Vom Wunsch nach Digitaler Souveränität bis zur Deutschen Verwaltungstrategie

Ein Reisebericht

Thomas Fricke

6. Juni 2023

re:publica

Wer bin ich?

- Berlin
- Cloud
  - Security Architect
  - Kubernetes Security Hacker
  - Critical Infrastructure
  - Baut Clouds
- Freelancer
- Cofounder of Endocode and Resility
- Open Source since 1988
- Linux since 0.95
- Promoviert in Statistischer Physik und Quantenmechanik, RWTH Aachen
- Gründungsmitglied des Innovationsverbund Öffentliche Gesundheit e.V

re:publica

Souveränität – ein problematischer Begriff

- Spannende Diskussion unter Staatsrechtlern
- **Begriff von verhängnisvolle[r] Vieldeutigkeit**

  Hans Kelsen, nach Herder Staatslexikon Online
- Hans Kelsen
  - **Respekt gegenüber Minderheiten als „höchsten Wert“ einer repräsentativen Demokratie**
  - Architekt der österreichischen Bundesverfassung, bis heute
  - Verfassungsgerichtsbarkeit
  - **Positivistischer Rechtsbegriff**
- Gegenspieler von Carl Schmitt

  Souverän ist, wer über den Ausnahmezustand entscheidet

  im Staatsrecht

re:publica

Digitale Souveränität

- Komplexität im Quadrat
  - Digital
  - Juristisch
- Unklare Definition
- Auch brauchbar

  Digitale Souveränität" beschreibt „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.

  CIO Bund

- Gegensätze
  - privat
  - Staat
  - EU
  - Bund
  - Länder
  - Kommunen
  - Merkel: "Ausspähen unter Freunden geht gar nicht" Süddeutsche Zeitung Oktober 2013
  - **Digitale Gewalt ist häufig Teil von (Ex)Partnerschaftsgewalt, Stalking und Trennung** LAG Autonomer Frauenhäuser Schleswig-Holstein über Digitale Gewalt
  - Cloud Act
  - Schrems I, II, III, IV ...

Meine Definitionen im Sinne von Hans Kelsen

Souveränität

Digital souverän ist,
wer über den Zugriff
auf Daten entscheidet

Minderheitenschutz

Höchster Wert der *Digitalen* Demokratie
ist der Schutz der
***sensitivsten Daten* von Minderheiten**

re:publica

Medizinische Daten im AI Datensatz

Aktuelle Gefahren

- Chat Kontrolle
  - Netzpolitik: Überwachungsmonster
  - bricht auch Sicherheit in Industrie und Verwaltung
- Steuer ID, Bund ID
- Zentrale Elektronische Patientenakten
- Herumgecyber ohne Strategie
- Sinnlose Leuchtturm-Projekte

Wieso sinnlose Leuchturmprojekte?

- Wer erinnert sich noch an DE-Mail?
- beA - Stümperei mit dem besonderen elektronischen Anwaltspostfach
- eID Fiasko: Stellungnahme des CCC
- sprich niemals jemand in der Verwaltung auf die Bundesdruckerei an
- Digitaler Führerschein
- Frag den Staat zur Hotelbuchung BMI ID Wallet
- SSI Desaster
  Anhörung über Digitale Identitäten im Bundestag
- Werte, so wichtig: Sensitivste Daten von Geflüchteten...
  BAMF gewinnt eGovernment-Preis mit Blockchain-...
  So wurde man CIO Bund: *Trotz dieser Bedenken will Markus Richter die Blockchain für das BAMF nutzen.*
- Subvention für die Auto Industrie in Gaia-X: Catena-X

