Buzzword Digitale Souveränität

Unternehmen sind so stark wie nie zuvor von der Innovationskraft der Cloud abhängig. KI-Workloads, datengetriebene Geschäftsmodelle, globale Skalierung und kurze Time-to-Market basieren auf Managed Cloud Services und skalierbaren Infrastrukturen der Cloud-Provider. Ohne Cloud werden Organisationen schon mittelfristig die technischen Grundlagen für ihre Wettbewerbsfähigkeit fehlen.

Autorinnen:
Frauke Harms
Business Area Lead for Cloud Solutions.
Alena Mattfeldt
Senior Cloud Consultant

BTC AG
www.btc-ag.com

Digitale Souveränität umsetzen

Gleichzeitig rückt damit die Frage der digitalen Souveränität, also der selbststimmten und informierten Wahl des passenden technischen Rahmens für Workloads, ins Zentrum strategischer und operativer Entscheidungen. Was lange vor allem Leitbild und politische Debatte war, ist für CIOs und IT-Architekten zum tagtäglichen Entscheidungsmaßstab geworden: Nicht ob, sondern wie digitale Souveränität umgesetzt wird, ist die zentrale Frage. Geopolitische Spannungen, extraterritoriale Zugriffsgesetze wie der US CLOUD Act sowie Worst-Case-Szenarien – von Dienstblockaden bis zu erzwungenen Entzügen von Zugriffsrechten – schärfen die Risikowahrnehmung zusätzlich.

Parallel verschärfen Data Act, NIS2 und AI-Act die Anforderungen an Datenkontrolle, Resilienz und Governance. Digitale Souveränität entwickelt sich zur regulativen und geschäftskritischen Pflichtaufgabe.

Das Spannungsfeld

Damit entsteht ein Spannungsfeld: Wie lassen sich Kontrolle, Nachvollziehbarkeit und rechtliche Sicherheit mit dem Bedarf an technischer Leistungstiefe und Skalierbarkeit in Einklang bringen? Klar ist: Nicht die Anzahl der Clouds ist entscheidend, sondern die Passung der Plattformen zur jeweiligen Anwendung – technisch, organisatorisch und geopolitisch.

Souveränität als Architekturfrage

Weg vom Entweder-oder. In vielen Diskussionen wird digitale Souveränität noch immer so behandelt, als ginge es um eine Grundsatzentscheidung: Cloud ja oder nein, Hyperscaler oder europäischer Provider, Rechenzentrum oder Public Cloud. In der Praxis zeigt sich jedoch: Souveränität ist keine Frage des Entweder-oder, sondern eine Architekturfrage.

Eine völlig autarke IT-Landschaft lässt sich angesichts globaler Lieferketten, proprietärer Technologien sowie weltweit verteilter Hardware- und Netzwerkinfrastrukturen weder realistisch planen noch wirtschaftlich betreiben. Technische und organisatorische Abhängigkeiten lassen sich nicht gänzlich vermeiden, im Gegenteil, sie sind bei jeder Betriebsform, egal ob Cloud oder Betrieb im lokalen Rechenzentrum nach DSGVO erforderlich und nachzuweisen. Entscheidend ist, in welchem Maß Entscheider eine bewusste Gestaltung und Kontrolle ihrer IT-Landschaft angehen.

IT-Landschaft

Konkret rückt die Fähigkeit in den Fokus, Workloads und Daten bewusst zu platzieren und bei Bedarf verlagern zu können. Dazu braucht es zunächst eine saubere IT-Inventur: Welche Anwendungen laufen wo, welche technischen und organisatorischen Abhängigkeiten bestehen, wo befinden sich Daten mit hohem Schutzbedarf? Containerisierung und standardisierte Schnittstellen erhöhen die Portabilität zwischen Rechenzentrum, Private Cloud und Hyperscaler und reduzieren das Risiko eines Lock-ins.

Souveränitätscheck

Ein „Souveränitätscheck" je Anbieter wird zur Pflicht: Jurisdiktion und anwendbares Recht, Datenstandorte, Verschlüsselungsmodelle, Zugriffsmöglichkeiten von Behörden, Exit-Szenarien und Migrationsaufwände müssen systematisch bewertet werden. Hilfreich sind dabei strukturierte Bewertungsmodelle, etwa in Form eines „Sovereign Cloud Compass", der Unternehmen zwingt, ihre eigenen Prioritäten (z. B. Innovationshöhe vs. Jurisdiktionsrisiko) explizit zu gewichten und die Konsequenzen transparent macht. Digitale Souveränität ist damit nicht nur eine IT-Frage. Sie erfordert das abgestimmte Zusammenwirken von IT, Fachbereichen, Informationssicherheit, Datenschutz, Rechtsabteilung und – bei geschäftskritischen Themen – auch der Unternehmensleitung.

