OSB Open Source Business ALLIANCE

Bundesverband für digitale Souveränität e.V.

FOSSGIS e.V.

WIR SPIELEN MIT OFFENEN KARTEN

Workshop

Es ist doch nur Software

Ausschreibung mit OSS - aber sicher?!

16.10.2023

15 – 16:30 | online

Workshopthemen heute

- Vorstellung FOSSGIS e.V. und OSBA
- Einleitung ins Thema
- Rechtliche Sicherheit (Miriam Seyffarth)
- Technische Sicherheit BSI-Grundschutz, technische Lösungen (Torsten Friebe)
- Wo geht die Reise hin? Cyber Resiliance Act usw. (Florian Micklich)
- Facts & Fiction - Vorurteile in der Verwaltung und Möglichkeiten der Ausschreibung innerhalb bestehender Verwaltungsvorschriften und "Standards" (Torsten Wiebke)
- Fragen und Antworten (alle)

FOSSGIS e.V. und OSBA

FOSSGIS e.V.

- Adresse: Bundesallee 23, 10717 Berlin
- Telefon: +49 30-62932037
- Local Chapter OpenStreetMap-Foundation
- Local Chapter OSGeo-Foundation
- FOSSGIS-Konferenz
- Mitgliedschaft: https://fossgis.de/verein/mitgliedschaft/

Open Source Business Allience (OSBA)

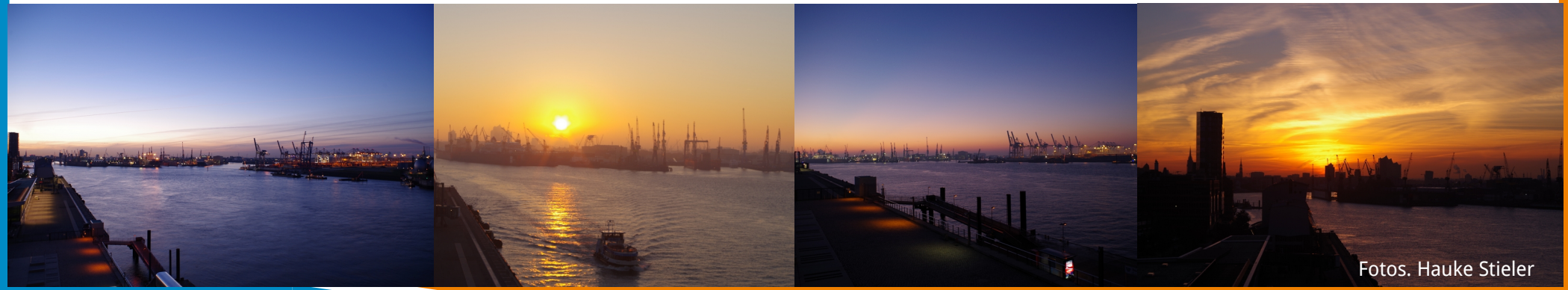
- Adresse: Pariser Platz 6a, 10117 Berlin
- Telefon: +49 (0) 30 / 300 149-3377
- Wirtschaftsverband für OSS-Unternehmen, > 200 Mitglieder
- vertritt OSS-Firmen und Institutionen
- https://osb-alliance.de/ueber-uns/was-ist-die-osb-alliance
- Working Group Beschaffung von OSS für den öffentlichen Sektor

FOSSGIS-Konferenz

- ist im D-A-CH-Raum die wichtigste Konferenz für Freie und Open Source Software im Geobereich sowie für die Themen Open Data und OpenStreetMap.
- Vorträge, Demosessions, Workshops, Anwendertreffen, Communitysessions, OpenStreetMap-Event
- Jedes Jahr im März an einem anderen Ort

FOSSGIS-Konferenz 2024

- 20.-23. März 2024 in Hamburg an der TUHH
- Einreichung Beitrag bis 06.11.2023
- Anmeldung ab Januar 2024
- Konferenzhomepage: https://fossgis-konferenz.de



Es ist doch nur Software - Ausschreibung mit OSS - aber sicher?!

Rechtliche Sicherheit:

Gutachten zur vorrangigen Beschaffung und Entwicklung von Open Source Software in der Bundesverwaltung

Miriam Seyffarth, Leitung Politische Kommunikation der OSB Alliance

16. Oktober 2023

Die Open Source Business Alliance

OSB Open Source Business ALLIANCE
Bundesverband für digitale Souveränität e.V.

Ausgangsfrage

- Kann rechtssicher gesetzlich geregelt werden, dass Open Source Software in Vergabeverfahren vorrangig vor proprietärer Software beschafft wird?
- Das Gutachten zielt dabei auf Gesetzgebungsmöglichkeiten auf Bundesebene ab, nicht auf einzelne Vergabeverfahren
- ABER: Die Argumentation aus dem Gutachten lässt sich zum Teil auf einzelne Vergabeverfahren und eine grundsätzliche Diskussion über den Vorrang für Open Source übertragen

Ausgangssituation

- Open Source Software wird bereits von der öff. Verwaltung in Bund, Ländern und Kommunen regelmäßig beschafft
- Dabei gibt es allerdings noch Hürden (z.B. EVB-IT, Unwissenheit/Vorurteile über Open Source etc.)
- Die Bundesregierung will, dass Open Source Software in der öff. Verwaltung verstärkt zum Einsatz kommt

Koalitionsvertrag zu Open Source Software

„Darüber hinaus sichern wir die digitale Souveränität, u. a. durch das Recht auf Interoperabilität und Portabilität sowie das Setzen auf offene Standards, Open Source und europäische Ökosysteme“

„Für öffentliche IT-Projekte schreiben wir offene Standards fest. Entwicklungsaufträge werden in der Regel als Open Source beauftragt, die entsprechende Software wird grundsätzlich öffentlich gemacht.“

Digitalstrategie zu Open Source Software

„Die technologische und digitale Souveränität Deutschlands ist Leitmotiv der Digital- und Innovationspolitik der Bundesregierung und zahlt auf das übergeordnete Ziel der strategischen Souveränität Europas ein. Technologische und digitale Souveränität sind notwendig, um Handlungsfähigkeit zu stärken und Abhängigkeiten zu reduzieren. Dies wiederum sind Bedingungen für Wettbewerbs- und Innovationsfähigkeit sowie Resilienz. Insoweit zielen wir zur Erreichung technologischer und digitaler Souveränität auf […] die konsequente Förderung von Open Source-Ansätzen […] ab“

Digitalstrategie Deutschland

Regelungen in den Bundesländern

- Schleswig-Holstein: Vorrang für Open Source im E-Government-Gesetz (seit 2022)
- Thüringen: Vorrang für Open Source im E-Government-Gesetz (seit 2018) und im Vergabegesetz (seit 2020)
- Bayern: Vorrang für Open Source im Bayerischen Digitalgesetz (seit 2022)
- Baden-Württemberg: Vorrang für Open Source in der Verwaltungsvorschrift (seit 2021)

Regelungen in anderen EU-Staaten

Frankreich, Portugal, Spanien und die Tschechische Republik haben Regelungen zum Vorrang von Open Source Software bei der Beschaffung laut einer Studie des Wissenschaftlichen Dienstes des Bundestages

Dreh- und Angelpunkt: § 97 GWB

Gesetz gegen Wettbewerbsbeschränkungen (GWB)

§ 97 Grundsätze der Vergabe

Diskriminierungsverbot:

(2) Die Teilnehmer an einem Vergabeverfahren sind gleich zu behandeln, es sei denn, eine Ungleichbehandlung ist aufgrund dieses Gesetzes ausdrücklich geboten oder gestattet.

