Digitale Nachhaltigkeit

Steffen Ullrich

2. Juni 2022

Digitale Nachhaltigkeit

- Souveränität
- Beherrschbarkeit
- Robustheit
- Sicherheit
- Zukunftsfähigkeit

- Was bedeutet der Begriff
- Was sind die Aspekte
- Wo können wir (genua) beitragen

Steffen Ullrich
Technologie Fellow IT-Sicherheit
Produktentwicklung, Forschung, Strategie

steffen_ullrich@genua.de

Digitale Nachhaltigkeit

- Souveränität
- Beherrschbarkeit
- Robustheit
- Sicherheit
- Zukunftsfähigkeit

- Was bedeutet der Begriff
- Was sind die Aspekte
- Wo können wir (genua) beitragen

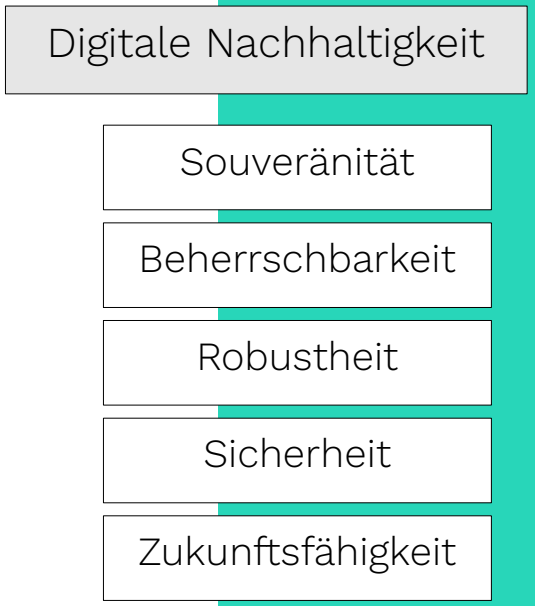
Digitale Nachhaltigkeit

Nachhaltigkeit

- im engeren Sinn:
  Ökologie, Grün, sparsamer Ressourceneinsatz, Umweltverträglichkeit …
- im weiteren Sinn:
  so agieren, dass wir uns auch in Zukunft wohl fühlen

Digitale Nachhaltigkeit

- Chancen der Digitalisierung langfristig nutzen
  Effizienz, Flexibilität, Bestehen im Wettbewerb, …
- Risiken und Nebenwirkungen langfristig beherrschen*
  *beherrschen ist nicht zwingend eliminieren



Warum überhaupt Digitalisierung

Digitalisierung für mehr **Flexibilität**

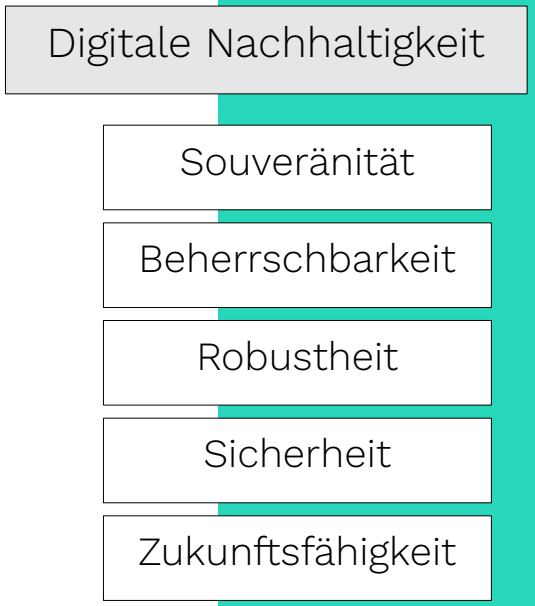
- passender auf vielfältige Bedürfnisse eingehen

Digitalisierung für höhere **Effizienz**

- schneller auf Bedürfnisse eingehen
- mit weniger Eigenaufwand

Relevant aus wirtschaftlicher und politischer Sicht

- Bestehen in einem kompetitiven dynamischen internationalen Markt
- mit wirtschaftlicher **Stärke**
- und davon abgeleitet politischer Stärke



