

Digitale Souveränität

Wie geht das ohne Bullshit-Bingo?

Notwendigkeit digitaler Souveränität

Digitale Souveränität

= Fähigkeit, digitale Komponenten, d.h. **Software, Dienste, Hardware, Daten, Prozesse**, autonom nutzen, kombinieren, anpassen und **kontrollieren zu können**.

- ✓ Flexibilität und Agilität
- ✓ resiliente IT-Infrastruktur
- ✓ Innovationsfreiheit



Digitale Abhängigkeit

= fehlende Wechselfähigkeit und damit verbundene Risiken für:

- ! Kostensteigerungen
- ! Produktivitätseinbußen
- ! Datenschutzgesetze
- ! Innovationsgrenzen

Definitionen am Markt

Beispiel: Amazon Web Services



»AWS bietet schon heute eine breite Palette an Datenschutz-Funktionen, Zertifizierungen und vertraglichen Zusicherungen an, die Kunden Kontrollmechanismen darüber geben, **wo ihre Daten gespeichert sind, wer darauf Zugriff erhält und wie sie verwendet werden.**«

Definitionen am Markt

Beispiel: Amazon Web Services



Legale Anforderungen eingehalten



keine Kompatibilität, ggf. sogar neue Abhängigkeiten

Definitionen am Markt

Beispiel: Delos Cloud



- Stellt Features der Microsoft Cloud bereit
- Zielgruppe: Öffentliche Verwaltung
- Hosting in Deutschland, dt. Firma
- Telemetriedatenaustausch zu Microsoft durch BSI reguliert

Definitionen am Markt

Beispiel: Delos Cloud



DELOS
CLOUD



wahrscheinlich Trennung
von Cloud-Act



weiterhin Feature-Lock-In,
Preisabhängigkeit

Definitionen am Markt

Beispiel: Juniper Mist AI



- Juniper: Netzwerkgerätehersteller: WLAN, Router, Switches
- Juniper Mist = automatisiertes Netzwerkmanagement
- Marketing mit digitaler Souveränität
 - Wahl Speicherort: USA, UK, EU, Kanada, Australien
 - Lizenz sichert Dateneigentum

Definitionen am Markt

Beispiel: Juniper Mist AI



Datenschutz adressiert

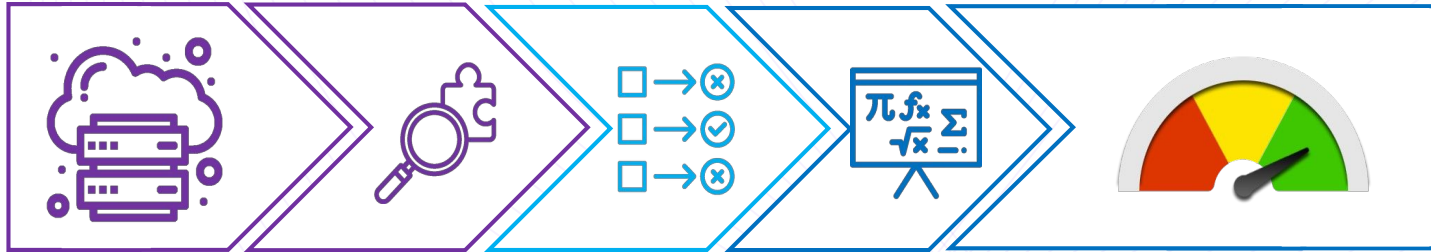


weiterhin US-Entität

Quantifizierung digitaler Souveränität



Quantifizierung digitaler Souveränität

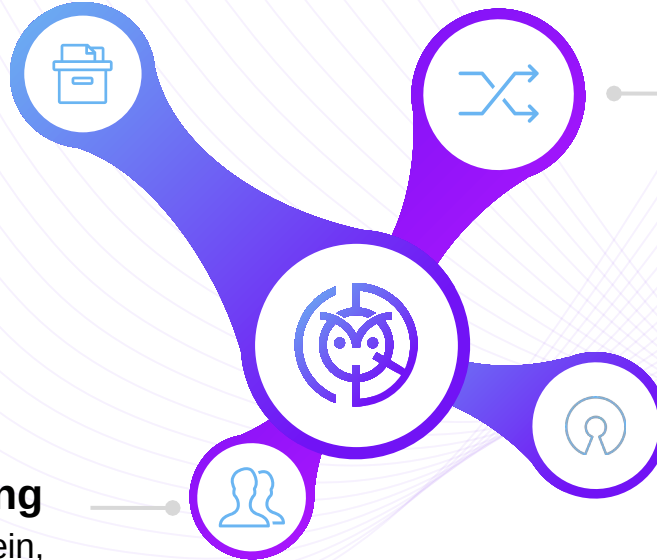


- ✓ allgemeine Bereiche mit festen Kriterien
- ✓ detaillierter Souveränitätsscore zwischen 0 und 5
- ✓ individuelle Wichtung der Komponenten