Strategische Beschaffung:

(3) Bei der Vergabe werden Aspekte der Qualität und der Innovation sowie soziale und umweltbezogene Aspekte nach Maßgabe dieses Teils berücksichtigt.

Ist eine Priorisierung von Open Source möglich?

„Wegen des Systemcharakters von Software mit dem besonderen Aspekt der offenen Standards, der Kompatibilität und den Gesichtspunkten von Kooperation und Nachhaltigkeit **erscheint eine generelle Bevorzugung [von Open Source Software] nicht nur sinnvoll, sondern erforderlich**, um insbesondere Lock-In-Effekten bei Einsatz proprietärer Software entgegenzuwirken und eine langfristige Umstellung der Verwaltung zu bewirken, die für die Erreichung des Ziels der Herstellung digitaler Souveränität der Verwaltung am effektivsten erscheint.“

Gesetzliche Regelungsoptionen

- Verankerung in §97 Gesetz gegen Wettbewerbsbeschränkungen (GWB)
- Verankerung im 2. Abschnitt des Kartellvergaberechts
- **Verankerung in der Vergabeverordnung für öffentliche Aufträge (VgV)**
- Verankerung als Haushaltsgrundsatz
- Erlass allgemeiner Verwaltungsvorschriften
- **Verankerung im E-Government-Gesetz des Bundes**

Formulierungsvorschlag aus dem Gutachten

- Zur Gewährleistung einer weitreichenden Interoperabilität sind neue Anwendungen und Technologien mit offenen Schnittstellen sowie Standards auszustatten und hierüber nutzbar zu machen. Neue Anwendungen und Technologien sollen möglichst abwärtskompatibel sein.
- Der Einsatz von Open-Source-Software soll vorrangig vor solcher Software erfolgen, deren Quellcode nicht öffentlich zugänglich ist und deren Lizenz die Verwendung, Weitergabe und Veränderung einschränkt sowie Anwendungen und Technologien eingesetzt werden, die über ihren gesamten Lebenszyklus nachhaltig sind.
- Bei neuer Software, die von der öffentlichen Verwaltung oder speziell für diese entwickelt wird, ist der Quellcode unter eine geeignete Freie-Software- und Open-Source-Lizenz zu stellen und zu veröffentlichen, soweit keine sicherheitsrelevanten Aufgaben damit erfüllt werden und dies lizenzrechtlich zulässig ist.

Formulierung im Kabinettsentwurf zum OZG 2.0

„Bei der Bereitstellung der IT-Komponenten im Sinne des Absatzes 1, soll dort, wo es technisch möglich und wirtschaftlich ist, Open-Source-Software vorrangig vor solcher Software eingesetzt werden, deren Quellcode nicht öffentlich zugänglich ist oder deren Lizenz die Verwendung, Weitergabe und Veränderung einschränkt.“

Neuer Gesetzentwurf zum OZG 2.0: Der Teufel steckt jetzt im Detail

FEATURED, PRESSEMITTEILUNGEN, STELLUNGNAHMEN, VERBANDS-NEWS

Am 24. Mai hat die Bundesregierung einen Gesetzentwurf für das neue Onlinezugangsgesetz beschlossen, der im nächsten Schritt von Bundestag und Bundesrat abgestimmt werden muss, bevor er in Kraft tritt. In dem aktuellen Gesetzentwurf finden sich gute und wichtige Punkte zu Open Source Software und der Veröffentlichung von Standards. Allerdings ist der Entwurf noch nicht präzise genug, um die angestrebten Ziele auch tatsächlich zu erreichen, und muss daher an einigen Stellen noch nachgebessert werden. In ihrer Stellungnahme hat die OSB Alliance die wichtigsten Schwachpunkte und möglichen Schlupflöcher aufgezeigt und Verbesserungsvorschläge formuliert.

12. Juni 2023

Koalitionsvertrag zur Vergaberechtsreform

„Wir wollen die öffentlichen Vergabeverfahren vereinfachen, professionalisieren, digitalisieren und beschleunigen. Die Bundesregierung wird die öffentliche Beschaffung und Vergabe wirtschaftlich, sozial, ökologisch und innovativ ausrichten und die Verbindlichkeit stärken, ohne dabei die Rechtssicherheit von Vergabeentscheidungen zu gefährden oder die Zugangshürden für den Mittelstand zu erhöhen.“

CIO Bund zu Beschaffung und Vergabe

Markus Richter, CIO Bund, am 2. Juni 2023:

„Das Beschaffungswesen ist für uns – und das sieht man auch im Koalitionsvertrag – nicht irgendein Instrument, sondern es ist das entscheidende Instrument, wenn es darum geht, den Public Sector nachhaltiger und digitaler aufzustellen, und um wichtige Vorgaben aus dem Koalitionsvertrag umzusetzen, also den politischen Willen, den die Gesellschaft von uns zu Recht erwartet.“

Danke für die Aufmerksamkeit!

Kontakt: seyffarth@osb-alliance.com

OSB Open Source Business ALLIANCE

Bundesverband für digitale Souveränität e.V.

FOSSGIS e.V.

WIR SPIELEN MIT OFFENEN KARTEN

Workshop

Technische Sicherheit

BSI-Grundschutz und technische Lösungen

Torsten Friebe

friebe@lat-lon.de | @torfri

Frage

Ist denn Open-Source-Software überhaupt sicher?

Open Source öffnet Hackern Tür und Tor?

- Ende 2021 schaffte es die Nachricht über eine Sicherheitslücke in dem Open-Source-Projekt Apache Log4j bis in die Tagesschau.

Nach Einschätzung des BSI führte die als ***log4shell*** genannte Sicherheitslücke zu einer kritischen Bedrohungslage (Warnstufe rot 🚦).