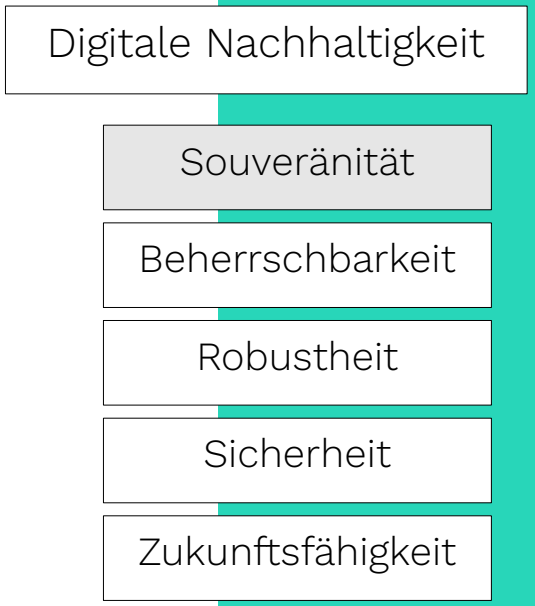
Souverän die Zukunft gestalten

Zukunft selbstbestimmt gestalten bedeutet **souverän** agieren zu können

- keine Abhängigkeiten, die die Handlungsfähigkeit signifikant einschränken

Technologien sind **verfügbar** und **kontrollierbar**
Software, Hardware, Infrastrukturen, Kompetenzen, Rohstoffe, ...

- keiner kann mir die Nutzung einschränken oder verbieten
  explizite Verknappung
- keiner kann mich an Weiterentwickung oder Anpassung hindern
  Lizenzen, Patente, ...
- sie stehen in ausreichender Menge zur Verfügung
  implizite Verknappung
- sie stehen in ausreichender Qualität zur Verfügung
  Nutzbar ohne Schaden an Safety, Verfügbarkeit, Vertraulichkeit, Zuverlässigkeit

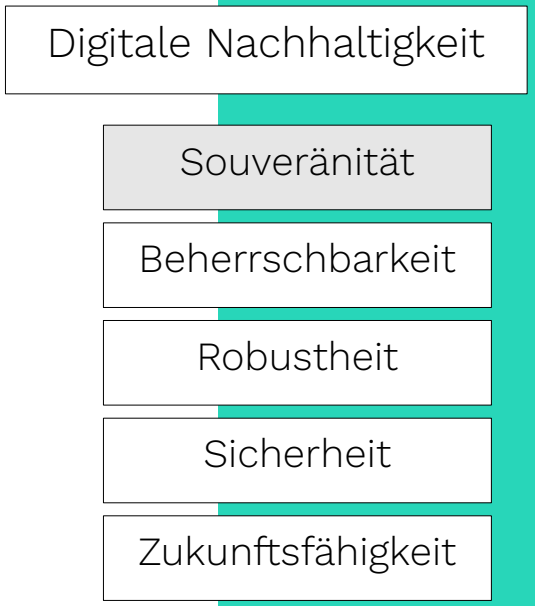


Souveränität ist nicht Autarkie

Volle Kontrolle würde Autarkie bedeuten, aber

- die heutige Welt ist zu komplex um alles zu können
- nur die eigenen Technologien und Fähigkeiten zu nutzen ist ein Wettbewerbsnachteil, wirtschaftlich wie politisch

