Open Source: Ohne Vertrauen geht es nicht!

DB Systel
Moving the digital future. Together.

DB Systel GmbH | Cornelius Schumacher | Chief Technology Office | 17.9.2019

Vorstellung

- Cornelius Schumacher
- Open Source Steward bei DB Systel

- DB Systel: Digitalisierungspartner der Deutschen Bahn

- Open Source Steward: Unterstützung und Compliance von Einsatz und Entwicklung von Open-Source-Software

- Cornelius.Schumacher@deutschebahn.com

Open Source Policies

- Was ist das?
  - Regeln für den Umgang mit Open-Source-Software im Unternehmen
- Wozu ist es gut?
  - Rahmen für optimale Nutzung von Open-Source im Unternehmen
  - Rahmen für Zusammenarbeit mit der Open-Source-Community
  - Wahrung der Unternehmensinteressen
  - Transparenz über den Open-Source-Prozess
    - Intern
    - Gegenüber Kunden
    - In der Community

Vertrauen ist gut, Kontrolle ist besser?

Freiheit geht einher mit Verantwortung?

Vertrauen als Treiber von Open Source

- Open Source kommt mit großen Freiheiten
- Braucht Vertrauen:
  - In die Menschen: Motivation, Autonomie
    - Nicht dass Menschen keine Fehler machen, das wäre naiv
    - Aber dass Menschen lernen, Fehler addressieren, Risiken sehen und entsprechende Maßnahmen ergreifen
  - In die Prozesse: Reduktion von geistiger Last
  - In die Automation: Geschwindigkeit, Skalierung, Sicherheit

Komponenten einer Open Source Policy

Verwendung von Open Source Software
Szenarien

- Nutzen als Anwender
- Als Teil eines Services verwenden
- Als Teil eines Produktes ausliefern
- Anpassen
- Angepasste Version ausliefern

Verwendung von Open Source Software
Anforderungen (1/2)

- Kriterien für Auswahl von Projekten
  - Akzeptable Lizenzen
  - Gesundheit von Projekt und Community
  - Technische Kriterien (Abhängigkeiten, Programmiersprache)

- Externe Anforderungen
  - Verpflichtungen durch die Lizenz
  - Attribution
  - Source-Code zu Verfügung stellen (copyleft)
  - Kombination von Lizenzen
  - Datenschutz (insbesondere bei Services)

Verwendung von Open Source Software
Anforderungen (2/2)

- Interne Anforderungen
  - Archiv von Code, um Release-Builds reproduzieren und fixen zu können (z. B. Sicherheitsupdates)
  - Dokumentation der Verwendung (Bill of Materials)
  - Genehmigung der Verwendung (Lizenz-Review)
  - Patente

Contributions zu Open Source Software
Szenarien

- An der Community teilnehmen (Diskussion, Bug Reports, etc.)
- Code zu existierendem Projekt beitragen
- Nicht-Code Contributions: Dokumentation, Design, ...
- Eigenes Projekt betreiben

Contributions zu Open Source Software
Anforderungen (1/3)

- Externe Anforderungen
  - Lizenz
  - Developer Certificate of Origin (DCO)
  - Contributors License Agreement (CLA)
  - Contribution Policies
  - Code of Conduct
  - Kultur

Contributions zu Open Source Software
Anforderungen (2/3)

- Interne Anforderungen für Contributions an existierende Projekte
  - Schutz von proprietärem Code
  - Schutz von Geschäftsgeheimnissen
  - Überprüfung des Rechts, Code beizutragen (interne, 3rd party)
  - Dokumentation von Contributions
  - Marketing als "Good Citizen"
  - Attribution (Copyright-Hinweise, Versions-Kontroll-Richtlinien, AUTHORS files)