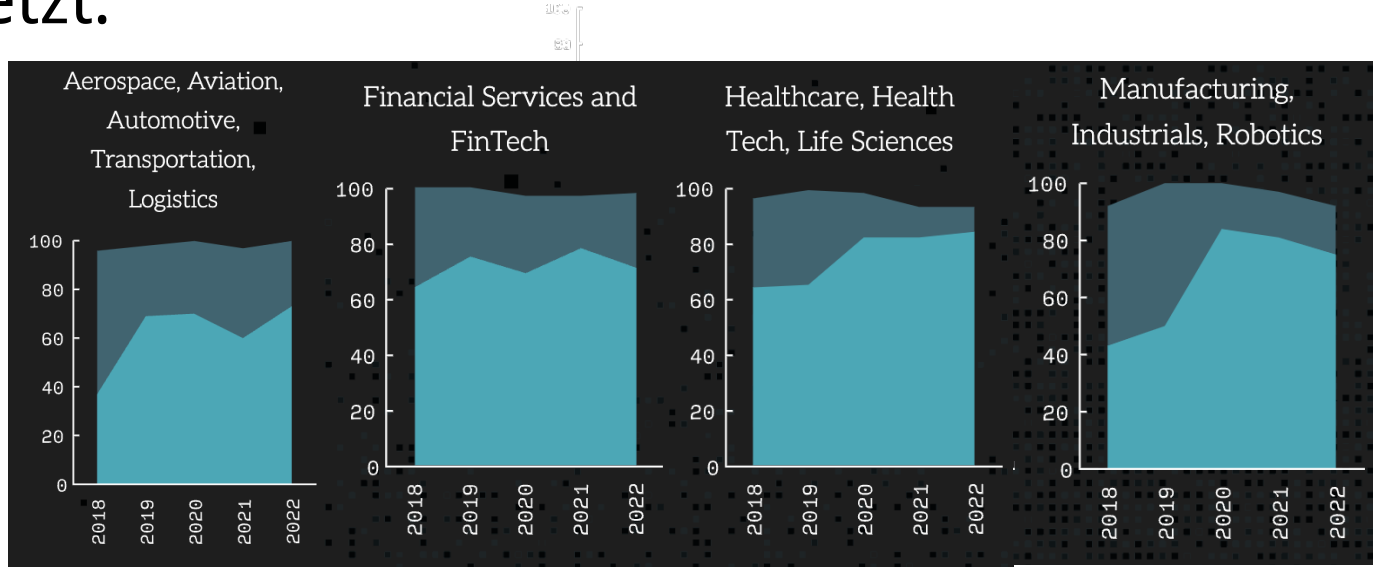
- Folge: Viele Hersteller mussten ihre Software aktualisieren, so u.a. auch die Firma Apple deren Cloud-Angebot icloud.com betroffen war.
- Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Jeder kann Fehler in den Code einbauen?

- Im März 2022 versteckte der Entwickler Brandon Miller in dem von ihm verwalteten OSS-Software-Modul Node-ipc Sabotagecode.
- Folge: auf Rechnern mit russischer und belarussischer IP-Adresse wurden Dateien gelöscht und durch Herz-Emojis ❤️ ersetzt.
- Der Name der Update-Version des rund 24 Stunden verfügbaren Software-Moduls lautete: peacenotwar 😇

Für kritische Bereiche ist Open Source nicht einsetzbar?

- Laut einer Umfrage von Synopsys wird Open-Source-Software auch in kritischen Infrastrukturen und Industrien eingesetzt:

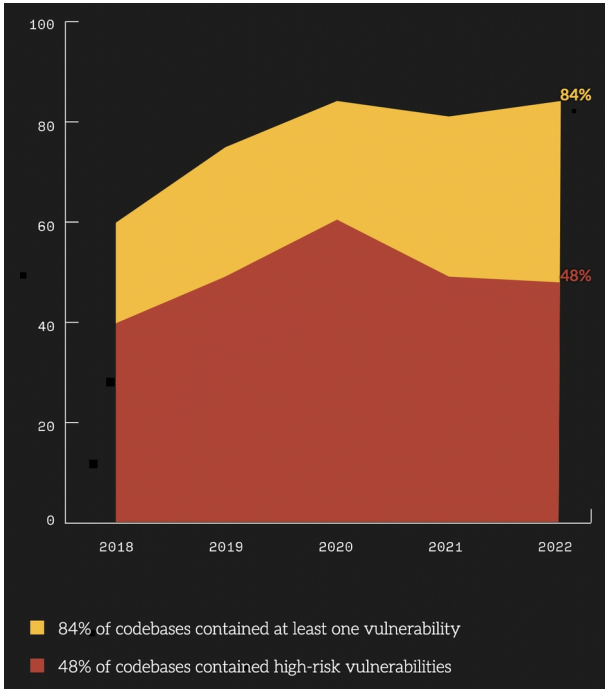


Quelle: Open Source Security & Risk Analysis (OSSRA) Report 2023 - Synopsys

Sicherheitslücken überall?

- Jedoch in **84%** der in der Studie untersuchten Software-Komponenten war **mindestens 1 Sicherheitslücke** enthalten.

- Häufigsten Ursachen dafür sind:
  - Verwendung von veralteten Softwareständen
  - Keine Aktualisierung innerhalb der letzten 4 Jahre
- Quelle: Open Source Security & Risk Analysis (OSSRA) Report 2023 - Synopsys



Ist denn OSS sicher?

- **JA!** Das Bundesamt für Sicherheit in der Informationstechnik (BSI) schätzt Open-Source-Software als mindestens genauso sicher ein wie proprietäre Software.
- Quelle:
  Bundesamt für Sicherheit in der IT (BSI)

Sicher ist sicher?

- Untersuchung der **National Vulnerability Database** (NVD) an der TU München zur Sicherheit von OSS stellte 2014 fest, dass es keinen Unterschied zwischen proprietärer (closed source) und freier (open source) Software bzgl. Sicherheitsmängeln nach dem **Common Vulnerability and Exposures (CVE)** Standard gibt.
- Weder bei der **Schwere** des **CVSS** noch der **Dauer** bis zur Bereitstellung eines Patches sind signifikante Unterschiede festzustellen.

Vertrauen

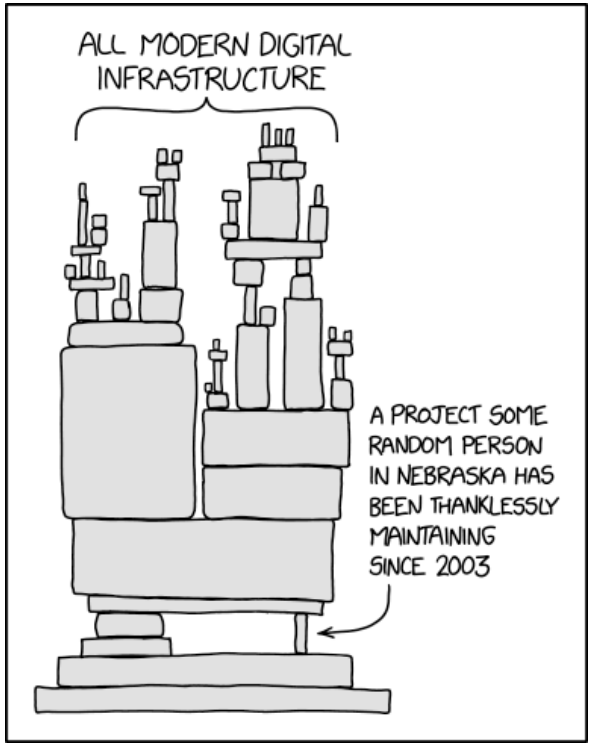
- Oft entscheiden sich aber auch große Unternehmen ganz bewusst, den Quellcode von Teilen ihrer Programme öffentlich zu machen und erhoffen sich, dass so viele Entwickler:innen daran mitarbeiten und Fehler aufdecken.
- Quelle: CISPA-Studie „Committed to Trust: A Qualitative Study on Security & Trust in Open Source Software Projects”, 2022

Groß & Klein

- Je größer der Umfang eines OSS-Projekts und die Zahl der Mitwirkenden ist, desto größer ist auch ihr Bedarf an Sicherheits- und Vertrauensprozessen.
- Kleinere Projekte scheinen Sicherheits- und Vertrauensvorfälle erst zu behandeln, wenn sie auftreten.
- Quelle: CISPA-Studie

Unterstützung für die Kleinen

- Kleineren OSS-Projekten mangelt es oft an personeller Besetzung und finanziellen Mitteln, um Richtlinien und Leitfäden zu erarbeiten oder komplizierte Prüfprozesse zu etablieren.
- Diese Open-Source-Projekte mit einer geringen Anzahl von Mitwirkenden und begrenztem Zugang zu Ressourcen benötigen Unterstützung.