Alternative zur Autarkie sind beherrschbare Abhängigkeiten



Souverän durch beherrschbare Abhängigkeiten

Vertrauen

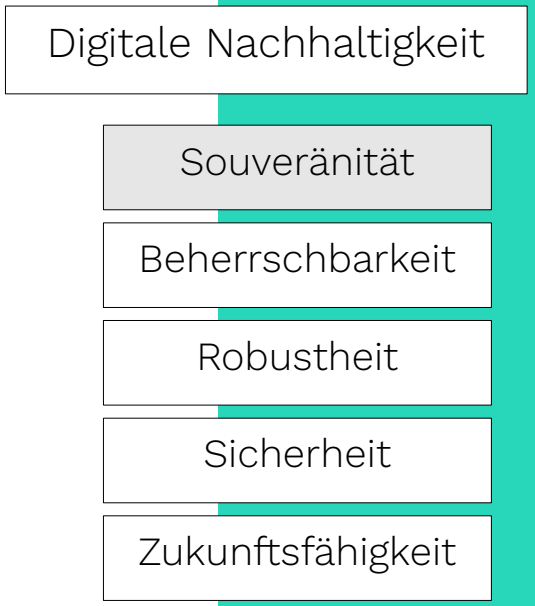
- gleiche bzw. zueinander passende Werte, gemeinsame Interessen, keine störende Konkurrenz
- abgestuftes Vertrauen: Deutschland, EU, "westliche Welt", ...

Verträge

- robuster gegen Änderungen des Umfelds, sofern starkes Rechtssystem
- je stärker Staaten und Firmen, destso besser die Verhandlungsposition

Vertrauen und Verträge haben Grenzen

- inner- und zwischenstaatliche **Konflikte** schädigen Vertrauen und Verträge
- Restrisiken bleiben und müssen akzeptiert oder mitigiert werden



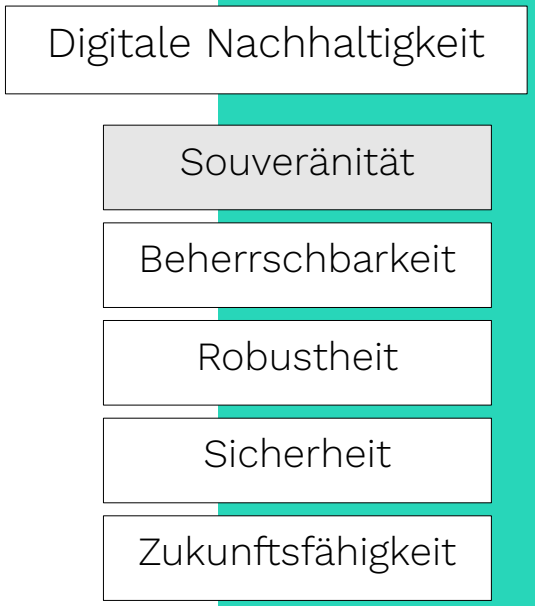
Souverän durch beherrschbare Abhängigkeiten

Gegenseitige Abhängigkeiten als Motor gemeinsamer Interessen

- (fragiles) Gleichgewicht der Abhängigkeiten
  wo jede Seite versucht ist, die Abhängigkeit zu verringern

Kritikalität von Abhängigkeiten verringern

- mehrere Provider mit unterschiedlichen Interessen,
  um Risiko gleichzeitiger Ausfälle zu vermeiden
- Rückfallpläne mit notfalls schlechteren Alternativen,
  um nicht komplett ausgeliefert zu sein



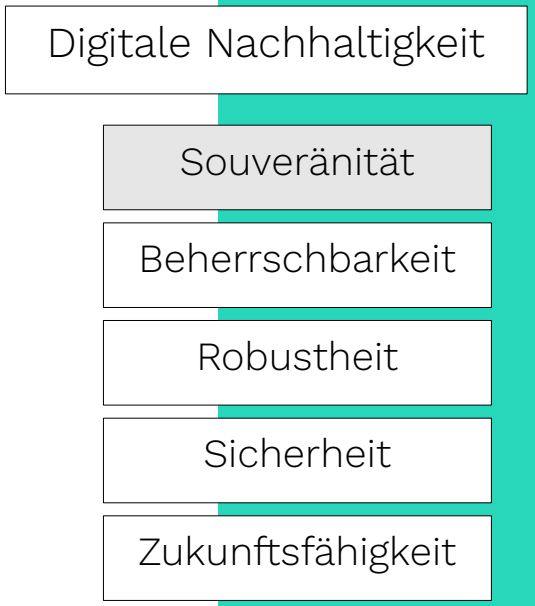
Souverän durch vermeidbare Abhängigkeiten