Mit freundlicher Genehmigung von Ralph Ruthe

re:publica

Widersprüche

- Bundesmessenger BUM

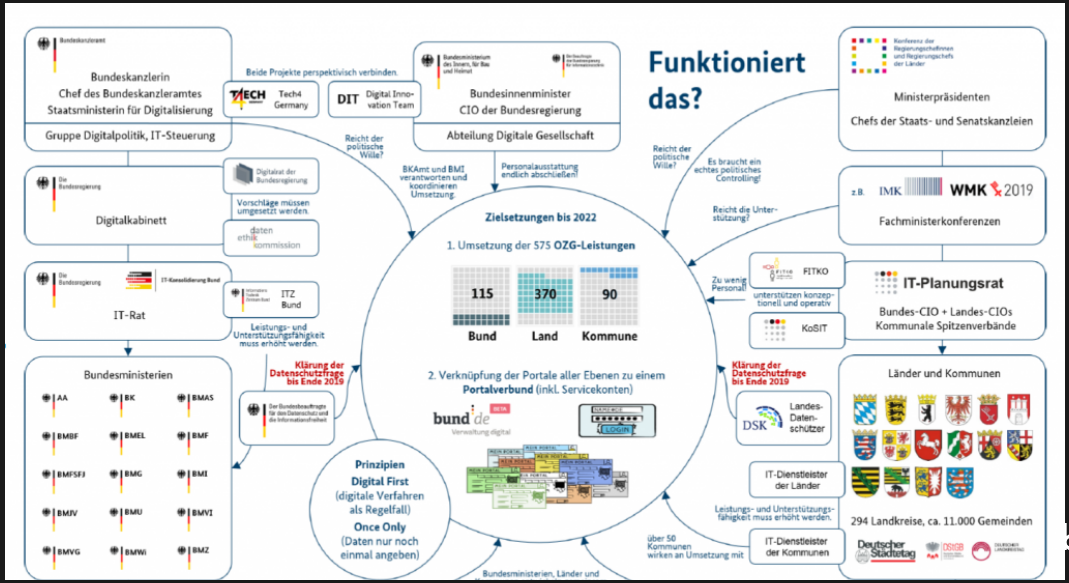
  Matrix + Erweiterungen

- Förderungen
  - TOR durch NSA
  - Sovereign Tech Fund fördert
    - VPN Wireguard
    - Ende zu Ende Verschlüsselung OpenMLS

- EU Once Only
  - braucht keine zentrale ID
  - grenzüberschreitend

re:publica

Online Zugangsgesetz



IT Planungsrat

17 Mitglieder + Berater

- Staatsekretär:innen
- Minister:innen
- Lebensläufe
  - Jurist:innen 7
  - Verwaltung 1
  - Politologie 1
  - Kaufmann, BWL 3
  - Humanmedizin 1
  - Volkswirt 2
  - Kriminologe 1
  - Chemiker 1

IT 0

IT - Planungsrat Gruppenfoto Hamburg

- Beschlüsse dreimal im Jahr
- dazwischen Umlaufverfahren

Online Zugangsgesetz

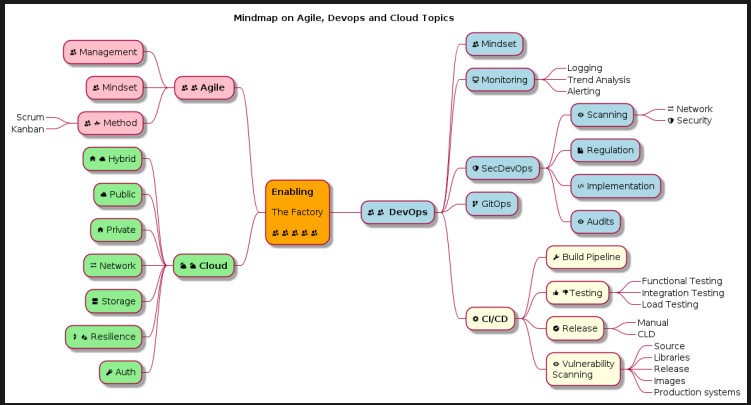
- größter Change Prozess
- sensibelste Daten
- ohne Kenntnisse von Change Prozessen
- ohne Cloud Strategie
- *Wenn sie einen Scheißprozess digitalisieren, dann haben sie einen scheiß digitalen Prozess* von Thorsten Dirks, 2015

re:publica

Softwarefactory

- Agilität
- Cloud Infrastruktur
- Entwicklung, Sicherheit und Betrieb
- Vollautomatisierung CI/CD Pipeline