Grundpfeiler für digitale Souveränität

Datensouveränität

Datenhoheit,
Datenmigrierbarkeit



Kompetenzentwicklung

Problembewusstsein,
Wissen über IT-Infrastruktur

Komponenten

Existenz von Alternativen,
Migrationsaufwände

Open Source

Einsatz von Open Source,
Communitystabilität

Datensouveränität

Sicherstellen, dass Daten in Zukunft verwendet werden können.



Datenlokalisierung

Wo liegen die Daten (Cloud Act)?
Wie sicher liegen die Daten?



Datenzugriff

Sind die Daten erreichbar?
Ist Zugriffskontrolle souverän?



Datenexport/portabilität

Ist Export möglich?
Standardisierte Formate?
Migrationstools?



Verschlüsselung

Ist Entschlüsselung gewährleistet?



Komponenten



Services

SaaS, PaaS, IaaS



Hardware

Ausfallsicherheit, Support,
Ersatzteile



Cloudinfrastruktur

Alternativanbieter,
Migrationsaufwand



Tools

Alternativen,
Featurevollständigkeit,
Schnittstellenkompatibilität,
Verfügbarkeit



Kompetenzentwicklung

Wie sind Kompetenzen bezüglich digitaler Souveränität im Unternehmen entwickelt?



Risikobewusstsein

bei Führung und Mitarbeitern zur Erkennung von Lock-Ins



Kenntnisse eigener Infra

Wissen ist abrufbar intern vorhanden, Zuständigkeiten sind klar



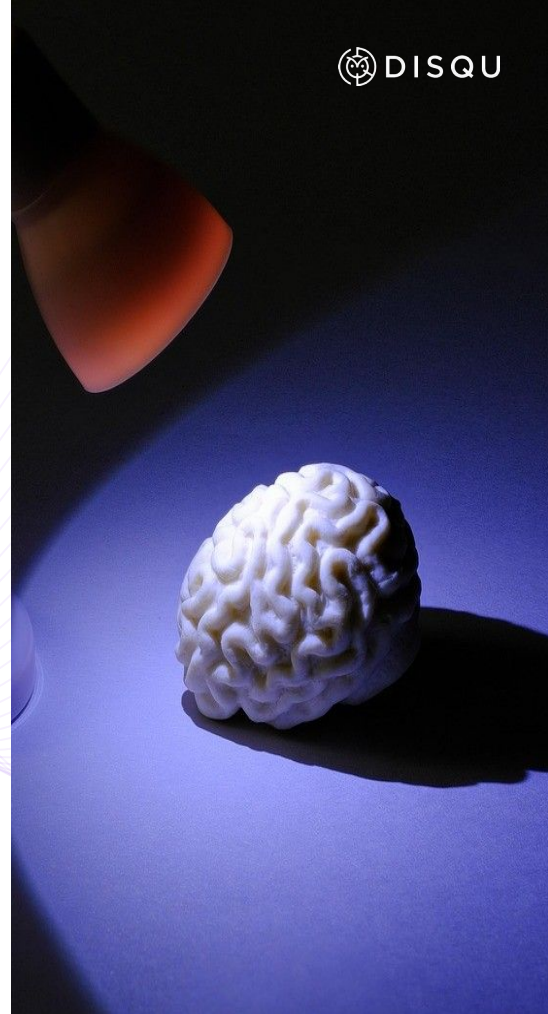
Strategie

Sind mögliche Alternativen und Migrationspfade bekannt?



