

Digitale Souveränität

Mehr Resilienz, Kontrolle und Compliance

Kevin Nicholls

24. Juni 2026 | IT4B Digital Summit | Lübeck

- Ausbildung zum Informatik-Kaufmann
- Über 10 Jahre Berater für Datenschutz
 - Betreuung von ca. 40 Kunden
 - Von KMU über Konzerne bis zu Behörden
- Zertifizierter Datenschutzbeauftragter
- Coach für KI-Kompetenz



Datenschutz

Externe Datenschutzbeauftragung, Audits, E-Learning, Dienstleister-Auditierung etc.



Informationssicherheit

Aufbau eines ISMS bis zur Zertifizierung, Informationssicherheitsbeauftragter etc.



Compliance & Strategie

Beratungsleistungen zu Compliance- sowie bei konzeptionellen und strategischen Fragestellungen



Digitale Souveränität



Digitale Souveränität

Digitale Souveränität beschreibt die Fähigkeit eines Unternehmens, seine digitalen Systeme, Daten, Prozesse und Abhängigkeiten **selbstbestimmt, kontrolliert** und **resilient** zu gestalten und zu betreiben.

- **Kontrolle** über Daten, IT-Systeme und Entscheidungsprozesse
- **Unabhängigkeit** von einzelnen Anbietern, Staaten oder Technologien
- **Transparenz** über technische und rechtliche Rahmenbedingungen
- **Handlungsfähigkeit** auch bei Störungen, Ausfällen oder geopolitischen Veränderungen

Herausforderungen

- Cloud- und Plattformabhängigkeiten
- Regulatorische Anforderungen (DSGVO, NIS2, DORA, AI Act)
- Cyberangriffen
- Lieferkettenrisiken/-angriffe
- Schutz von Geschäfts- und Betriebsgeheimnissen sowie sensiblen Daten
- Geopolitische Risiken (Sanktionen, Exportkontrollen, extraterritoriale Gesetze)

- Unklarer Datenzugriff durch Drittstaaten (z. B. CLOUD Act)
- Anbieterabhängigkeit (Vendor Lock-in)
- Black-Box-Services ohne ausreichende Kontrollmöglichkeiten (insbesondere bei KI-Diensten und Cloud-Architektur)
- Cybersecurity & Resilienz
 - » Abhängigkeit von externen Sicherheitsdiensten
 - » Unzureichende Reaktionsfähigkeit bei Angriffen
 - » Mangelnde Transparenz über Sicherheitsmaßnahmen von Dienstleistern
- Recht & Compliance
- Geopolitische Einflüsse

Thema ist nicht neu, erfährt aber durch Trump & Co aktuell eine Renaissance

CLOUD Act)

ollmöglichkeiten
hitektur)

men von Dienstleistern

<https://www.heise.de/news/Wie-ein-franzoesischer-Richter-von-den-USA-digital-abgeklemmt-wurde-11087453.html>



Status-Quo-Erhebung und Risikobewertung

- **Wo** liegen unsere sensibelsten Daten und **wer** hat Zugriff?
- **Welche** (kritischen) Geschäftsprozesse hängen von einzelnen Anbietern ab?
- **Wie** können wir zentrale Systeme realistisch wechseln / zurückholen?
- **Was** tun wir, falls ein Anbieter ausfällt oder wegbricht (Notfallpläne)?

Sind rechtliche, technische und organisatorische Aspekte **abgestimmt**?

Digitale Souveränität bedeutet nicht vollständige Autarkie.

Entscheidend ist nicht, jede externe Abhängigkeit zu vermeiden, sondern sie bewusst zu steuern.

Ziel ist ein tragfähiges Gleichgewicht zwischen **Nutzen** externer Dienste und Wahrung eigener **Kontrolle**.

- Abhängigkeiten können große Risiken verursachen
- Ursachen hierfür sind vielfältig
- Ziel ist nicht die Autarkie, sondern ein risikobewusstes Steuern von externen Diensten und Anbietern



Fragen?

UIMC

Mancher ertrinkt lieber,
als daß er um Hilfe ruft.

– *Wilhelm Busch*

knicholls@uimc.de