Quelle: Randall Munroe.

Frage

Wo kann der BSI-Grundschutz helfen?

BSI-IT-Grundschutz

- Der IT-Grundschutz ist Methode, Anleitung, Empfehlung und Hilfe zur Selbsthilfe für Behörden, Unternehmen und Institutionen, die sich mit der Absicherung ihrer Daten, Systeme und Informationen befassen.
- Beinhaltet technische und organisatorische Maßnahmen zum Aufbau eines Informationssicherheitsmanagements (ISMS).

BSI-Standards

- BSI-Standard 200-1: Management für Informationssicherheit (ISMS)
- BSI-Standard 200-2: Die IT Grundschutz Vorgehensweise, BSI-Methodik
- BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz
- BSI-Standard 200-4: Anleitung für Aufbau eines Business Continuity Management System (BCMS)

IT-Grundschutz-Bausteine

- ISMS: Sicherheitsmanagement
- ORP: Organisation und Personal
- CON: Konzeption und Vorgehensweise
- OPS: Betrieb
- DER: Detektion und Reaktion
- APP: Anwendungen
- SYS: IT-Systeme
- IND: Industrielle IT
- NET: Netze und Kommunikation
- INF: Infrastruktur

Aufbau eines Bausteins

- Jeder Baustein beginnt mit einer Einleitung und Zielsetzung sowie einer Beschreibung der Gefährdungslage
- Anforderungen werden in den Kategorien Basis, Standard und erhöhter Schutzbedarf unterteilt
- Auswahl an Anforderungen am Beispiel von CON.8 Software-Entwicklung:
  - CON.8.A5 Sicheres Systemdesign (B)
  - CON.8.A12 Ausführliche Dokumentation (S)
  - CON.8.A18 Regelmäßige Sicherheitsaudits für die Entwicklungsumgebung (H)

BSI-TR SBOM

- BSI Technische Richtlinie (TR) zu Software Bill of Materials (SBOM)
- Eine SBOM listet die Bestandteile einer Software mit Version, Quelle, Lizenz u.a. Informationen auf.
- Quelle: BSI-TR SBOM

Zielgruppen

- Der IT-Grundschutz richtet sich an unterschiedliche Anwendergruppen, u.a. auch an
- Software-Entwickler (**Dev**elopment)
- IT-Administratoren (**Op**erations)

DevSecOps

- **DevOps** beschreibt eine Sammlung von Methoden und Techniken für die SW-Entwicklung (**Dev**elopment) und den IT-Betrieb (**Op**erations)
- **DevSecOps** erweitert dies um den Bereich Sicherheit und IT-Compliance

Fazit

Open-Source-Software -
aber sicher!

Studie der OSBA

- Inhalt: Vergleich der Sicherheit von Open Source und proprietärer Software
- **Vorteile von OSS**: niedrigere Kosten sowie höhere Transparenz und Sicherheit
- **Vorteile von proprietärer Software**: umfänglichen Support durch den Anbieter und rechtliche Klarheit durch bindende Verträge.

Software-Qualität

- *„Quelloffenheit und kollaborative Entwicklungsmodelle helfen Software sicherer zu machen.“*
  (Elmar Geese, Sprecher der Arbeitsgruppe Security in der OSB Alliance)

Anreize für IT-Sicherheit in OSS

- Um die Software-Sicherheit zu verbessern wäre deshalb ein möglicher Ansatz, stärkere ökonomische Anreize zu geben, um Sicherheitslücken zu patchen.
- z.B. durch Bug Bounty Programme
- Quelle: Analyse zur Sicherheit von Open-Source Software, TU München, 2014

Cyber Resilience Act (CRA)

- Durch politische Vorgaben wie z.B. dem CRA kommen auf Software-Hersteller neue Anforderungen zu und stellen grundlegende Anforderungen an die Sicherheit des gesamten Produktlebenszyklus einer Software.

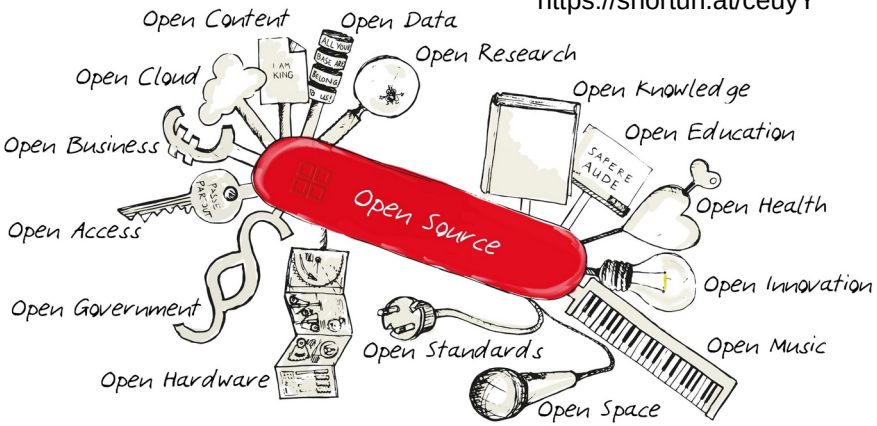
Wo geht die Reise hin?

Cyber Resilience Act (CRA)

Open-Source Bedeutung

- Ansatz in der Software-Entwicklung, bei dem der geschriebene Quellcode veröffentlicht wird und von allen einseh- und bearbeitbar ist
- 78-96 % aller Softwareprodukte enthalten heutzutage Open-Source-Komponenten.
- FOSS führt zur Stärkung der digitalen Souveränität (in der öffentlichen Verwaltung)
- FOSS Komponenten sind unabhängig, überprüfbar, gestaltbar und austauschbar
- Win-Win Situation beim **Open-Source-Ökosystem** durch Verflechtung von ehrenamtlichen und kommerziellen Akteuren und Organisationen

https://shorturl.at/ceuyY



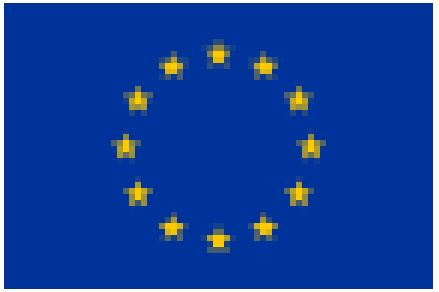
Fostering Open Source Software Security 2023

Study about the impact of open source software and hardware… 2021

Studie zur Sicherheit von Open Source und proprietärer Software 2021

Cyber Resilience Act (CRA)