Kostenmanagement

Überwachung und Vergleich der Kostenentwicklung



Open Source



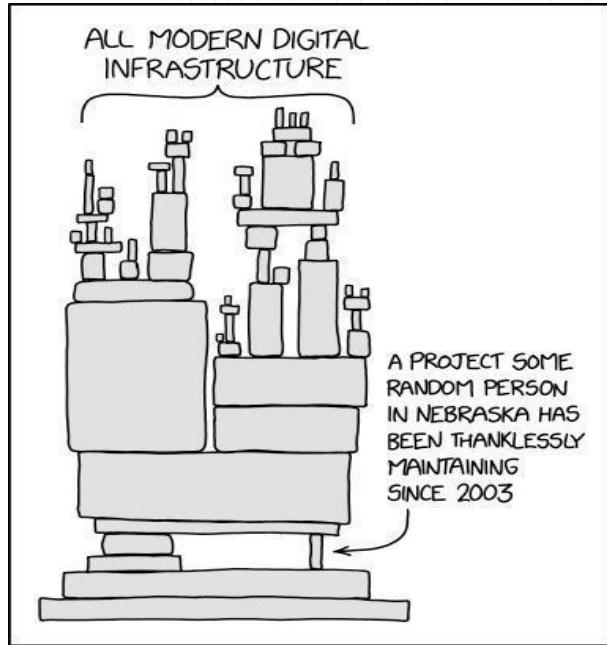
Anteil



Community

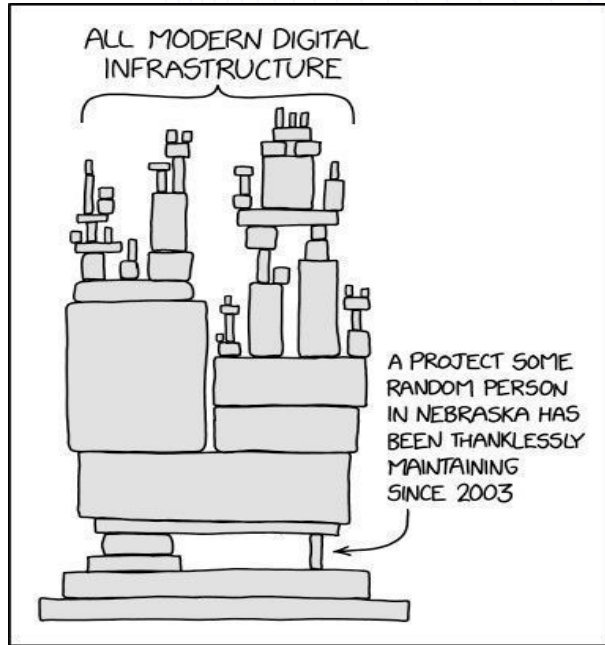


Open Source als Allheilmittel?

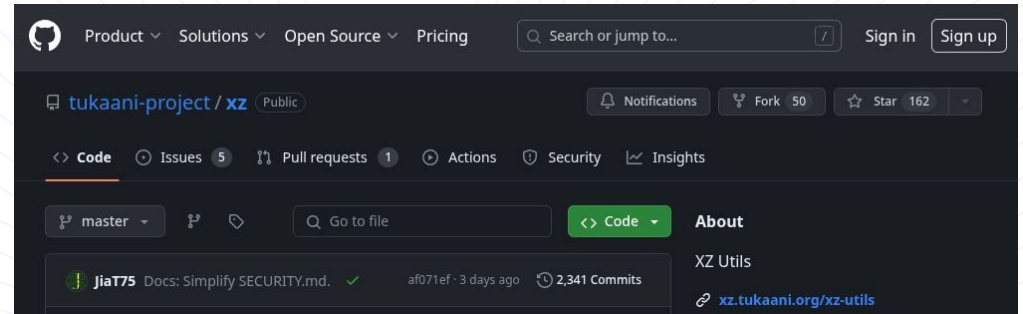


<https://xkcd.com/2347/> (License: CC BY-NC 2.5)

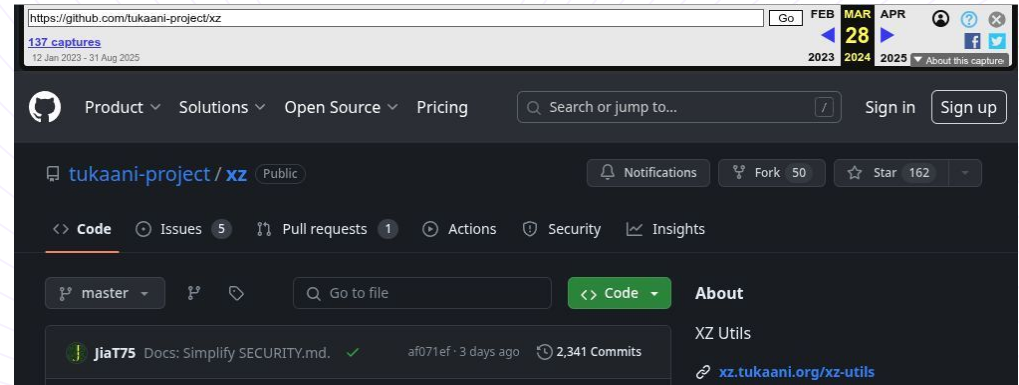
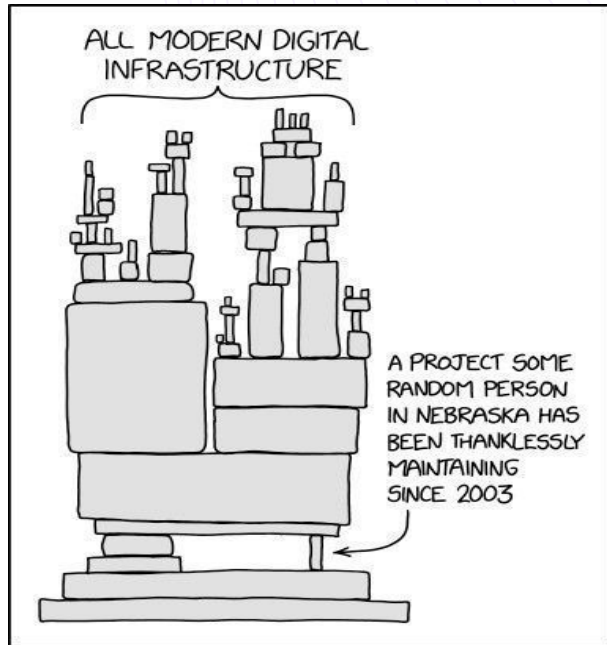
Open Source als Allheilmittel?



