

Digitale Souveränität in Deutschland

Rechenzentren zwischen Anspruch und Realität

Go

Sovereign!

BTC



Digitale Souveränität ist längst kein theoretisches Leitbild mehr, sondern ein zentraler Faktor in Architektur- und Beschaffungsentscheidungen. Geopolitische Spannungen, extraterritoriale Zugriffsgesetze und der Wunsch nach nachweisbarer Datenkontrolle haben das Thema aus Strategiepapieren in operative Entscheidungsräume geholt.

Lokale Rechenzentren und globale Cloud-Lösungen markieren dabei nur zwei Pole des Spektrums. Dazwischen wachsen hybride und regionale Modelle: Gartner zufolge planen 61 Prozent der IT-Führungskräfte in Westeuropa, künftig stärker auf solche regionalen oder lokalen Cloud-Anbieter zu setzen. Dass alle EU-Mitgliedsstaaten die „Declaration on European Digital Sovereignty“ unterzeichnet haben, verdeutlicht den politischen Anspruch. Doch politische Erklärungen allein schaffen noch keine Souveränität. Sie bilden den Ausgangspunkt, doch die Umsetzung entscheidet sich in Architektur, Infrastruktur und Governance.



Autoren:

Alena Mattfeldt (oben)

Senior Cloud Consultant

Norbert Rosebrock (unten)

BTC AG

www.btc-ag.com

Was digitale Souveränität im Kern meint

Gegenwärtig treffen Unternehmen auf eine Landschaft, in der sie Verfügbarkeit, Innovationsgeschwindigkeit und Compliance parallel realisieren müssen. Digitale Souveränität ist daher weniger ein Endzustand, sondern eine Fähigkeit: IT-Umgebungen so zu gestalten, dass Entscheidungen bewusst möglich sind und nicht aus fehlenden Provider-Alternativen heraus erzwungen oder gar unreflektiert umgesetzt werden.

In der Praxis lässt sich diese Fähigkeit entlang dreier Dimensionen konkretisieren:

- **Rechtsraumsouveränität**, also die Frage, ob Daten und Systeme EU-externer Jurisdiktion unterliegen.
- **Technologische Souveränität**, also ob proprietäre Lock-ins oder offene Software-Stacks mit Open-Source-Komponenten eingesetzt werden.

- **Operative Souveränität**, also ob Betrieb, Prozesse und Zugriffspfade transparent, auditierbar und mit eigenen oder kontrollierbaren Fachkräften beherrschbar sind.

Der Begriff wird im Markt breit, aber oft unscharf verwendet. Digitale Souveränität bedeutet nicht, alle Technologien selbst herstellen zu müssen. Eine vollständig autarke IT wäre angesichts global verteilter Lieferketten und proprietärer Software-Stacks weder realistisch noch wirtschaftlich erreichbar. Chips, Netzwerke oder Virtualisierungstechnologien entstehen meist international. Auch klassische On-Premises-Infrastrukturen verfügen daher häufig über externe Abhängigkeiten.

