Open-Source-Software BSI-Grundschutzfähig machen

Stefan Schumacher, https://www.kaishakunin.com/posts/vortraege/misc/25kieluxa/

$Id: 190_Schumacher_OpenSource-Grundschutzfaehig.adoc,v 1.4 2025/09/17 14:38:51 stefan Exp $

PGP: 7B2B 45B1 330E 579E 3C3E 9B34 089D 8068 8050 ECCF

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-Grundschutz-Zertifizierung. Und diese ist für FLOSS mit einigen Herausforderungen verbunden, denn (noch) bevorzugen die Anforderungen des Grundschutzkompendiums 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-Grundschutzfähigkeit (und damit auch teilweise die Sicherheit) zu erhöhen.

Struktur des Vortrages

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

OpenSSL OpenSSF Scorecard Validation – 20250316
Aggregate score: 7.2 / 10

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			

1 Stefan Schumacher

Feyrer, H., Schumacher, S. & Weinem, M. (2007). NetBSD – Das portabelste Betriebssystem der Welt. In B. Lutterbeck, M. Bärwolff & R. A. Gehring (Hrsg.), *Open Source Jahrbuch 2007* (S. 315–326). Berlin: Lehmanns Media. Verfügbar 17. März 2007 unter http://www.opensourcejahrbuch.de/download/jb2007/osjb2007-04-06-feyrerschumacherweinem.pdf

Schumacher, S. (2011). Sicherheit messen: Eine Operationalisierung als latentes soziales Konstrukt. In S. Adorf, J.-F. Schaffeld & D. Schössler (Hrsg.), *Die sicherheitspolitische Streitkultur in der Bundesrepublik Deutschland: Beiträge zum 1. akademischen Nachwuchsförderpreis Goldene Eule des Bundesverbandes Sicherheitspolitik an Hochschulen (BSH)* (S. 1–38). Magdeburg: Meine Verlag. Verfügbar unter https://portal.dnb.de/opac.htm?method=simpleSearch&cqlMode=true&query=idn%3D1016863993

Schumacher, S. (2012). Timeo Danaos et dona ferentes: Zur Funktionsweise von Schadsoftware. *Magdeburger Journal zur Sicherheitsforschung*, *4*, 189–221. Verfügbar 30. März 2025 unter https://codeberg.org/0xKaishakunin/Publikationen/src/branch/main/MagdeburgerJournalSicherheitsforschung//MJS-014.pdf

Schumacher, S. (2012). Vom Cyber-Kriege: Gibt es einen Krieg im Internet? *Magdeburger Journal zur Sicherheitsforschung*, *4*, 285–307. Verfügbar 30. März 2025 unter https://codeberg.org/0xKaishakunin/Publikationen/src/branch/main/MagdeburgerJournalSicherheitsforschung//MJS-018.pdf

Schumacher, S. (2013). Vom Cyber-Frieden. *Magdeburger Journal zur Sicherheitsforschung*, *5*, 354–368. Verfügbar 30. März 2025 unter https://codeberg.org/0xKaishakunin/Publikationen/src/branch/main/MagdeburgerJournalSicherheitsforschung//MJS-023.pdf

Schumacher, S. (2015). Psychology of Security: A Research Programme. *Magdeburger Journal zur Sicherheitsforschung*, *10*, 667–674. Verfügbar 30. März 2025 unter https://codeberg.org/0xKaishakunin/Publikationen/src/branch/main/MagdeburgerJournalSicherheitsforschung//MJS_041_SchumacherPsychology.pdf

Schumacher, S. (2016). IT-Sicherheit in der Wasserversorgung: Schutz kritischer Infrastrukturen. *Magdeburger Journal zur Sicherheitsforschung*, *11*, 667–685. Verfügbar 30. März 2025 unter https://codeberg.org/0xKaishakunin/Publikationen/src/branch/main/MagdeburgerJournalSicherheitsforschung//MJS_042_Schumacher_Trinkwassersicherheit.pdf

Schumacher, S. (2020). Informationssicherheit in Versorgungsunternehmen umsetzen: Einige praktische Erfahrungen. *Magdeburger Journal zur Sicherheitsforschung*, *20*, 995–1002. Verfügbar 30. März 2025 unter https://codeberg.org/0xKaishakunin/Publikationen/src/branch/main/MagdeburgerJournalSicherheitsforschung//MJS_070_Schumacher_Versorgungsunternehmen.pdf

Schumacher, S. (2015). Psychology of Security: A Research Programme. *Magdeburger Journal zur Sicherheitsforschung*, *10*, 667–674. Verfügbar 30. März 2025 unter https://codeberg.org/0xKaishakunin/Publikationen/src/branch/main/MagdeburgerJournalSicherheitsforschung//MJS_041_SchumacherPsychology.pdf

2 BSI

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

3 Post-Quanten-Kryptographie

Module-Lattice-Based Key-Encapsulation Mechanism Standard: FIPS 203. (2024). National Institute of Standards & Technology. Verfügbar 17. August 2025 unter https://doi.org/10.6028/NIST.FIPS.203

Module-Lattice-Based Digital Signature Standard: FIPS 204. (2024). National Institute of Standards & Technology. Verfügbar 17. August 2025 unter https://doi.org/10.6028/NIST.FIPS.204

Stateless Hash-Based Digital Signature Standard: FIPS 205. (2024). National Institute of Standards & Technology. Verfügbar 17. August 2025 unter https://doi.org/10.6028/NIST.FIPS.205

Recommendation for Stateful Hash-Based Signature Schemes: NIST Special Publication 800-208. (2020). National Institute of Standards & Technology. Verfügbar 19. August 2025 unter https://doi.org/10.6028/NIST.SP.800-208