- Ziel Verbraucher und Unternehmen beim Kauf oder der Nutzung von Hardware oder Software mit digitaler Komponente zu schützen
- Einführung verbindlicher Cybersicherheitsanforderungen für Hersteller und Händler über den gesamten Produktlebenszyklus
- Verbraucher und Unternehmen sind durch die auferlegte Transparenz in der Lage, festzustellen, welche Produkte cybersicher sind, oder sie so einzurichten, dass dies gewährleistet ist
- **CE-Kennzeichnung** durch (Selbst-) Zertifizierung von Software und Hardware, um anzuzeigen, dass sie den neuen Standards entsprechen



CRA Anforderungen

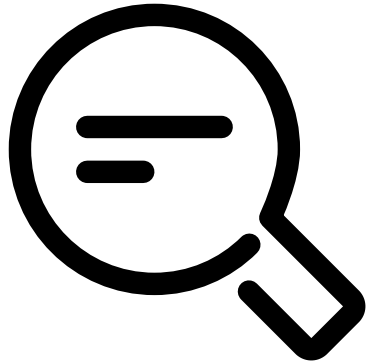
- Verlangt die Verwendung von SBOMs, Sicherheitspatches und Benutzer-"Call-Home"-Funktionalität
- Erfordert eine Unterstützung der Produkte für mindestens 5 Jahre
- Schränkt die Veröffentlichung von unfertiger Software zu Testzwecken ein
- Fordert Prozesse und Dokumention für jede einzelne Veröffentlichung

Umsetzung würde laut Prognosen von der EU eine Kostensteigerung von 25% bedeuten

Strafe bei Nichteinhaltung von bis zu 15 Mio. € bzw. 2,5 % des gesamten weltweiten Jahresumsatzes des Unternehmens

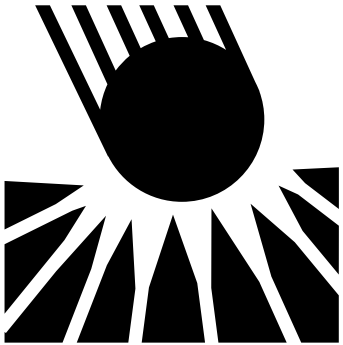
Wenn das ABER nicht wäre!

- Die Ziele des CRA sind ausdrücklich zu befürworten, Qualität und Sicherheitsstandards von IT-Produkten zu erhöhen, aber…
- Der CRA strebt eine Ausnahme für OSS an, sofern diese nicht für kommerzielle Aktivitäten eingesetzt wird, aber…
  - ➔ Das Problem liegt in der konkreten Definition von „kommerziell“ und „unklaren“ Textbausteinen
  - ➔ CRA Fassungen sind für proprietäre Produkte geschrieben und berücksichtigen die besonderen Entwicklungs- und Vertriebsmodelle von Open-Source derzeit nur unzureichend
  - ➔ Intention die finanzielle Belastung der EU-Wirtschaft zu verringern, indem OSS-Projekte und OSS-Stiftungen mit der Konformitätsprüfung beauftragt werden



Bedeutung

Aktuell ist die klare Intention von den politischen Entscheidern keine Ausnahmen für OSS-Stiftungen und den meisten OSS-Projekten zu gewähren!

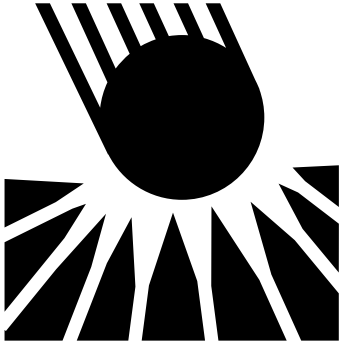


- Der aktuelle Wortlaut bedeutet vor allem eine **Rechtsunsicherheit**
- **Überregulierung** des OSS-Ökosystems

5 ausgewählte Fallbeispiele sollen die Problematiken aufzeigen

Fallbeispiel 1

Einige der Verpflichtungen sind für OSS praktisch unmöglich zu erfüllen da die Autoren oft keine Ahnung haben, wie der Code irgendwann verwendet werden könnte und Verpflichtungen in der Lizenz klar ausgeschlossen werden.

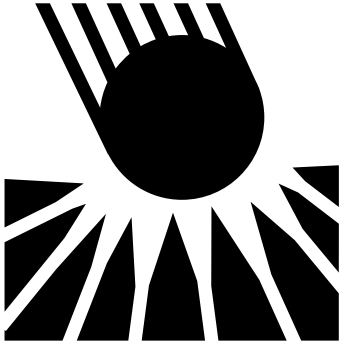


- Widerspricht fundamental der OSS-Philosphie
- OSS-Autoren wissen weder wer ihr Software irgendwann nutzen wird noch haben sie die Kontrolle darüber, wie ihr Code nachgelagert integriert wird
- Forderungen und mögliche Strafen liegt bei den Autoren und nicht bei denen, die diese kommerziell anderweitig einsetzen

Fallbeispiel 2

Jedes OSS-Projekt, an denen sich Personen beteiligen, die bei einem kommerziellen Unternehmen beschäftigt sind, wird als kommerzielle Tätigkeit betrachtet

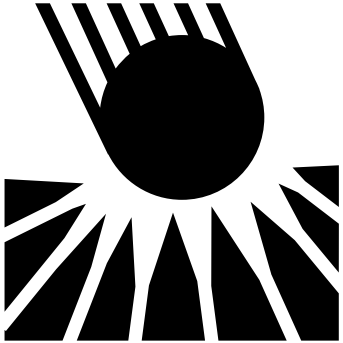
- Das trifft auf nahezu alle bedeutenden OSS-Projekte zu
- Unmöglich dies zu überprüfen und Ablehnung von Personen oder Beiträgen wäre die Konsequenz
- Unternehmen können ihren Angestellten verbieten, sich an OSS-Projekten zu beteiligen



Fallbeispiel 3

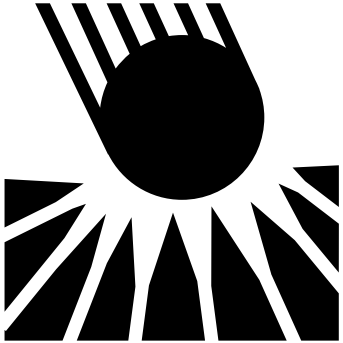
Jedes Projekt oder Stiftung, das wiederkehrende Spenden von kommerziellen Unternehmen annimmt, wird als kommerziell angesehen

- Gegen die gängige Praxis des Open-Source-Ökosystems
- Nachhaltigkeit von Open-Source ist ernsthaft gefährdet
- Spenden stellen keine Gewinnerzielung dar. Ein Wegfall würde die Sicherheit sogar verringern
- Stiftungen müssten Haftung für ehrenamtlich entwickelte Standards oder Software übernehmen obwohl sie dieses nicht mit einer Gewinnerzielungsabsicht verbunden ist



Fallbeispiel 4

Open-Source-Forschungsprojekt wären kommerziell, wenn diese z.B. mit EU-Mitteln gefördert oder ein kollaboratives Arbeiten mit Firmen bestünde