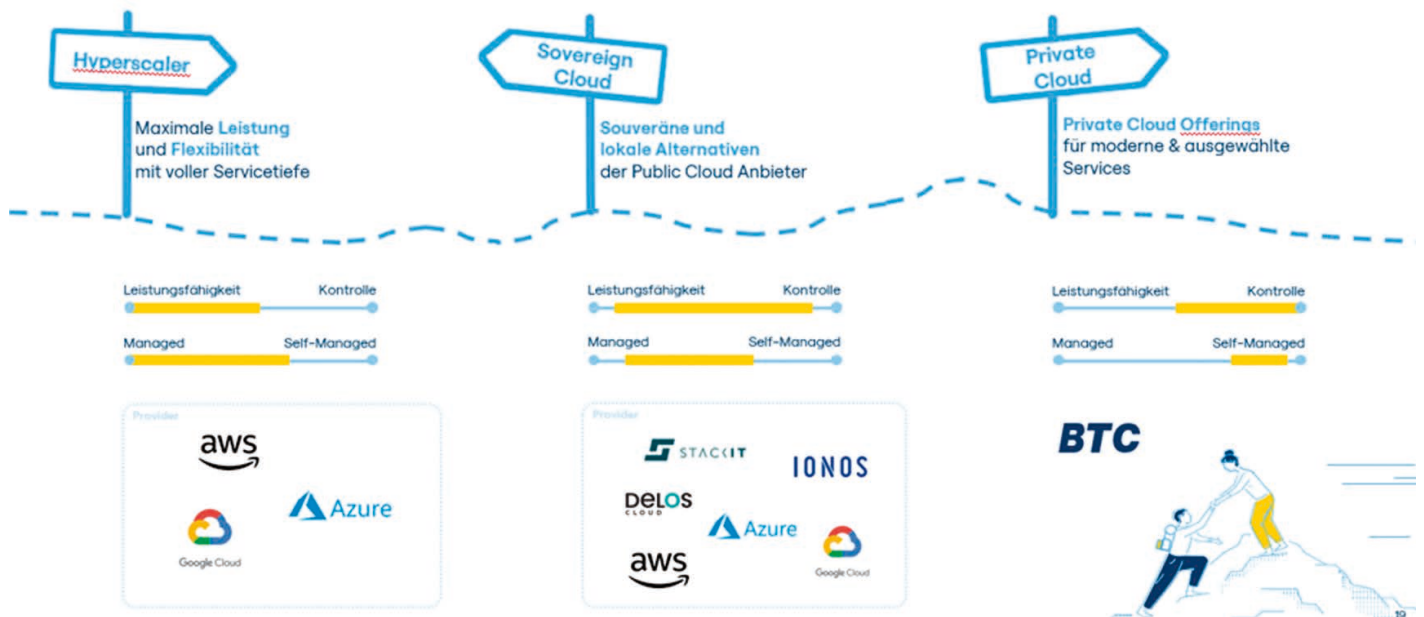
Informierte Entscheidungen treffen

Relevant ist daher nicht die Abwesenheit von Abhängigkeiten, sondern die Fähigkeit, letztere zu steuern. Ob Infrastruktur migrierbar ist, ob es niedrigschwellig möglich ist, einen Plattformwechsel von einem Hyperscaler zu einem anderen oder aus der Cloud-Welt zurück in On-Premises-Lösungen vornehmen zu können, ob Zugriffe technisch und rechtlich kontrollierbar sind und ob sich Systeme an neue regulatorische Anforderungen anpassen lassen, sind die entscheidenden Kriterien. Souveränität misst sich also nicht daran, ob eine Organisation vollkommen autark handelt, sondern daran, ob sie den Rahmen geschaffen hat, informierte Entscheidungen zu treffen. Digitale Souveränität bedeutet Wahlfreiheit, nicht Autarkie. Welche Rolle spielen in diesem Zusammenhang nun aber lokale Rechenzentren und Cloud-Lösungen?

Europäische Alternativen

Europäische Rechenzentren und souveräne Cloud-Modelle wachsen zusammen. Die europäische Cloud-Landschaft befindet sich in einer Phase des Ausbaus. Anbieter investieren in Rechenzentrumskapazitäten, adressieren Public-Sector-Anforderungen und entwickeln

Digitale Souveränität durch individuelle Provider-Auswahl



souveräne Cloud-Stacks. Große Hyperscaler reagieren ihrerseits mit Sovereign-Cloud-Segmenten. Neben den etablierten Hyperscalern treten auch immer mehr europäische Alternativen in den Blickwinkel von IT-Leitenden. Sie basieren auf offenen Standards, werden automatisiert betrieben und stellen Self-Service-Mechanismen bereit.

Ihr Fokus liegt darauf, Compute-, Storage-, Container- und Datenbankdienste sowie Netzwerk- und Connectivity-Services bereitzustellen, die ohne die im Rechenzentrum oft monatelangen Projektvorläufe nutzbar sind. Gerade bei KI- und datenintensiven Workloads sind performante Netze, Latenzen und verfügbare Bandbreiten oft der eigentliche Engpass, wie jüngste Cloud-Ausfälle gezeigt haben. Damit bieten die europäischen Plattformen einen Mittelweg zwischen Cloud Services und dem eigenen Rechenzentrum.

Herausforderungen

Viele Unternehmen stehen dabei vor der Herausforderung, die eigenen bestehende Rechenzentren beispielsweise im Energiebereich für vollständige Schwarzfallfähigkeit vorzuhalten. Regulatorische Vorgaben oder kritische Infrastrukturanforderungen erfordern oft lokale Kontrolle über Systeme und Daten. Dies bindet erhebliche Ressourcen in Betrieb und Wartung, während

gleichzeitig der Druck steigt, moderne Cloud-Prinzipien wie Automatisierung und Infrastructure as Code zu integrieren.

