

## Digitale Souveränität – was bedeutet sie wirklich auf technischer Ebene?

Kaum ein Begriff prägt die aktuelle Digitalisierungsdebatte so stark wie die „Digitale Souveränität“. Im Kontext von Cloud-Strategien, Hyperscaler-Abhängigkeiten, europäischen Plattforminitiativen oder föderalen Cloud-Ansätzen ist er allgegenwärtig. Zugleich bleibt er häufig unscharf. Während politische Programme und Strategiepapiere Souveränität als Leitprinzip formulieren, stellt sich in der technischen Umsetzung eine viel konkretere Frage: Woran lässt sich digitale Souveränität tatsächlich messen – und wo sind ihre Grenzen?

Zunächst ist eine unbequeme, aber notwendige Feststellung zu treffen: Hundertprozentige digitale Souveränität existiert nicht.

Digitale Systeme basieren auf globalen Lieferketten, internationalen Standards, Open-Source-Komponenten und hochspezialisierten Plattformen. Hardware stammt aus weltweiten Produktionsnetzwerken, Softwarebibliotheken werden gemeinschaftlich entwickelt, selbst kryptografische Standards entstehen in internationalen Gremien. Vollständige Autarkie wäre technisch kaum realisierbar und wirtschaftlich kaum vertretbar.

Digitale Souveränität kann daher nie völlige Unabhängigkeit bedeuten. Sie bedeutet vielmehr: bewusst gestaltete, kontrollierbare Abhängigkeit.

Damit verschiebt sich die Diskussion von einer ideologischen hin zu einer architektonischen Perspektive. Digitale Souveränität ist kein Produkt, kein Cloud-Label und kein Marketingversprechen. Sie ist eine Eigenschaft von Architekturentscheidungen – über den gesamten Lebenszyklus eines Systems hinweg.

In der öffentlichen Debatte wird Souveränität häufig mit Infrastruktur gleichgesetzt. Rechenzentren innerhalb der EU, nationale Anbieter oder sogenannte „Sovereign Clouds“ gelten als Ausdruck technischer Unabhängigkeit. Diese Aspekte sind nicht irrelevant. Jurisdiktion, regulatorische Einbettung und physische Zugriffsmöglichkeiten spielen insbesondere im öffentlichen Sektor eine zentrale Rolle. Doch sie beantworten nur einen Teil der Frage. Ein System kann in einem europäischen Rechenzentrum betrieben werden und dennoch strukturell abhängig sein – etwa von proprietären Plattformdiensten, nicht portablen Datenmodellen oder exklusivem Betriebs-Know-how.

**Standort schafft juristische Nähe, aber noch keine technische Autonomie.**

Um digitale Souveränität greifbar zu machen, lohnt sich ein differenzierter Blick auf mehrere Ebenen. Die erste ist die Infrastruktur-Souveränität. Sie umfasst Standortkontrolle, regulatorische Absicherung und technische Isolation. Diese Dimension ist sichtbar und vergleichsweise klar beschreibbar. Gleichzeitig ist sie – entgegen

der öffentlichen Wahrnehmung – häufig die am leichtesten veränderbare. Infrastruktur kann migriert werden, sofern Anwendungen und Daten darauf vorbereitet sind.

Die zweite Ebene ist deutlich anspruchsvoller: Plattform-Souveränität. Hier entstehen die eigentlichen Lock-in-Effekte moderner IT-Landschaften. Abhängigkeiten ergeben sich nicht primär aus virtuellen Maschinen, sondern aus Platforddiensten: Datenbankservices mit proprietären Schnittstellen, Identity- und Access-Management-Lösungen, Messaging-Systeme, Analytics- oder KI-Services. Containerisierung allein schafft noch keine Portabilität, wenn Anwendungen tief in spezifische Service-Ökosysteme integriert sind. Ein Kubernetes-Cluster ist technisch transportabel. Eine Anwendung, die auf mehrere proprietäre APIs angewiesen ist, ist es nicht.

#### **Der Lock-in der Zukunft ist ein API-Lock-in.**

Doch auch hier gilt: Absolute Austauschbarkeit ist eine Illusion. Jede Plattformscheidung erzeugt Abhängigkeiten. Die Frage ist nicht, ob Abhängigkeiten entstehen – sondern ob sie transparent, vertraglich gestaltbar und technisch beherrschbar sind. Souveränität bedeutet daher nicht „keine Bindung“, sondern „Bindung mit Exit-Option“.