<https://xkcd.com/2347/> (License: CC BY-NC 2.5)

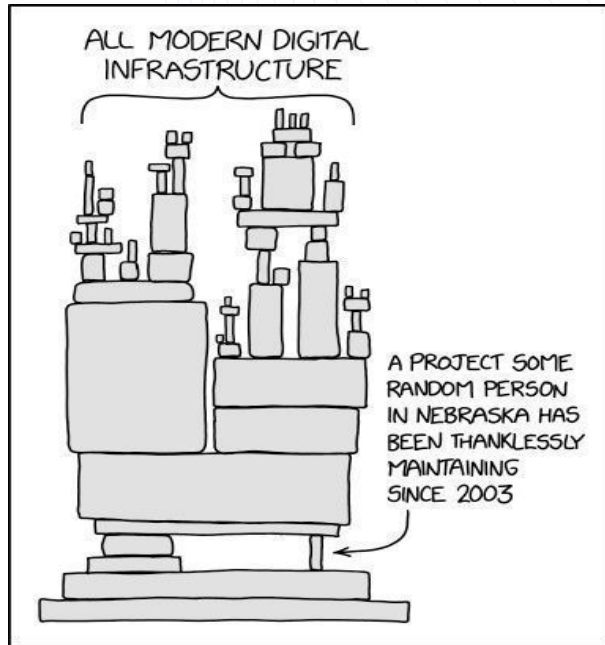


Open Source als Allheilmittel?



<https://xkcd.com/2347/> (License: CC BY-NC 2.5)

Open Source als Allheilmittel?



<https://xkcd.com/2347/> (License: CC BY-NC 2.5)