Verlässlichkeit

Wichtig für den Erhalt nicht nur gefühlter, sondern tatsächlicher Verlässlichkeit des eigenen Rechenzentrums ist dementsprechend, es auf dem neuesten Stand der Technik zu halten: Automatisierung ersetzt manuelle Konfiguration, Infrastructure as Code beschleunigt die Bereitstellung und reduziert Fehler. Platform Engineering und Site Reliability Engineering lösen klassische DevOps- und Ticketprozesse ab. Containerisierung stellt die Portabilität von Anwendungen sicher und macht diese leicht administrierbar. Steigende GPU-Dichten in KI-Workloads erfordern zudem effizientere Kühlkonzepte, höhere Rackleistungen und energieoptimierte Infrastrukturen.

Damit steigt nicht nur der Energiebedarf, sondern auch die sicherheitstechnische Komplexität. Hohe Packungsdichten, Spezialhardware und geteilte KI-Infrastrukturen verlangen neue Sicherheitskonzepte, die physische, logische und operative Schutzmechanismen kombinieren. Der Sicherheitsfokus verschiebt sich damit vom reinen Standort hin zur Fähigkeit, verteilte Hochleistungsumgebungen konsistent zu betreiben und abzu-

sichern. Dazu zählen Architekturen aus zentralen KI-Trainingszentren für das Modelltraining und regionalen Edge-Rechenzentren für die Modellanwendung.

Lösungen im europäischen Rechtsraum, die auf offenen Standards basieren, versuchen diesen Spagat zu adressieren. Sie zielen darauf ab, bestehende Infrastrukturen schrittweise zu modernisieren, ohne Legacy-Systeme vollständig verlagern zu müssen. Für Unternehmen bleibt die Frage, wie sie ihre bestehenden Rechenzentren wirtschaftlich betreiben und gleichzeitig in eine mehrgleisige Architekturstrategie integrieren können.

Abhängigkeiten und Partnerschaften bewusst gestalten

Digitale Souveränität wird durch die Fähigkeit erreicht, mit Anbietern und Betriebsmodellen flexibel umzugehen. Besonders wertvoll sind Anbieter, die mittels verschiedener Cloud-Services unterschiedliche Betriebsmodelle und cloud-agnostische Architekturen unterstützen und damit Szenarien ermöglichen, ohne große technische Anpassungen vorzunehmen. Cloud-agnostische Architekturen mindern Abhängigkeiten und schaffen Spielräume, was inzwischen auch Hyperscaler stärker adressieren. Entscheidend ist dabei jedoch nicht nur die technische Architektur, sondern auch

die personelle und organisatorische Fähigkeit zum Wechsel. Fehlende Cloud-, Plattform- und Betriebsexpertise kann Providerabhängigkeit ebenso verstärken wie proprietäre Technologie.

Anforderungen

Eine Providerentscheidung ist deshalb mit der richtigen Architektur kein irreversibles Commitment, sondern ein Weg, der sich mit den Anforderungen weiterentwickelt und den Unternehmen idealerweise gemeinsam mit einem Partner gehen. Wichtig ist, dass dieser Partner anbieteroffen berät, Cloud-Strategien langfristig begleitet und auch Umstellungen unterstützt, wenn Anforderungen sich ändern. Zugriffe durch Behörden, proprietäre Komponenten im Rechenzentrum oder technologische Eingriffsmöglichkeiten bleiben relevante Faktoren, die transparent diskutiert und in einer realistischen Risikoabwägung und resultierenden Szenarien betrachtet werden müssen. Welche Modelle sich dabei aktuell in der Praxis durchsetzen, zeigt ein Blick auf den Markt.

Realität im Markt – Hybridität als Normalzustand

Die Praxis zeigt ein differenziertes Bild, aber keinen eindeutigen Trend. Während Hyperscaler in den vergangenen Jahren stark nachgefragt wurden und fester Bestandteil

Fremdbestimmung

Souveränität

Autarkie

Andere entscheiden,
was wir tun

Wir haben die
Kontrolle über unser
Handeln

Wir machen alles
selbst

von Cloud- und IT-Strategien sind, werden klare Single-Cloud-Strategien aufgeweicht. Abhängig von der Kritikalität der Workloads und der Datenklassifizierung betrachten Unternehmen nun auch für ausgewählte Use Cases europäische Cloud-Alternativen und souveräne Angebote der Hyperscaler. Aber auch das lokale Rechenzentrum, idealerweise mit einer zeitgemäßen, auf Open Source basierenden Technologie, beziehen sie in die Entscheidungsfindung ein.