Noch fundamentaler ist die Datenebene. Digitale Handlungsfähigkeit basiert letztlich auf der Kontrolle über Datenmodelle, Semantik und Schnittstellen. Exportierbare Daten allein genügen

nicht, wenn ihre Struktur nur innerhalb eines bestimmten Systems sinnvoll interpretierbar ist. Souveränität bedeutet daher, Daten technologieunabhängig zu modellieren, Schnittstellen standardisiert zu definieren und Migrationspfade realistisch zu kalkulieren. Wer sein Datenmodell nicht kontrolliert, kontrolliert auch nicht seine digitale Zukunft.

Gerade in föderalen Strukturen gewinnt diese Dimension an Bedeutung. Wenn Register oder Fachverfahren jeweils eigene proprietäre Datenlogiken etablieren, entsteht langfristig eine fragmentierte Landschaft, in der Interoperabilität nur mit erheblichem Integrationsaufwand möglich ist. Souveränität im Verbund erfordert daher abgestimmte Standards und gemeinsame Governance – nicht maximale technische Vielfalt.

Eine häufig unterschätzte Dimension ist die Betriebs-Souveränität. Selbst die portabelste Architektur bleibt theoretisch, wenn das erforderliche Know-how ausschließlich extern gebunden ist. Digitale Souveränität setzt eigenes Architekturverständnis, Cloud- und Plattformkompetenz sowie die Fähigkeit voraus, Exit-Szenarien realistisch zu bewerten. Viele Exit-Strategien existieren als Vertragsklausel oder Präsentationsfolie. Technisch durchgespielt oder organisatorisch vorbereitet wurden sie jedoch selten.

#### **Eine Exit-Strategie ist kein Dokument, sondern eine Fähigkeit.**

Sie beantwortet konkrete Fragen: Wie lange dauert eine Migration? Welche Datenmengen sind betroffen? Welche Services



müssten ersetzt werden? Welche Kompetenzen stehen intern zur Verfügung? Ohne belastbare Antworten bleibt Souveränität ein theoretisches Konstrukt.

Vor diesem Hintergrund erscheint auch die häufig propagierte Multi-Cloud-Strategie in einem differenzierteren Licht. Mehrere Anbieter parallel zu nutzen, reduziert nicht automatisch Abhängigkeiten. Vielmehr steigen Komplexität, Governance-Aufwand und Skill-Anforderungen. Technische Souveränität entsteht nicht durch die Anzahl der Provider, sondern durch die Qualität der Architektur. Eine standardisierte Plattform mit klar definierten Schnittstellen kann souveräner sein als eine unkoordinierte Multi-Cloud-Landschaft, die mehrere parallele Bindungen erzeugt.

Digitale Souveränität ist daher kein Zustand, der vollständig erreicht werden kann. Sie ist ein kontinuierlicher Gestaltungsprozess. Jede technologische Entscheidung verschiebt das Gleichgewicht zwischen Effizienz, Innovationsfähigkeit und Abhängigkeit. Absolute Autarkie wäre weder realistisch noch wünschenswert. Moderne digitale Wertschöpfung basiert gerade auf Vernetzung und Spezialisierung.

**Die entscheidende Frage lautet deshalb nicht: Sind wir vollkommen unabhängig?**

Sondern: Haben wir unsere Abhängigkeiten verstanden, gestaltet und – wenn nötig – die Fähigkeit, sie zu verändern?

Souveränität zeigt sich nicht in der Abwesenheit von Bindungen, sondern in der Fähigkeit zur selbstbestimmten Anpassung. Sie entscheidet sich nicht allein im Rechenzentrum

und nicht im Cloud-Label. Sie entscheidet sich im Architekturboard, in Datenmodellen, in Plattformstrategien und im Kompetenzaufbau.

Erst wenn Organisationen technisch belastbar beantworten können, dass sie ihre digitalen Strukturen im Bedarfsfall eigenständig weiterentwickeln oder neu ausrichten können, wird aus dem politischen Leitbegriff digitale Souveränität eine operative Realität – wissend, dass sie niemals absolut, aber sehr wohl strategisch gestaltbar ist.

Digitale Souveränität bedeutet nicht, keine Abhängigkeiten zu haben – sondern sie zu verstehen, zu gestalten und im Bedarfsfall verändern zu können.



AUTOR:  
Nils-Alexander Fleischer,  
Abteilungsleiter Public Sector, msg

## IMPRESSUM

### **Herausgeber**

msg systems ag  
Robert-Bürkle-Straße 1  
85737 Ismaning/München  
Deutschland

### **Redaktionsleitung:**

Lennard Munschke  
msg systems ag  
Rummelsburger Seeblick 1, 10317 Berlin  
Mobil: +49 1734685830  
E-Mail: public-affairs@msg.group

### **Verantwortlich:**

Dr. Jürgen Zehetmaier (Vorsitzender),  
Michael Rasch,  
Karsten Redenius,  
Dr. Frank Schlottmann  
Aufsichtsratsvorsitzender: Johann Zehetmaier