<https://github.com/tukaani-project/xz>

137 captures
12 Jan 2023 - 31 Aug 2025

Product Solutions Open Source Pricing Search or jump to... Sign in Sign up

tukaani-project / xz Public Notifications Fork 50 Star 162

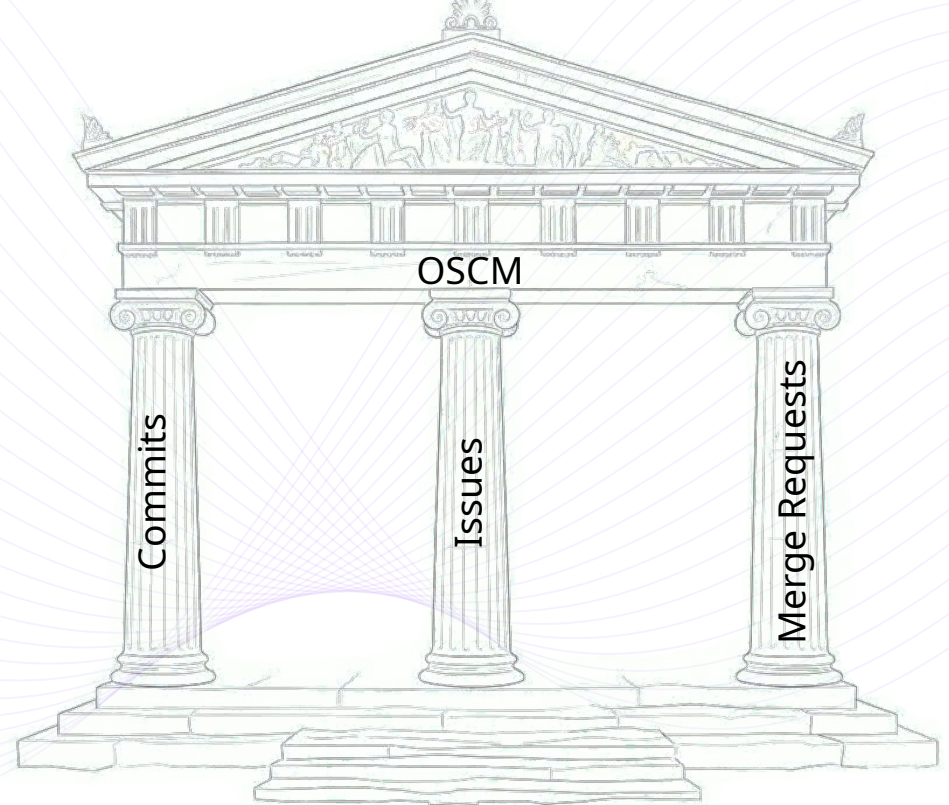
CVE-2024-3094: liblzma backdoor

XZ Utils 5.6.0 (2024-02-24) and 5.6.1 (2024-03-09) release tarballs contain a backdoor that was inserted by a malicious co-maintainer. It was [discovered by Andres Freund](#) and made public on 2024-03-29. The incident is known as [CVE-2024-3094](#).

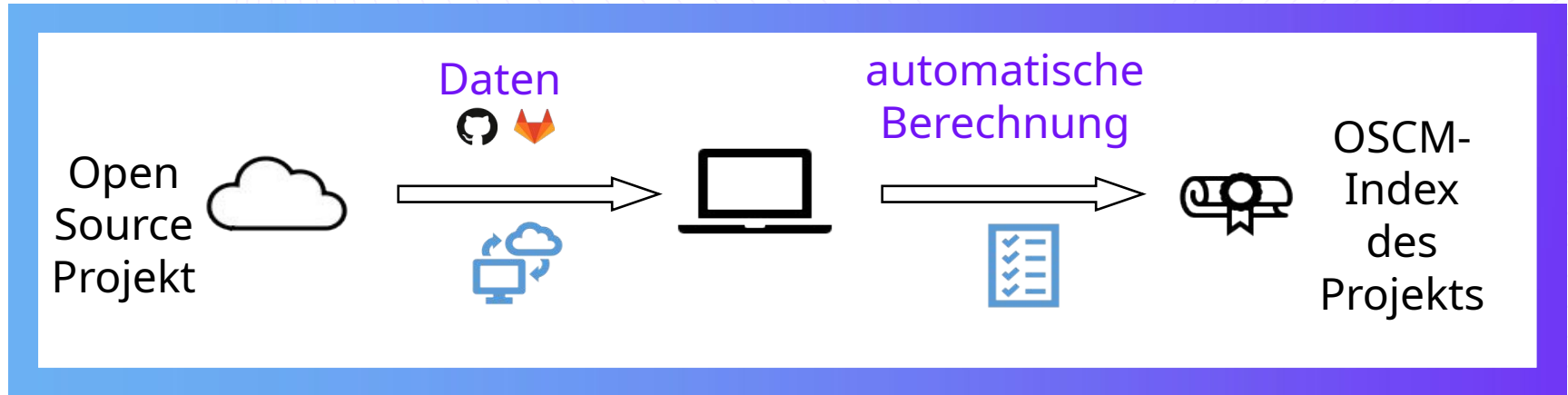
This is still being investigated. See the [XZ Utils backdoor](#) page for more information and also the [XZ Utils review notes](#).

Community Aktivität messbar machen

- 3 Kernbereiche
- Kriterien: 0 bis 5 Punkte
 - Schwellendefinition der Punkte
- Gesamtdurchschnitt für schnellen Gesamteinblick

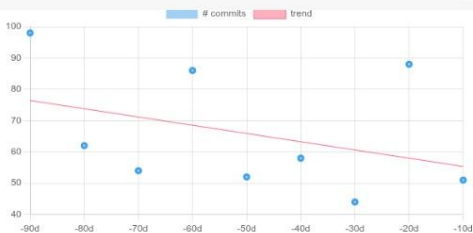


Community Aktivität messbar machen





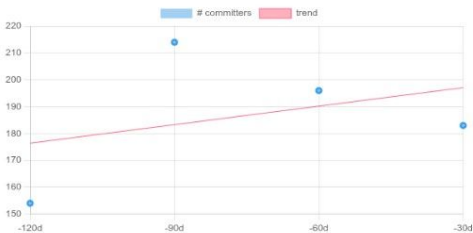
Overall result Metrics based on: Commits Issues Pull Requests



Score: 0/5

This metric checks the trend of the amount of commits. Therefore, the number of commits in the last nine 10 day timespans is counted. To get the trend, a linear regression is applied to those values. Stable and increasing numbers are a good indicator. Steeper decreasing will result in a lower score.