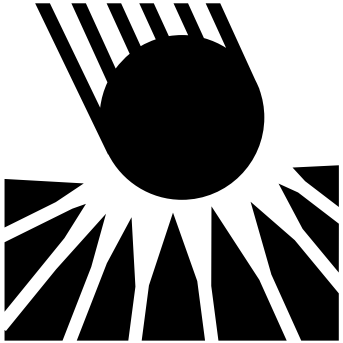


- Gängige Praxis und bestehende Kollaboration wären gefährdet
- Die Arbeit mit internationale akademische Akteuren und Partnern aus der Wirtschaft würden sich verringern oder nicht stattfinden
- Weitreichende Konsequenzen für Forschung und Innovation in Deutschland und der EU

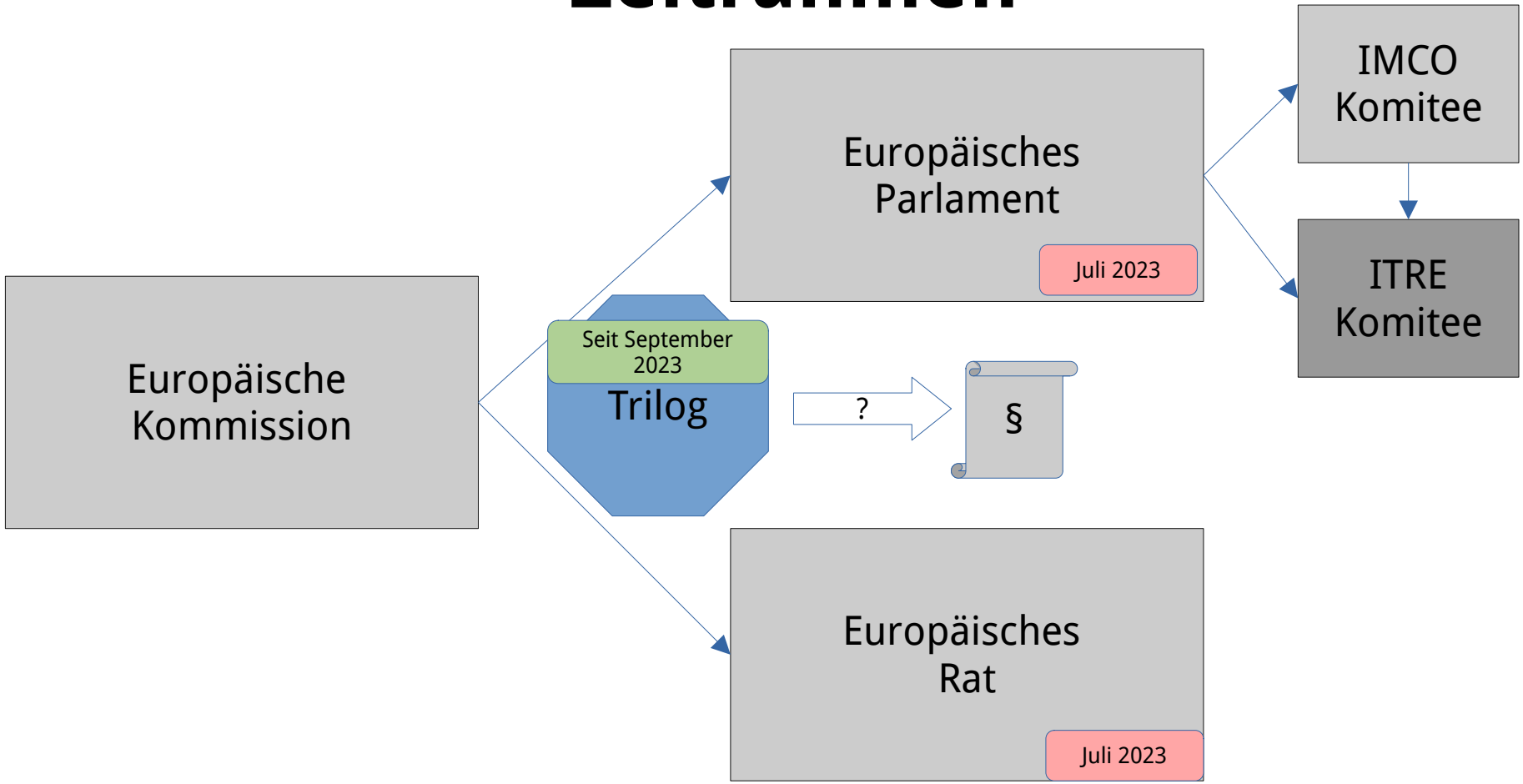
Fallbeispiel 5

Die CRA verlangt die Offenlegung schwerwiegender, nicht behobener und ausgenutzter Schwachstellen gegenüber der ENISA (einer EU-Institution) innerhalb einer Frist von Stunden, bevor diese behoben werden

- Fundamental gegen die gängige Praxis bei Schwachstellen
- Erzeugen eines zentralen Registers von ungepatchte Sicherheitslücken macht Software nicht sicherer
- Kern der fairen und gleichberechtigten Berichtskultur wird gebrochen, auf die Open Source angewiesen ist



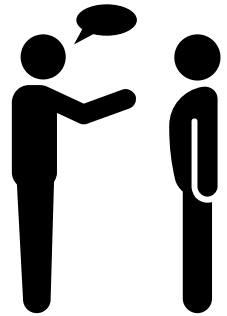
Zeitrahmen


Europäische Kommission
Seit September 2023
Trilog
?
§
Europäisches Parlament
Juli 2023
IMCO Komitee
ITRE Komitee
Europäisches Rat
Juli 2023

Was kann man tun

Die Bundesregierung muss sich bei den anstehenden Trilogverhandlungen dafür einsetzen, dass im CRA das Open-Source-Ökosystem und damit wichtige Teile der deutschen und europäischen IT-Wirtschaft sowie die digitale Souveränität Deutschlands ausreichend geschützt werden

nicht den Ersteller einer OSS in die Pflicht nehmen, sondern den "InVerkehr-Bringer" bzw. Nutzer, der damit einen Dienst anbietet, wenn hierfür Geld verlangt wird bzw. ein Geschäftsmodell darauf gründet.



Jede Person als auch Unternehmen mit politischem oder wirtschaftlichem Ansehen kann aktiv werden, in dem eine Nachricht an einen Parlamentarier des eigenen Landes geschrieben werden und auf die Problematik aufmerksam gemacht wird

Quellen und zum Nachlesen

OSBA: Stellungnahme zum Cyber Resilience Act

Eclipse Foundation: Open Letter to the European Commission on the Cyber Resilience Act

Linux Foundation: Cyber Resilience Act: it’s time to act to #FixTheCRA!

European Commission: CRA -Shaping Europe’s digital future

Apache Foundation: Save Open Source: The Impending Tragedy of the Cyber Resilience Act

Python Software Foundation: The EU's Proposed CRA Law May Have Unintended Consequences for the Python Ecosystem

No cyber resilience without open source sustainability

Open Letter on the Significance of Free and Open Source Software in the EU’s Proposed CRA

Facts and Fiction

Erfahrungen aus der Verwaltung

Erfahrungsaustausch - keine Rechtsberatung!

