 ggf. Mitigationsmaßnahmen durchführen.
3. interne Entwicklungsübernahme prüfen/durchführen

Checkliste

Ist die Lizenz FLOSS? (Lex Redis)

- White-/Blacklisting von Lizenzen
- GPL, LGPL, MIT, ISC,
- BSD: 0/1/2/3/4 Clause, Patente ...
- `https://opencode.de/de/wissen/rahmenbedingungen/standardisierte-open-source-lizenzen`
- `https://www.bitkom.org/sites/main/files/2022-06/220624-Bitkom-Leitfaden-Open%20Source-3.0_0.pdf`
- Problemfeld: Protokolle und deren Lizenzierbarkeit

Checkliste

- Ist die Software wichtig, komplex und/oder einfach ersetzbar? (Migrierbarkeit) (Lex Imaginary)
- Gibt es Aktivität? (Bus-Faktor)
- Wie wird mit Sicherheitsproblemen umgegangen? (Projekthistorie)
- Unterstützung durch etablierte NPO (Lex ValKey)
- Integrierbarkeit in interne Prozesse (z.B. Versionsverwaltungssystem)



- stefan.schumacher2@dataport.de
- https://gitlab.opencode.de/StefanSchumacher/phoenixflossquellenrichtlinie
  - Richtlinie Checkliste
  - Vortragsfolien und Videos aus Chemnitz/Kiel