Eigene Kompetenzen auf- und ausbauen

- vorrangig an kritischen Stellen: Schlüsseltechnologien
- Aufbau von Kompetenzen, Forschungsprojekte
- Industrieansiedelungen

Open Source und Standards

- nicht zwingend sicherer
- aber auf jeden Fall kontrollierbarer: Zugriff, Anpassbarkeit, ...

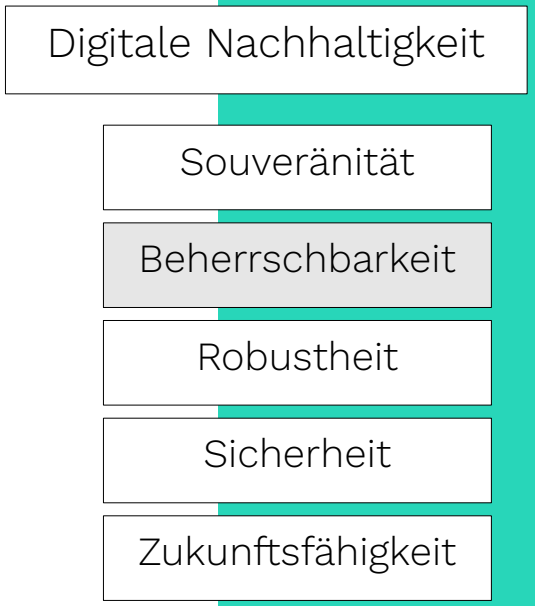


Digitale Technologien beherrschen

Zunehmende Digitalisierung führt zu steigender Komplexität bei gleichzeitig höheren Anforderungen an Verfügbarkeit, Zuverlässigkeit und Vertraulichkeit.

Diese technologischen Herausforderungen gilt es zu beherrschen

- Richtige Balance zwischen einerseits Flexibilität und Leistungsumfang und andererseits Komplexität und Qualität finden
- Limitierten Einfluß auf technische Abhängigkeiten berücksichtigen: Softwarekomponenten, Hardware, Dienstleister, XaaS, ...
- Ausreichend Ressourcen (Zeit, Geld, Leute) und Kompetenzen bereitstellen
- Absichern gegen Angriffe (Cyber-Sicherheit) und unerwartete Situationen (Robustheit)

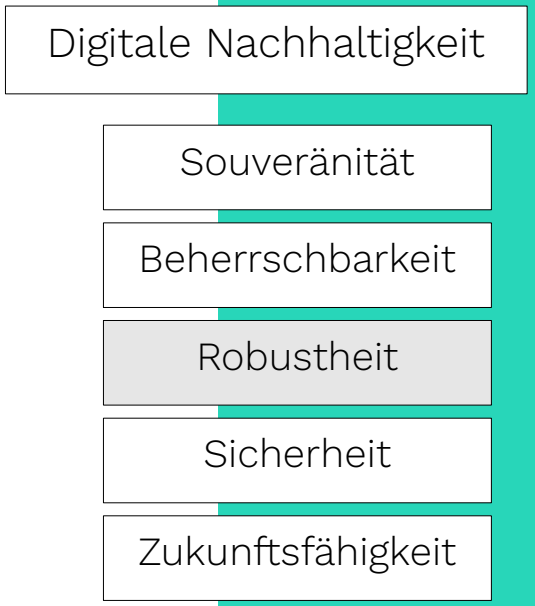


Robuste, stabile Digitalisierung

Aufrechterhaltung der wesentlichen Prozesse auch in unerwarteten Situationen

- Robustheit und Fehlertoleranz per Design
  Unerwartetes einplanen, Gefahrenmodellierung, Redundanz, Notbetrieb, ...
- Richtige Balance zwischen Effizienz und Robustheit finden
  Leistungsfähigkeit der Lieferkette, Verfügbarkeit Personal, ...
- eingeschränkte aber ausreichende Funktionalität auch bei Problemen
  Stromausfall, Internetausfall, Denial of Service, Sicherheitslücken, Angriffe, Lieferprobleme, Pandemien, Sanktionen ...