Committers



Score: 5/5

This metric checks how many people are contributing code to the project (counting the number of commits). Therefore, the number of different people creating commits is counted for four timeframes of 30 days. These numbers are interpolated to linear function, to check if the trend of committers is going down, up or stays stable. The more the trend is going down, the less points are given to the project.

Elephant in the room

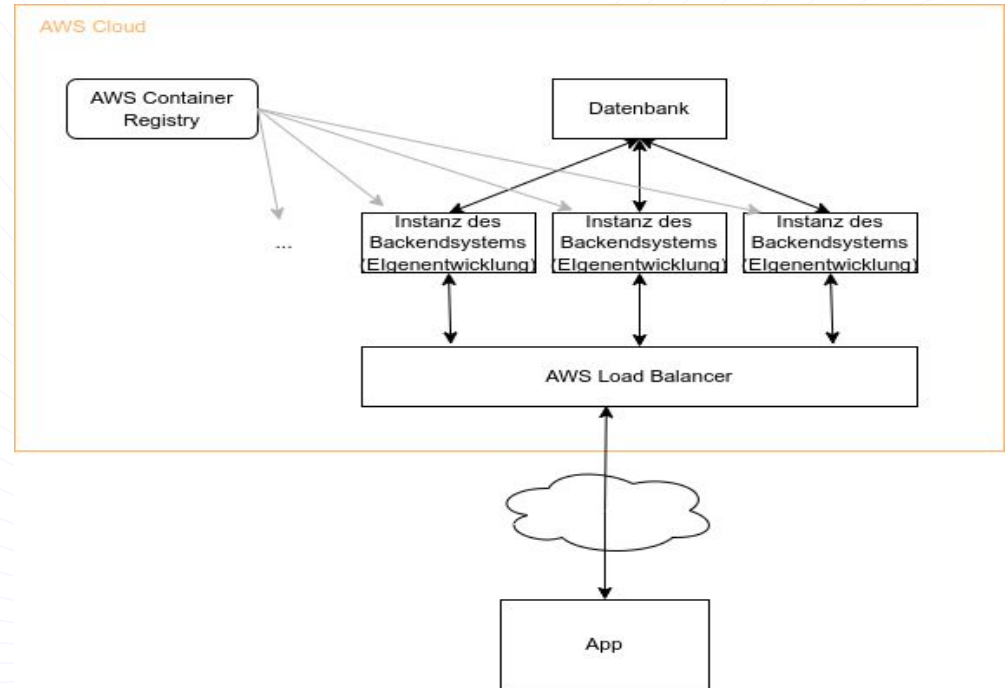


Score: 5/5

This metric checks how many people are contributing half of the commits to the project. They are called elephants in the room. It is not good for a project, if there is only one elephant in the room, so more people needed to reach 50% of the comments is better. Basis are all commits in the last 120 days.

Quantifizierung am Beispiel

- App: Vermittlung von Taxifahrten
- App + Backend selbst entwickelt
 - App: Kotlin + Android SDK
 - Backend: Python + FastAPI
- Backend wird in Amazon Web Services betrieben
 - Anwendung als Docker-Container
 - Infrastruktur (Hosting, Datenbank, Load Balancing) von AWS bezogen



Datensouveränität

Sicherstellen, dass Daten in Zukunft verwendet werden können.



Datenlokalisierung

Wo liegen die Daten
(Cloud Act)?
Wie sicher liegen die
Daten?



Datenzugriff

Sind die Daten
erreichbar?
Ist Zugriffskontrolle
souverän?



Datenexport/portabilität

Ist Export möglich?
Standardisierte Formate?
Migrationstools?



Verschlüsselung

Ist Entschlüsselung
gewährleistet?



Bewertung 1.1: Datenlokalisierung

Bewertung	Beschreibung
0 Punkte	keine Sicherung des Speicherorts, Informationen über Ausfallwahrscheinlichkeit und Schutz vor fremdem Datenzugriff fehlen
1 Punkt	Leichte Absicherungsmaßnahmen. Mittelschwere Vorfälle können Ausfälle verursachen, Zugriff durch Dritte unwahrscheinlich.
2 Punkte	Gute Absicherung. Schwere Vorfälle können Ausfälle verursachen, Zugriff durch Dritte nur in Extremsituationen möglich.
3 Punkte	
4 Punkte	Unabhängiges Backup (nicht an gleichem Speicherort; nicht bei gleichem Anbieter, falls es ein Drittanbieter ist) der Daten vorhanden. Zugriff durch Dritte unwahrscheinlich.
5 Punkte	Unabhängiges Backup (nicht an gleichem Speicherort; nicht bei gleichem Anbieter, falls es ein Drittanbieter ist) der Daten vorhanden. Zugriff durch Dritte nahezu ausgeschlossen.