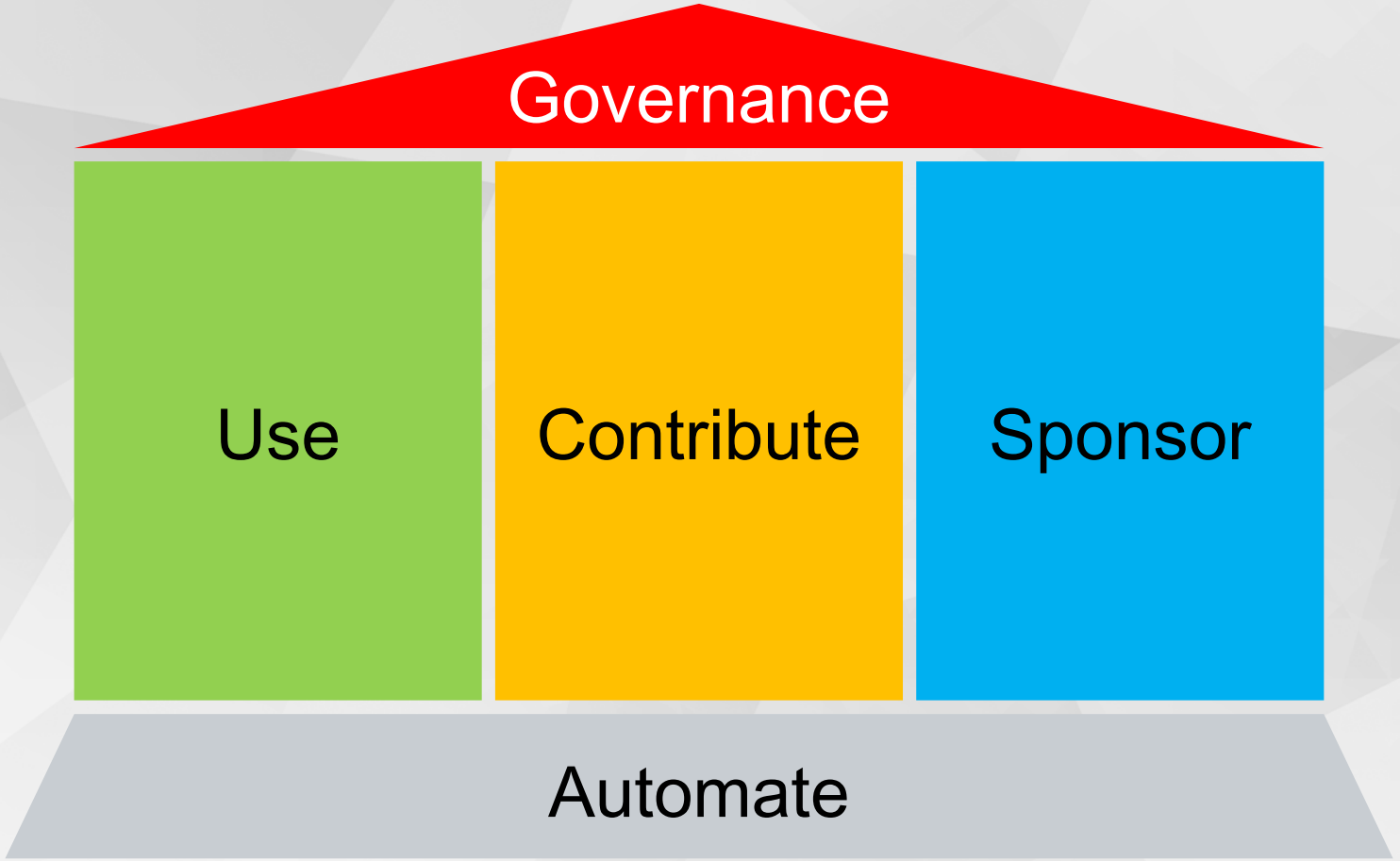
Contributions zu Open Source Software
Anforderungen (3/3)

- Eigene Projekte
  - Auswahl der Lizenz
  - Verantwortung als Maintainer
  - Einbinden von externen Entwicklern als Maintainer
  - Anforderungen an externe Contributions (Lizenz, DCO, CLA, ...) (Spiegel der externen Anforderungen)
  - Infrastruktur (Code Hosting, Kommunikations-Platform, Release-Prozess, ...)
  - Best Practices

Sponsoring von Open Source Software
Szenarien

- Mitgliedschaft in Open-Source-Organisationen
- Event-Sponsoring
- Bezahlen von Entwicklern

Konstruktion einer Open Source Policy



Checkliste Open Source Policy

- Projekt-Auswahl
  - Lizenzen, Projekt-Gesundheit, Technik
- Externe Bedingungen
  - Rechtlich, kulturell
- Interne Anforderungen
  - Schutz des Geschäfts, Risikomanagement, Außenwirkung
- Rahmen für eigene Projekte
  - Externe Bedingungen für andere, Nachhaltigkeit
- (Sponsoring von Open Source Projekten)

Wie war das mit dem Vertrauen?