SecDevOps: Secure Development and Operations
Sichere Entwicklung und Betrieb



software factory mindmap

re:publica

Widerstände

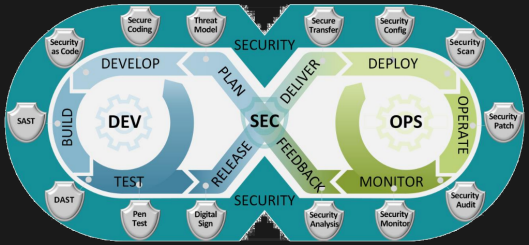
- alles wird umgebaut
  - Change Process
  - neuere Ansätze: Neuroleadership
- irrationales Verhalten
  - Flucht
  - Angriff
  - Schockstarre
- SCARF
  - Status
  - Certainty
  - Autonomy
  - Relatedness
  - Fairness
- bestehende Geschäftsinteressen
  - Platzhirsche
  - Hyperscaler
- Restruktierung der gesamten Organisation
- 2-5 Jahre

re:publica

SecDevOps

Cloud Native Computing Foundation and US Department of Defense

- DevOps mit Security von Anfang an: **DevSecOps**
- Alle Prozesse umstellen
- Vorlage vom US Verteidigungsministerium (DoD)



The main characteristic of DevSecOps is to improve customer outcomes and mission value by automating, monitoring, and applying security at all phases of the software lifecycle: plan, develop, build, test, release, deliver, deploy, operate, and monitor.

This leads to a change to the organizational culture, along with the development of new collaborative processes, technologies and tools to automate the process and to apply consistent governance. A project must advance in all four areas to be successful.

re:publica

Historie

- Für SuSE im Bundestag 2001:

  Computerwoche Halbherziger Wunsch der Politik nach Linux

- Marktanalyse von PwC Strategy 2019

  Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern

- Architekturrichtlinie für die IT des Bundes 2022
- Ehrenamtliche Mitarbeit des Sprechers
  - Juni 2020 "Ein Ort für öffentlichen Code" – OpenCode
  - gelegentliche Beiträge zur AG Cloud 2021

    Deutsche Verwaltungscloud-Strategie: Rahmenwerk der Zielarchitektur
- Gegen $$ Cash

  Sovereign Tech Fund, Souveräner Arbeitsplatz (Teilzeit, freiberuflich)

re:publica

Open Source wird bindend

- Deutsche Verwaltungscloud-Strategie: Rahmenwerk der Zielarchitektur und zahlreiche weitere Dokumente
- opencode.de verlangt OSI Lizenzen
- Wichtige Projekte wie z.B. der Bundesmessenger sind auf OpenCode
- Souvereign Tech Fund sehr aktiv für Infrastruktur Projekte
- Prototype Fund schiebt Projekte an
- Zendis ist ein Open Source Program Office OSPO
- Gematik baut auch ein OSPO auf!

re:publica

Clouds

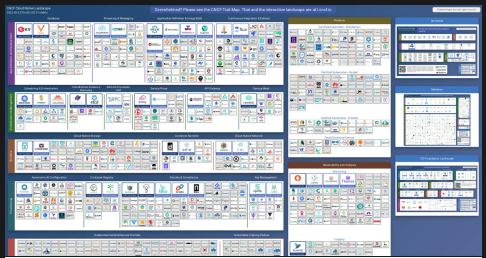
- Moderne Software Entwicklung- und Betrieb
- Cloud $\neq$ Hyperscaler Cloud
- Private Clouds
- Kubernetes
- Microservices
- Skalierung
- Lose gekoppelte Dienste
- Hosting in DE
- DVS-007-R1 schließt Hyper Scaler nicht aus

DVS-007-R1 Hoheit über Krypto-Module und Schlüssel MUSS

Die Kryptomodule / Schlüssel müssen in Hoheit der ÖV sein, um den Zugriff auf die gespeicherten Daten selbstbestimmt zu kontrollieren.
Technologien zur Verschlüsselung müssen durch die Cloud-Standorte anpassbar sein, um jederzeit die Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) umsetzen zu können.