- Apps betreiben nur Caching, halten keine Daten lokal vor
- Backend speichert sämtliche Daten in PostgreSQL-Datenbank (als AWS RDS-Cluster bezogen)

Bewertung 1.1: Datenlokalisierung

Bewertung	Beschreibung
0 Punkte	keine Sicherung des Speicherorts, Informationen über Ausfallwahrscheinlichkeit und Schutz vor fremdem Datenzugriff fehlen
1 Punkt	Leichte Absicherungsmaßnahmen. Mittelschwere Vorfälle können Ausfälle verursachen, Zugriff durch Dritte unwahrscheinlich.
2 Punkte	Gute Absicherung. Schwere Vorfälle können Ausfälle verursachen, Zugriff durch Dritte nur in Extremsituationen möglich.
3 Punkte	
4 Punkte	Unabhängiges Backup (nicht an gleichem Speicherort; nicht bei gleichem Anbieter, falls es ein Drittanbieter ist) der Daten vorhanden. Zugriff durch Dritte unwahrscheinlich.
5 Punkte	Unabhängiges Backup (nicht an gleichem Speicherort; nicht bei gleichem Anbieter, falls es ein Drittanbieter ist) der Daten vorhanden. Zugriff durch Dritte nahezu ausgeschlossen.

- Apps betreiben nur Caching, halten keine Daten lokal vor
- Backend speichert sämtliche Daten in PostgreSQL-Datenbank (als AWS RDS-Cluster bezogen)

Bewertung 1.6: Datenportabilität

Bewertung	Beschreibung
0 Punkte	Keine einheitlichen Datenformate Keine Definition der Programme, die diese Daten verarbeiten können müssen
1 Punkt	Mindestanforderungen an genutzte Datenformate und verwendende Programme sind definiert: Dokumentierte Schnittstellen des Datenaustauschs.
2 Punkte	Alternative Programme können einen Großteil der verwendeten Datenformate verarbeiten.
3 Punkte	Alle Daten lassen sich in offene Datenformate konvertieren , Migrationstools werden vorgehalten.
4 Punkte	Alle Daten in offene Datenformate konvertierbar, Migrationstools und -verfahren sind getestet.
5 Punkte	Alle Daten liegen in standardisierten Datenformaten vor. Alle genutzten Schemata der Datenformate liegen ebenfalls vor.

- Apps betreiben nur Caching, halten keine Daten lokal vor
- Backend speichert sämtliche Daten in PostgreSQL-Datenbank

Bewertung 1.6: Datenportabilität

Bewertung

Beschreibung

0 Punkte

Keine einheitlichen Datenformate

Keine Definition der Programme, die diese Daten verarbeiten können müssen

1 Punkt

Mindestanforderungen an genutzte Datenformate und verwendende Programme sind definiert:
Dokumentierte Schnittstellen des Datenaustauschs.

2 Punkte

Alternative Programme können einen Großteil der verwendeten Datenformate verarbeiten.

3 Punkte

Alle Daten lassen sich **in offene Datenformate konvertieren**, Migrationstools werden vorgehalten.

4 Punkte

Alle Daten in offene Datenformate konvertierbar, **Migrationstools und -verfahren sind getestet.**

5 Punkte

Alle Daten liegen in **standardisierten Datenformaten** vor. Alle genutzten Schemata der Datenformate liegen ebenfalls vor.

- Apps betreiben nur Caching, halten keine Daten lokal vor
- Backend speichert sämtliche Daten in PostgreSQL-Datenbank

Komponenten



Services

SaaS, PaaS, IaaS



Hardware

Ausfallsicherheit, Support,
Ersatzteile



Cloudinfrastruktur

Alternativanbieter,
Migrationsaufwand



Tools

Alternativen,
Featurevollständigkeit,
Schnittstellenkompatibilität,
Verfügbarkeit