Facts and Fiction

Einleitung

- Staatsexamen
- Freiberufliche Tätigkeit für Landesbehörde
- Anstellung in Landesbehörde in zwei Bundesländern
- Diverse Fachtagungen verschiedener Behörden bei denen immer auch Ausschreibungen und Software thematisiert wird

Nachfolgend Erfahrungen und Interpretationen

Erfahrungsaustausch - keine Rechtsberatung!

Facts and Fiction
“Digitalisierung“

Erfahrungen eines Lehrers:

- Verpflichtung zum digitalen Klassenbuch – geht nur manchmal wegen Internet und am Whiteboard → nur in der Pause wegen Datenschutz
- PCs und Whiteboards veraltet und unbenutzbar langsam
- 24 Rechner für 32 Schüler pro Klasse
- WLAN unbenutzbar langsam oder nicht vorhanden
- Drucken nicht möglich, weil PCs noch mit Windows 7 und deshalb nicht an LAN angeschlossen
- Schulsoftware nicht mit Windows 11 kompatibel

Facts and Fiction
“Digitalisierung“

Erfahrungen an Forschungseinrichtung:

- Softwareausstattung jenseits der Anforderungen und Möglichkeiten → i.d.R. Datascience mit Excel, Dokumentation mit Word
- Speicherplatzbeschränkung, z.B. von 500 GB je Fachgebiet → wohin mit den Messdaten?
- Zugang zu Internetdiensten eingeschränkt bis unmöglich, z.B. ssh-Verbindung zu Server oder Videokonferenz nur über privaten Rechner und Leitung,
- Offline-Daten, z.B. für GIS-GNSS-Erfassung unmöglich da Synchronisierung z.B. via USB, Cloud verboten

Facts and Fiction
“OSS in Verwaltung - Vorurteile“

Highlights persönlicher Erfahrungen:

- Wir können OSS, insbesondere QGIS nicht nutzen weil wir dann auch alle Daten als Open Data veröffentlichen müssen.
  Die Daten von Open Street Map können wir aus den gleichen Gründen nicht nutzen.
- Die Daten von Open Street Map können wir nicht nutzen da sie eine niedrige Qualität haben und wir dann für die veröffentlichten Informationen in Haftung kommen.
- xls(x) und shape-Dateien sind interoperabel weil ich sie immer öffnen kann

Facts and Fiction
“OSS in Verwaltung - Vorurteile“

Highlights persönlicher Erfahrungen:

- FOSS ist unsicher, weil jedermann sofort Sicherheitslücken identifizieren und nutzen kann.
- FOSS hat einen schlechteren Funktionsumfang.
- FOSS ist low Budget und hat damit weniger Komfort.
- Foss ist allgemein eigentlich unfassbar teuer – weil soviel nachgearbeitet werden muss
- Für FOSS gibt es, wenn der Entwickler keine Lust mehr hat, keinen Support, weil eine Vertragsbindung fehlt.
- Wir können FOSS bei uns nicht einsetzen weil die Mitarbeiter das nicht bedienen können.

Facts and Fiction
“OSS in Verwaltung - Vorurteile“

OSBA: Open Source: Sieben Vor(ur)teile unter der Lupe:

- OSS ist nur ein vorübergehender Trend
- OSS öffnete Hackern Tür und Tor
- Jeder kann Fehler in den Code einbauen
- OSS Communities sind ein Haufen Chaoten
- Aktuelle Kundenanforderungen kann OSS nicht erfüllen
- Für kritische Bereiche ist OSS nutzlos
- Support muss man bei OSS lange suchen

Facts and Fiction
“Ausschreibung und Standards“

Highlights persönlicher Erfahrungen:

- Wir mussten diese Datenbank, dieses Programm nehmen da wir Vergaberechtlich gezwungen sind, den billigsten Anbieter zu nehmen.
- Die Software XY würden wir ja auch gerne beschaffen/entwickeln, das verbieten aber die IT-Standards des Landes und der Behörde.
- Die IT-Richtlinien des Landes verbieten uns die Nutzung diverser Software aus Sicherheitsgründen, deshalb kopieren sich die Mitarbeiter das auf USB und verarbeiten die Daten auf ihren privaten Rechnern.

Facts and Fiction

“Ausblick und Möglichkeiten“

Ablaufschema Beschaffung

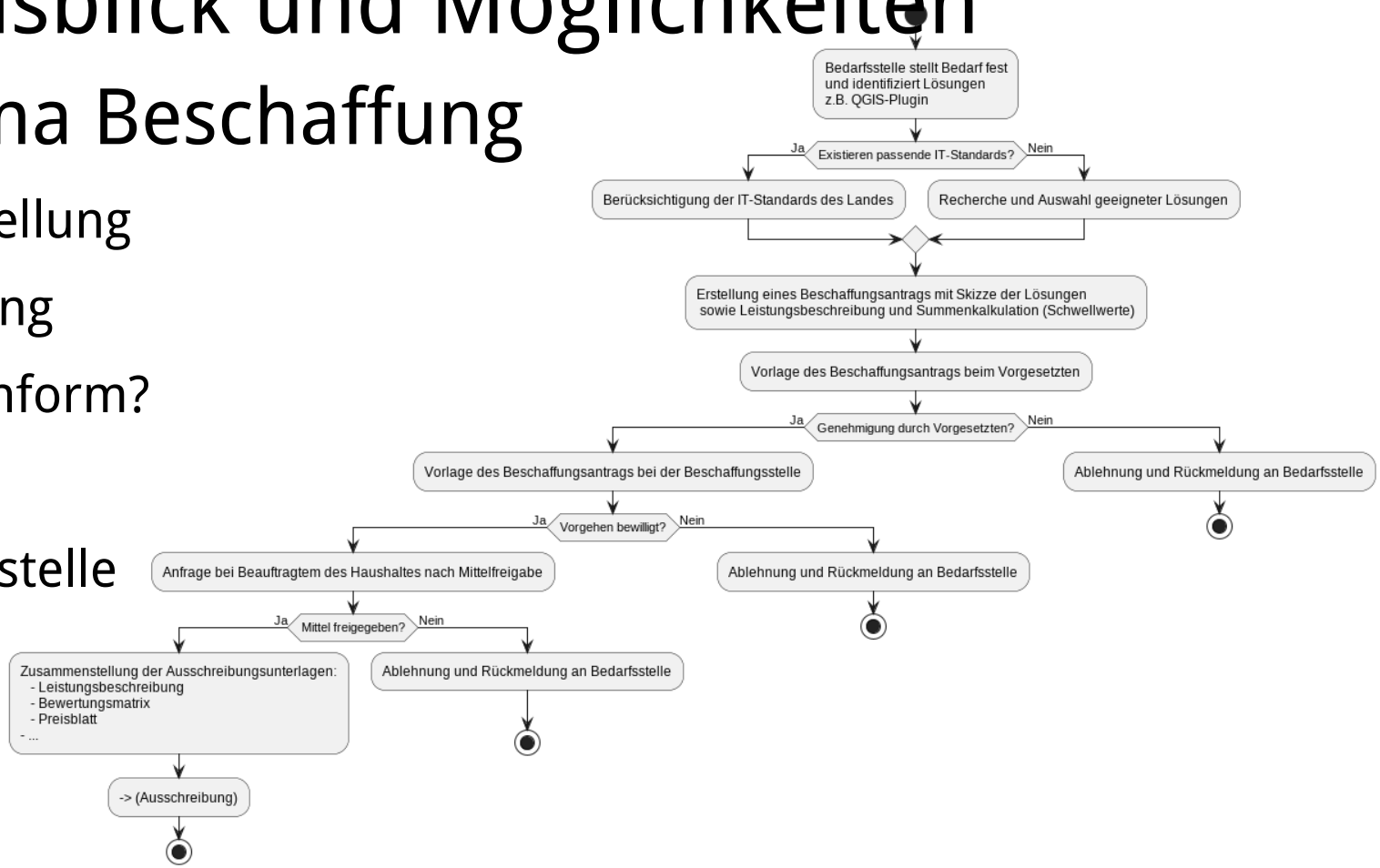
1 Bedarfsfeststellung

2 Lösungsfindung

3 Richtlinienkonform?

4 Vorgesetzte

5 Beschaffungsstelle



Facts and Fiction
“Ausblick und Möglichkeiten“

Landesstandards:

- Richtlinie über die Anwendung der IT-Strategie und von IT-Standards in der Landesverwaltung:
Die IT-Strategie legt verbindlich den Rahmen für den weiteren Ausbau der Informationstechnik in der Landesverwaltung fest. Alle Behörden, Einrichtungen und Betriebe des Landes planen und realisieren den IT-Einsatz in ihren jeweiligen Bereichen nach Maßgabe der in der IT-Strategie festgelegten Ziele, Leitlinien und Migrationswege.

- Die Strategie der Landesregierung sieht im gleichberechtigten Einsatz von Open Source Software (OSS) neben Closed Source Software (CSS) einen neuen zielführenden Ansatz, Lizenz- und Betriebskosten zu senken, den Wettbewerb zu beleben und bestehende Abhängigkeiten zurückzuführen. Daher unterstützt die Landesregierung den Einsatz von Open Source Software, soweit dies wirtschaftlich und inhaltlich sinnvoll ist.

Facts and Fiction
“Ausblick und Möglichkeiten“

Landesstandards:

Richtlinie über die Anwendung der IT-Strategie und von IT-Standards in der Landesverwaltung: **S**tandards und **A**rchitekturen für e**G**overnment-**A**nwendungen (SAGA)

- Verbindlich, Abweichungen unterliegen dem Genehmigungsvorbehalt
- Ziele: Wirtschaftlichkeit, Agilität, Offenheit, Sicherheit, Interoperabilität, Wiederverwendbarkeit, Skalierbarkeit
- Softwareklassifikation in „Beobachtet“, „Empfohlen“, „Verbindlich“
- Nur in begründeten Ausnahmen KÖNNEN beobachtete Standards empfohlenen Alternativen vorgezogen werden.

Facts and Fiction
“Ausblick und Möglichkeiten“

Landesstandards:

Standards und **A**rchitekturen für e**G**overnment-**A**nwendungen (SAGA) – Standards:

- Linux: Empfohlene Implementation: Red Hat Enterprise Linux ab Version 8.x, Suse Linux Enterprise Server ab Version 15 SP
- Datenbank: Empfohlene Implementation: Microsoft SQL, PostgreSQL 10.x, 11.x, 12.x
- GIS: nicht vorhanden aber gml, Kartenviewer-API, WFS, ...

Facts and Fiction
“Ausblick und Möglichkeiten“

Landesstandards:

- Einkauf und Entwicklung nicht ausgeschlossen: gibt es keinen beschriebenen Standard sind die Systeme so zu betrachten wie „vorgeschlagen“
- Erfüllung der beschriebenen Standards und
- IT-Grundschutz auf Basis der Sicherheitsmaßnahmen gemäß den Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und dem BSI-Grundschutzkompendium in der jeweils aktuellen Fassung gewährleistet werden.
- Feldversuch:

Dem Einsatz von [... Software] muss immer dann ein Feldversuch vorausgehen, wenn für den in Frage kommenden Anwendungsbereich […] ein neuer Standard auf der Ebene von Produkten empfohlen beziehungsweise festgelegt werden soll. Der Feldversuch wird unter Beteiligung der interessierten Ressorts und des zentralen IT-Dienstleisters durchgeführt, wobei die eGovernment- und IT-Leitstelle die Koordinierung übernimmt.

Facts and Fiction - Fazit
“Ausblick und Möglichkeiten“

Lösungsmöglichkeiten machen Arbeit für Bedarfs- und Beschaffungsstelle:

- Begründungen im Beschaffungsantrag, z.B. Schutzgut der Daten, Feldversuch, …
- Auseinandersetzung mit Beauftragten des Haushalts zur Wirtschaftlichkeitsklärung
- Erklärungen gegenüber der Beschaffungsstelle – „Beschaffungsstelle sollte [bei Beschaffung von Software] mit 20 verschiedenen Lizenzen umgehen können
- Leistungsbeschreibung: so genau wie nötig; Bewertungsmatrix und abbedungender EVB-IT-Vertrag nicht vergessen :)
- Dokumentation und IT-System-Verfahrensbeschreibung …

Facts and Fiction - Fazit

“Schwierigkeiten in der Digitalisierung“

- Wissen und Einstellung von Entscheidungsträgern – Peter Prinzip, Beförderung nach Zugehörigkeitsdauer …
- mangelnde Ausbildung, Befähigung, Erfahrung der Ausführenden
- Schwierigkeiten in Anwendungsfällen zu denken bzw. Prozesse zu transformieren – Schreibmaschine → MS-Word
- Angst zur Entscheidung bei Unsicherheit und kognitive Abkürzungen, z.B. wird zuerst an „Einkauf von der Stange“ und Service von außen statt an eigene Prozesse und Befähigung gedacht
- Fehlendes Durchhaltevermögen und Prozessbegleitung, gerade bei Versuchen oder Förderungen

Facts and Fiction - Fazit
“Schwierigkeiten für Foss“

- Starre Regularien und schwerfällige Änderung dieser
- Wissen und Einstellung zu Software und den damit eigentlich abzubildenden Prozessen
- Schwierigkeiten in Anwendungsfällen und Prozessen sowie der Möglichkeit der Unterstützung mit Software zu denken
- Angst zur Entscheidung bei Unsicherheit und kognitive Abkürzungen sowie Vermeidung von Arbeit, z.B. wird zuerst an „Einkauf von der Stange“ und Service von außen statt an die Erstellung eines Aktivitätsdiagrammes und einer Leistungsbeschreibung gedacht
- Fehlende Kreativität und fehlendes Durchhaltevermögen und Prozessbegleitung bei der Beschaffung

Facts and Fiction - Fazit

“Schwierigkeiten?“

- Lösbar :)
- Mehr Wissen und mehr Arbeit zu investieren
- Mitstreiter Notwendig

Wissen und Mitstreiter vorhanden :)

Fragen – Antworten - Zusammenfassung

Frage an Miriam:
Wie lange wir es denn dauern, bis der Vorrang OSS in der Beschaffung umgesetzt ist?
* Wunsch: zum Ende des Jahres
* Realität: Auch wenn es im Gesetz steht, passiert es nicht automatisch, es braucht viel Aufklärung und Information.