Cloud Native Strategy

- Kubernetes
- aus dem Borg Projekt von Google
- Cloud Native Computing Foundation CNCF
  Unterorganisation der Linux Foundation
  1,191 cards with a total of
  3,728,182 stars,
  market cap of $21.5T (Billionen)
  and funding of $53.4B.
  (Milliarden Faktor 6 ist der Unternehmenswert)
- Configuration as Code – GitOps
  Konfigurationen kommen immer aus Repositories
  - Eingebautes Network
    Das Netzwerk ist auch nur eine Konfiguration.
  - Automatisierung eingebaut
- Edge Computing (Neuralink)
  Dein Computer ist nur ein Edge Device meiner Cloud. Widerstand ist zwecklos



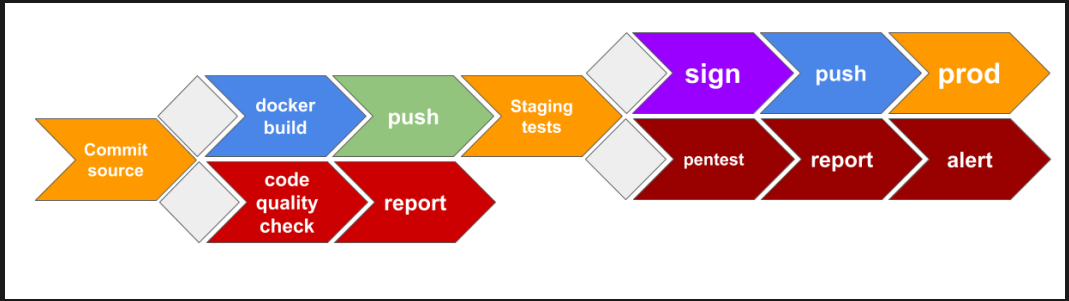
re:publica

Cloud Kompetenz?

- Sovereign Cloud Stack Summit
  - Hochschule Osnabrück
    - Campus Netz
    - Rechenzentrum im Container
      Katastrophenschutz
      Verteilter Einsatz
- Open Source Kubernetes Hersteller
  - Edgeless Systems
  - Kubermatic
- Viele Angebote für Betrieb
- GovDigital Gemeinsame leistungsfähige Cloud-Infrastruktur
  viele Anstalten des Öffentlichen Rechts
- Mehr Komplexität: Energiewende
  Rechenzentrum ohne Verluste
  - Erneuerbare Energie
  - Rechnen in Cloud
  - Nahwärme

  von JH-Computers und OSISM

Automatisierung in einer Deployment Pipeline



Deployment Pipeline – with Security

Was fehlt?

Technisch: BSI hat keine

- Cloud Strategie
  Grundschutz ist vorhanden
  reicht aber nicht
  SYS 1.6 Containerisierung,
  APP 4.4 Kubernetes
- Supply Chain Strategie
  ein paar Dutzend Bausteine
  und Technische Richtlinien
- Sicherheit von Deployment Pipelines
- Signatur Richtlinien für Container
- Verwaltungs
  ACME RFC 8555 Let's Encrypt

BTW: Cash€: Bitkom, August 2022

203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen

---

Unbezahlbar und kostet fast nichts:

Engagement der Zivilgesellschaft

re:publica

Beteiligungspyramide Zivilgesellschaft

re:publica

Fazit

- Open Source wird Standard
- in seiner Cloud Form
- Es gibt Fortschritt aber zu langsam
- Anfänge sind gemacht
- Übergang dauert mindestens 5 Jahre, eher 10+ Jahre
- Das ist zu langsam für das OZG
- Zu wenig technische Kompetenz in der Verwaltung
- Leuchtturmprojekte (*Wunderwaffen*) – vernebeln das Bild

  Blockchain, eID, KI
- BSI hat große Baustellen (Cloud, Supply Chain Security)
- Dialog mit Zivilgesellschaft hat begonnen!

re:publica

Fragen, Kritik, Anregungen?

Ein paar Antworten:

Buntes Bug Bounty

Mail: republica@thomasfricke.de

LinkedIn

Mastodon: @thomasfricke@chaos.social

Foss Security Campus, Berlin September 26-29th

re:publica