Bewertung 2.2: Flexibilität Cloudstruktur

Bewertung	Beschreibung
0 Punkte	keine Cloudanbieter mit gleichen Features
1 Punkt	gleiche Features, aber verschiedene Schnittstellen
2 Punkte	Es existieren schnittstellenkompatible Cloudanbieter mit gleichen Features
3 Punkte	2 oder mehr schnittstellenkompatible Cloudanbieter existieren
4 Punkte	Kompatibilität der Schnittstellen getestet
5 Punkte	Multicloud-Strategie aktiv oder Setup kann mit minimalen Anpassungen bei alternativem Anbieter gestartet werden (gleicher Technologiestack)

Genutzte Dienste in AWS-Infrastruktur:

- PostgreSQL-Cluster
- Load Balancer
- Docker Registry
- Docker Container als Service (ECS)

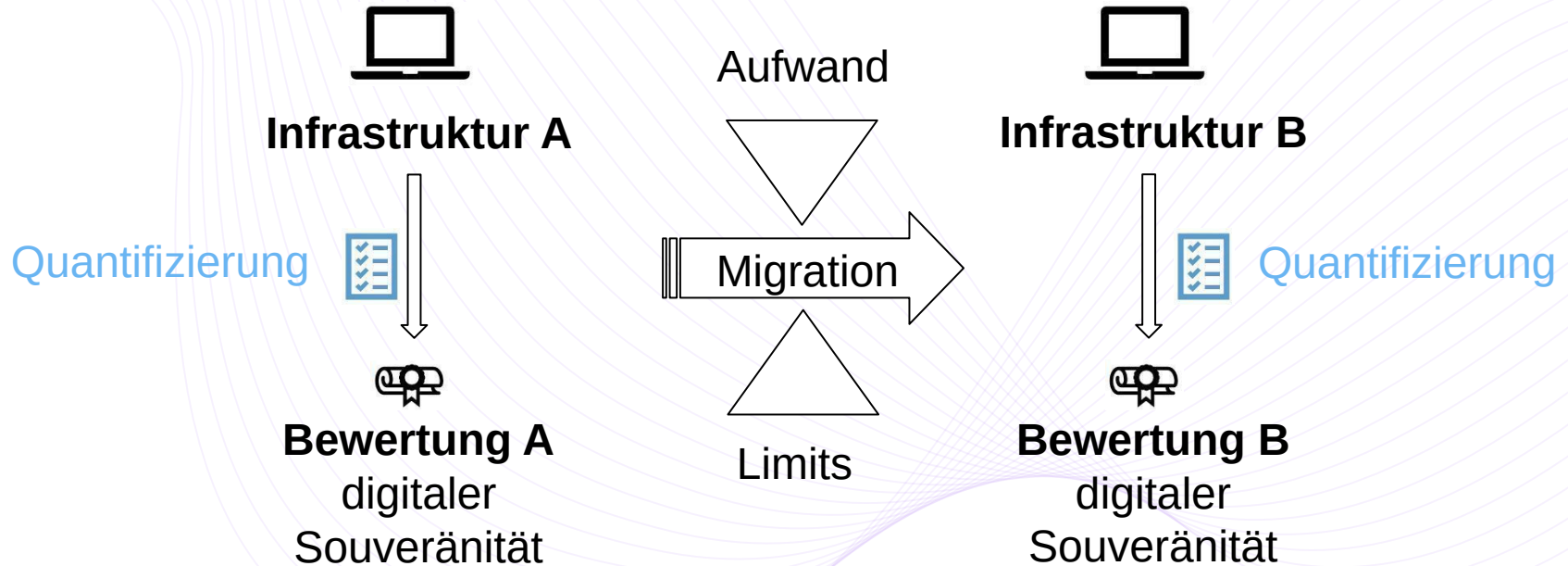
Bewertung 2.2: Flexibilität Cloudstruktur

Bewertung	Beschreibung
0 Punkte	keine Cloudanbieter mit gleichen Features
1 Punkt	gleiche Features, aber verschiedene Schnittstellen
2 Punkte	Es existieren schnittstellenkompatible Cloudanbieter mit gleichen Features
3 Punkte	2 oder mehr schnittstellenkompatible Cloudanbieter existieren
4 Punkte	Kompatibilität der Schnittstellen getestet
5 Punkte	Multicloud-Strategie aktiv oder Setup kann mit minimalen Anpassungen bei alternativem Anbieter gestartet werden (gleicher Technologiestack)

Genutzte Dienste in AWS-Infrastruktur:

- PostgreSQL-Cluster
- Load Balancer
- Docker Registry
- Docker Container als Service (ECS)

Verwendung der Quantifizierung



Soon: Open Source

Standard Quantifizierung:



Standard OSCM:



SLAC Secure Linux
Administration Conference

Be open
and source.

Vielen Dank für die Aufmerksamkeit

www.disqu.de
team@disqu.de