

Chemnitzer Linux-Tage 2025: Open-Source-Software BSI-Grundsutzfähig machen

Stefan Schumacher

Stefan.Schumacher2@dataport.de

\$Id: 190_Schumacher_OpenSource-Grundsutzfaehig.adoc,v 1.2 2025/03/20 08:27:15 stefan Exp \$

<https://chemnitzer.linux-tage.de/2025/de/programm/beitrag/190>

Abstract

Open Source Software ist fundamental, um die digitale Souveränität unserer Demokratie zu sichern. Aber auch aus Sicherheitssicht ist FLOSS kommerzieller Closed-Source meist weit überlegen. Doch die Sicherheitsfreigabe von Software erfolgt im Öffentlichen Dienst in der Regel über eine BSI-Grundsutz-Zertifizierung. Und diese ist für FLOSS mit einigen Herausforderungen verbunden, denn (noch) bevorzugen die Anforderungen des Grundsutzkompendiums kommerzielle Lösungen.

Da wir in unserem Projekt den öffentlichen Dienst mit FLOSS digitalisieren wollen, müssen wir auch diese BSI-Anforderungen (vor allem APP.3, APP.6 und OPS) erfüllen. Dazu haben wir einige eigene Methoden entwickelt, die ich in diesem Vortrag vorstellen möchte. Dazu gehört u.a. eine Richtlinie zur Bewertung von FLOSS-Quellen und -Projekten, um diese BSI-konform betreiben zu können. Auch einige Erfahrungen zur Containerisierung im Kubernetes-Betrieb werde ich vorstellen.

In diesem Vortrag stelle ich die von uns entwickelte Checkliste zum BSI-konformen Bezug von Open-Source-Software vor. Desweiteren zeige ich, was Open-Source-Projekte tun können um ihre BSI-Grundsutzfähigkeit (und damit auch teilweise die Sicherheit) zu erhöhen.

Struktur des Vortrages

1. Problemlage
2. Das BSI-Gesetz und rechtliche Grundlagen
3. Was ist Grundsutz?
4. Grundsutz in der Praxis — ein Beispiel
5. APP6 - Sichere Quellen und Open-Source-Software
 - a. im DevSecOps-Prozess
 - b. unser Prozess um FLOSS grundsutzfähig zu machen

- c. Die Checkliste dazu
 - i. Lizenzen
 - ii. Migrierbarkeit
 - iii. Aktivität
 - iv. Umgang mit Schwachstellen
 - v. Versionierung
- 6. Die Open Source Security Foundation Scorecard
 - a. automatisiertes Testen (eigener) Projekte
- 7. Das BSI Testtool für TLS
- 8. einige Empfehlungen für FLOSS-Projekte

Empfehlungen für Open-Source-Projekte

- Meldewege für Sicherheitslücken einrichten
 - Verschlüsselung anbieten (GnuPG-Key!)
- Prozess zur Behebung von Sicherheitslücken dokumentieren
- signierte Security Advisories anbieten
 - Webseite (Github Pages?)
- Release Notes
 - insbesondere wenn Sicherheitslücken geschlossen werden
 - CVE referenzieren, wenn vorhanden
- OpenSSF Scorecard automatisiert einbinden (Github-Action)
 - <https://scorecard.dev/>

Check scores:

SCORE	NAME	REASON	DOCUMENTATION/REMEDIATION
10 / 10	Binary-Artifacts	no binaries found in the repo	https://github.com/ossf/scorecard/blob/06a2dfee8f502b6e9dc056ca5ca247d3214d2c58/docs/checks.md#binary-artifacts
?	Branch-Protection	internal error: error during branchesHandler.setup: internal error: githubv4.Query: Resource not accessible by personal access token	https://github.com/ossf/scorecard/blob/06a2dfee8f502b6e9dc056ca5ca247d3214d2c58/docs/checks.md#branch-protection
10 / 10	CI-Tests	1 out of 1 merged PRs checked by a CI test -- score normalized to 10	https://github.com/ossf/scorecard/blob/06a2dfee8f502b6e9dc056ca5ca247d3214d2c58/docs/checks.md#ci-tests
2 / 10	CII-Best-Practices	badge detected: InProgress	https://github.com/ossf/scorecard/blob/06a2dfee8f502b6e9dc056ca5ca247d3214d2c58/docs/checks.md#cii-best-practices
0 / 10	Code-Review	Found 1/28 approved changesets -- score normalized to 0	https://github.com/ossf/scorecard/blob/06a2dfee8f502b6e9dc056ca5ca247d3214d2c58/docs/checks.md#code-review
10 / 10	Contributors	project has 45 contributing companies or organizations	https://github.com/ossf/scorecard/blob/06a2dfee8f502b6e9dc056ca5ca247d3214d2c58/docs/checks.md#contributors
?	Dangerous-Workflow	no workflows found	https://github.com/ossf/scorecard/blob/06a2dfee8f502b6e9dc056ca5ca247d3214d2c58/docs/checks.md#dangerous-workflow
10 / 10	Dependency-Update-Tool	update tool detected	https://github.com/ossf/scorecard/blob/06a2dfee8f502b6e9dc056ca5ca247d3214d2c58/docs/checks.md#dependency-update-tool
10 / 10	Fuzzing	project is fuzzed	https://github.com/ossf/scorecard/blob/06a2dfee8f502b6e9dc056ca5ca247d3214d2c58/docs/checks.md#fuzzing
10 / 10	License	license file detected	https://github.com/ossf/scorecard/blob/06a2dfee8f502b6e9dc056ca5ca247d3214d2c58/docs/checks.md#license
10 / 10	Maintained	30 commit(s) and 7 issue activity found in the last 90 days -- score normalized to 10	https://github.com/ossf/scorecard/blob/06a2dfee8f502b6e9dc056ca5ca247d3214d2c58/docs/checks.md#maintained
?	Packaging	packaging workflow not detected	https://github.com/ossf/scorecard/blob/06a2dfee8f502b6e9dc056ca5ca247d3214d2c58/docs/checks.md#packaging
0 / 10	Pinned-Dependencies	dependency not pinned by hash detected -- score normalized to 0	https://github.com/ossf/scorecard/blob/06a2dfee8f502b6e9dc056ca5ca247d3214d2c58/docs/checks.md#pinned-dependencies
0 / 10	SAST	SAST tool is not run on all commits -- score normalized to 0	https://github.com/ossf/scorecard/blob/06a2dfee8f502b6e9dc056ca5ca247d3214d2c58/docs/checks.md#sast
10 / 10	Security-Policy	security policy file detected	https://github.com/ossf/scorecard/blob/06a2dfee8f502b6e9dc056ca5ca247d3214d2c58/docs/checks.md#security-policy
8 / 10	Signed-Releases	5 out of the last 5 releases have a total of 5 signed artifacts.	https://github.com/ossf/scorecard/blob/06a2dfee8f502b6e9dc056ca5ca247d3214d2c58/docs/checks.md#signed-releases
?	Token-Permissions	No tokens found	https://github.com/ossf/scorecard/blob/06a2dfee8f502b6e9dc056ca5ca247d3214d2c58/docs/checks.md#token-permissions
10 / 10	Vulnerabilities	0 existing vulnerabilities detected	https://github.com/ossf/scorecard/blob/06a2dfee8f502b6e9dc056ca5ca247d3214d2c58/docs/checks.md#vulnerabilities
:wq			

- Kryptographische Verfahren: Empfehlungen und Schlüssellängen.* (2025). Technische Richtlinie. Version TR-02102-1 2025-01. Bonn: Bundesamt für Sicherheit in der Informationstechnik. Verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=5
- Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS).* (2025). Technische Richtlinie des BSI. Version TR-02102-2 2025-01. Bonn: Bundesamt für Sicherheit in der Informationstechnik. Verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=4
- Kryptographische Verfahren: X.509 Zertifikate und Zertifizierungspfadvalidierung.* (2025). Technische Richtlinie des BSI. Version TR-02102-3 2025-01. Bonn: Bundesamt für Sicherheit in der Informationstechnik. Verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-3.pdf?__blob=publicationFile&v=3
- Kryptographische Verfahren: Verwendung von Secure Shell (SSH).* (2025). Technische Richtlinie des BSI. Version TR-02102-4 2025-01. Bonn: Bundesamt für Sicherheit in der Informationstechnik. Verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-4.pdf?__blob=publicationFile&v=3
- Elliptic Curve Cryptography.* (2018, 1. Juni). Version 2.1.0. Bonn: Bundesamt für Sicherheit in der Informationstechnik. Verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03111/BSI-TR-03111_V-2-1_pdf.pdf?__blob=publicationFile&v=1
- TLS Test-Specification.* (2023, 15. Mai). Version 1.1.0. Bonn: Bundesamt für Sicherheit in der Informationstechnik. Verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03116/BSI-TR-03116-TS_v1.pdf?__blob=publicationFile&v=2
- Kompendium für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf (KomTK).* (2025, 1. Februar). Version 1.0.0. Bonn: Bundesamt für Sicherheit in der Informationstechnik. Verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Netzwerke/TK-Systeme/tk-systeme_node.html
- Migration zu Post-Quanten-Kryptografie: Handlungsempfehlungen des BSI.* (2020, 1. August). Bonn: Bundesamt für Sicherheit in der Informationstechnik. Verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf?__blob=publicationFile&v=1