Vertrauen in Beispielen (1/3)

- *"Patches that don’t require any review! (...) Any Google-maintained open source project like Chromium, Android, Go, etc."*

  https://opensource.google.com/docs/patching/

- *"We understand and sympathize with the desire to explore and ship technology projects outside of Google"*

  https://opensource.google.com/docs/iarc/

Vertrauen in Beispielen (2/3)

- *"WARNING: Code licensed under the GNU Affero General Public License (AGPL) MAY NOT be used at Google."*

  https://opensource.google.com/docs/using/agpl-policy/

- *"All code licensed under an OSI approved license can generally be used."*

  https://opensource.suse.com/suse-open-source-policy

Vertrauen in Beispielen (3/3)

- *"Don’t contribute code which gives us an edge over competitors"*

  https://opensource.zalando.com/docs/using/contributing/

- *"Für jedes geplante Contributions- oder Neuveröffentlichungsvorhaben ist eine Risikobewertung zu erstellen. Der Umfang der Risikobewertung hängt vom Risiko ab"*

  https://github.com/dbsystel/open-source-policies/blob/master/Open-Source-Contribution-Policy.md

Kriterien für Vertrauen

- Anwendung
  - Je kritischer, desto mehr Kontrolle notwendig
- Reife der Kontributoren
  - Je reifer, desto mehr Vertrauen möglich, strikte Regeln am Anfang
- Automatisierung
  - Vertrauen verschiebt sich von Personen zu Technik
  - Erfordert Kontrolle der Technik
- Differenziertes Vertrauen
  - Nicht über einen Kamm scheren
  - Risiko in Betracht ziehen
- Geschäftsmodell
  - Unterschiedliche Regeln für Lizenzverkauf, Support, Betreiben von Services, ...

Open Source Policies als Meßsystem für Vertrauen

- Aus Open Source Policies lässt sich ablesen, wo und wieviel Vertrauen besteht

- Wird die Policy überhaupt veröffentlicht?
  - Vertrauen in die Offenlegung von Prozessen
- Wieviel Freiheit hat der Einzelne?
  - Vertrauen in Mitarbeiter
- Wie automatisiert sind die Prozesse?
  - Vertrauen in Werkzeuge
- Wie breit ist der Anwendungsbereich der Policy?
  - Vertrauen in Geschäftsmodell

Fallstudie DB Systel

- Richtlinie Open Source Contribution
- (https://github.com/dbsystel/open-source-policies/blob/master/Open-Source-Contribution-Policy.md)
- Formaler Freigabeprozess für Contributions und Neuveröffentlichungen

- Zukünftige Verfeinerungen:
  - Vereinfachter Freigabeprozess bei geringem Risiko:
    - Geringer Umfang (Bug-Fixes, Snippets)
    - Definierte, gut verstandene, Lizenzen
    - Fachlich unkritische Themen (z.B. Standard-Werkzeuge, nicht-Code)
  - Wiederkehrende Contributions:
    - Gültigkeit der Freigabe für Serie von Contributions
    - Veränderung der Bedingungen (Projekt, Teilnehmer, Risiken) benötigt neue Freigabe
    - Periodische Überprüfung

Zusammenfassung

- Open Source braucht Vertrauen
- Vertrauen braucht einen Rahmen
- Eine Open Source Policy schafft den Rahmen
- Checkliste als Leitfaden
- Differenzierte Abwägung von Vertrauen und Kontrolle, abhängig von Anwendung, Reife, Automatisierung, Risiko und Geschäftsmodell

Vielen Dank für Ihre Aufmerksamkeit