Cyber-Sicherheit als wichtiger Faktor einer robusten Digitalisierung



Digitalisierung absichern gegen Vielfalt von Bedrohungen

Angriffe auf die Verfügbarkeit

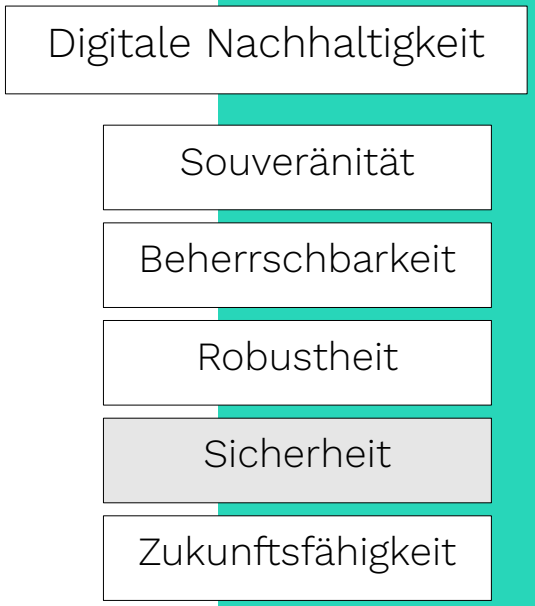
- Temporäre Störungen durch Denial Of Service
- Daten als Geiseln nehmen mit Ransomware
- Sabotage

Angriffe auf Vertraulichkeit

- Wirtschafts- und Industriespionage
- interne Daten veröffentlichen im Kontext Ransomware

Angriffe auf Integrität

- Identitätsmissbrauch
- Sabotage



Digitalisierung absichern

Robuste Sicherheit bereitstellen

- Kombination proaktiver und reaktiver Methoden für Defense in Depth
  Schadensvermeidung und Schadensbegrenzung
- proaktiv: Zugriffskontrolle und Analyse auf mehreren Ebenen
  Netzperimeter, Mikrosegment, Anwendung, ...
- reaktiv: Angriffserkennung, Anomalieerkennung,
  automatisierte Reaktionen, ...

Eigene Angebote dürfen selber nicht zum Sicherheitsproblem werden

- Security und Robustheit im Software-Design
  Sandboxen, Selbstbeschränkung von Anwendungen, ...
- und in Entwicklungsprozessen
  Peer Reviews, automatisierte Tests, gründliche Qualitätskontrolle ...
- unabhängige Kontrollen:
  Zertifizierungen, Zulassungen, Penetration Testing, ...

Digitale Nachhaltigkeit

- Souveränität
- Beherrschbarkeit
- Robustheit
- **Sicherheit**
- Zukunftsfähigkeit

Zukunft verstehen und mitgestalten
Schritt halten mit sich ändernden Bedürfnissen

Steigende Komplexität und Kritikalität benötigen …

- Weiter- und Neuentwicklung von Konzepten und Technologien
- um auch in Zukunft Digitalisierung robust und sicher zu beherrschen

Unsere Schwerpunkte für die Zukunft

- Zero Trust Networking und Automatisierung für einfache, skalierbare und granulare Absicherung komplexer verteilter Infrastrukturen
- KI nutzbar machen zum Beherrschen von Komplexität und zur Abwehr neuartiger Angriffe
- Mit Post-Quantum-Kryptographie Vertraulichkeit auch in Zukunft bereitstellen