Unternehmen setzen unterschiedliche Schwerpunkte

Auf den Standard-Lösungen und Regionen der Hyperscaler wird weiterhin das Gros der Workloads umgesetzt. Verantwortliche beobachten jedoch vermehrt auch die geopolitische Lage im Westen sowie im Osten. Prämisse der Stunde ist, die eigene IT nachvollziehbar und portabel aufzustellen, um im Fall der

Fälle handlungsfähig zu sein. Portabilität bedeutet dabei nicht nur technische Migrationspfade, sondern auch Vertragsmodelle, Datenformate und Betriebsprozesse, die einen realistischen Providerwechsel innerhalb planbarer Zeiträume ermöglichen. Dazu gehört auch die konkrete Auseinandersetzung mit europäischen Cloud-Anbietern und den souveränen Lösungen der Hyperscaler.

Sicher und performant

Auch der öffentliche Sektor nutzt zuletzt vermehrt Cloud-Dienste und lotet aktuell aus, wie eine sichere und zugleich performante Cloud-Strategie für Kommunen und Städte aussehen kann. Diese agieren aus Compliance- oder Governance-Gründen im Umgang mit Bürgerdaten oft vorsichtiger bei der Wahl ihrer Cloud-Anbieter und werden damit zum Souveränitäts-Gradmesser für andere Branchen, die schon seit Jahren auf Cloud

setzen. Hierbei ist bereits jetzt trotz hoher Compliance-Anforderungen ein Cloud-Mix zwischen verschiedenen Hyperscalern und europäischen Alternativen erkennbar. Klarer Treiber dieser Entwicklung ist die nötige Modernisierungsgeschwindigkeit der öffentlichen Verwaltung, die mit bestehenden Betriebsmodellen und Lösungen oft nicht mithalten kann.

Physische Nähe schafft Vertrauen

Hinzu kommt ein psychologischer Faktor, der im strategischen Diskurs häufig unterschätzt wird: Die physische Nähe zum lokalen Rechenzentrum koppelt sich bei vielen Entscheidern weiter mit hohem Vertrauen in Sicherheit und Unabhängigkeit. Dabei darf IT-Security nicht mit physischer Nähe verwechselt werden. Viele unternehmenseigene Rechenzentren erfüllen regulatorische Anforderungen wie NIS2 oder KRITIS sowie etablierte Standards

wie C5 nur unzureichend. Häufig fehlen zudem finanzielle und personelle Ressourcen, um ein Sicherheitsniveau zu erreichen, das große Cloud- und Rechenzentrumsanbieter mit spezialisierten Teams und hohen Investitionen umsetzen können.

Hierbei verfügen insbesondere die etablierten Cloud-Anbieter über Sicherheitsbudgets in Milliardenhöhe – ein Investitionsniveau, das für lokale Rechenzentren wirtschaftlich kaum erreichbar ist.

Ausblick

Souveränität wird zur gestalterischen Leitlinie. Europa investiert massiv in Rechenzentren, Cloud-Stacks, Energieeffizienz und offene Technologie-Ökosysteme. BITKOM platziert erfolgreich den Aktionsplan für leistungsfähige und nachhaltige Rechenzentren in Deutschland, um die digitale Infrastruktur auch national zu stärken. Gartner prognostiziert, dass bis 2030 mehr als drei Viertel der Unternehmen außerhalb der USA digitale Souveränitätsstrategien verfolgen werden. Diese Entwicklung bedeutet keinen Abgang auf Hyperscaler, sondern einen Wandel hin zu kombinierten Modellen.

Digitale Souveränität wird zum Designprinzip, nicht zum Zustand. Die Nutzung souveräner Angebote der Hyperscaler, die Auswahl europäischer Cloud-Anbieter sowie die Weiternutzung des lokalen Rechenzentrums sind hierbei abzuwägen. Souverän ist nicht, wer jede Abhängigkeit vermeidet, sondern wer sie kennt, steuert und im Bedarfsfall beenden kann. ◀

Digitale Souveränität beschreibt die Fähigkeit selbstbestimmt über die eigene IT-Infrastruktur und Daten zu entscheiden – mit voller Kontrolle über Zugriffe, Verarbeitung und Speicherort bei gleichzeitiger Leistungsfähigkeit.

Kontrolle

Selbstbestimmung
über IT-Entscheidungen

Leistungsfähigkeit

Technologische Exzellenz
für digitale Wettbewerbsfähigkeit

Souveränität bedeutet NICHT Isolation

Es geht um bewusste Entscheidungen mit Wahlfreiheit – nicht um Abschottung