Wie Unternehmen Risiken bewerten

In hochregulierten KRITIS-Bereichen wie öffentlicher Verwaltung, Energieversorgung oder Finanzsektor ist digitale Souveränität längst fest auf der Agenda. Dort stellt sich nicht mehr die Frage, ob souveräne Architekturen erforderlich sind, sondern wie konsequent sie ausgestaltet sein müssen, um Audit- und Compliance-Vorgaben zu erfüllen, ohne gleichzeitig Innovation und Geschwindigkeit auszubremsen. Genau diese Abwägungen sollten jedoch auch Unternehmen außerhalb der KRITIS-Branchen treffen und ihre eigenen Risikoprofile, Abhängigkeiten und Handlungsoptionen kritisch prüfen.

Übergang von abstrakten zu konkreten Risiken

Der zentrale Schritt in der Praxis ist der Übergang von abstrakten zu konkreten Risiken. Statt: „Wir müssen souverän werden" lautet die Frage: „Welche Risiken wollen wir tatsächlich adressieren und in welchen Workloads können wir sie akzeptieren?" Typischerweise stehen dabei im Fokus:

- Geopolitische Abhängigkeiten von einzelnen Staaten oder Rechtsräumen
- Single-Provider-Risiken und Ausfallszenarien
- Kritikalität eines Ausfalls oder Zugriffsverlustes auf bestimmte Workloads

Preis zusätzlicher Souveränität

Darauf aufbauend bewerten Unternehmen den Preis zusätzlicher Souveränität: Vollständige Redundanz über mehrere Provider kann schnell zu annähernd doppelten Betriebskosten und Komplexität führen.

Manchmal reicht ein erprobtes Notfall- und Exit-Konzept (z. B. technische, organisatorische und vertragliche Vorbereitungen für einen Wechsel), um im Ernstfall handlungsfähig zu bleiben. In anderen Fällen, etwa bei hochkritischen Kernprozessen, ist eine aktive Parallelhaltung notwendig.

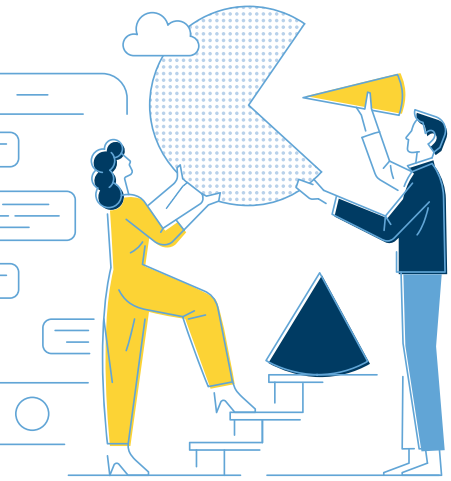
Architektur-Suche

Viele Organisationen gehen schrittweise vor und testen souveräne Cloud-Angebote in Proof of Concepts: Wie gut lassen sich regulatorische Anforderungen abbilden? Wie reibungslos funktioniert die Integration in bestehende Prozesse? Welche Performance- oder Feature-Unterschiede sind im Vergleich zu Hyperscalern akzeptabel? Damit verschiebt sich der Diskurs weg von Grundsatzfragen hin zu der pragmatischen Suche nach einer Architektur, die sowohl skalierbar als auch steuerbar bleibt.

Typische Stolpersteine auf dem Weg zur Cloud-Strategie

Auf dem Weg zu einer souveränen Cloud-Strategie begegnen vielen Organisationen ähnliche Stolpersteine:

- **Gleichbehandlung aller Daten:** Ohne differenzierte Workload-Klassifizierung entstehen überkomplexe Sicherheits- und Betriebsmodelle. Unkritische Daten werden überhärtet, während wirklich schützenswerte Informationen nicht ausreichend abgesichert sind. Abhilfe schafft ein abgestuftes Konzept, das Schutzbedarf und Business-Kritikalität konsequent berücksichtigt.
- **Zeitgleiche Migration:** Big-Bang-Migrationen überfordern Teams und Systeme. Verborgene Abhängigkeiten werden häufig erst im Störungsfall sichtbar – mit entsprechend hohem Betriebsrisiko. Ein schrittweises Vorgehen nach Clustern – etwa entlang von Domänen, Applikationsverbünden oder Datenclustern – reduziert diese Risiken und erhöht die Steuerbarkeit.
- **Start ohne vollständiges Bild:** Wer ohne saubere Inventur und Abhängigkeitsanalyse in die Cloud geht, riskiert Lock-ins, Sicherheitslücken und ungeplante Kosten. Die Devise lautet: erst Transparenz, dann Entscheidungen.



Diese Stolpersteine sind kein Zufall, sondern Ausdruck fehlender Grundlagen. Genau hier setzen die zentralen Bausteine einer souveränen Cloud-Strategie an.

Drei Säulen einer souveränen Cloud-Strategie

Eine tragfähige Cloud-Strategie, die digitale Souveränität ernst nimmt, ruht im Kern auf drei Säulen:

1. Datenklassifizierung

Ohne Klarheit über Schutzbedarfe drohen Fehlentscheidungen. Werden etwa Testdaten, Marketing-Workloads und HR-Informationen im selben Set-up betrieben, führt das entweder zu überzogenen Sicherheitsanforderungen für unkritische Daten oder zu Untersteuerung in sensiblen Bereichen. Eine systematische Klassifizierung nach Vertraulichkeit, Integrität und Verfügbarkeit ist Grundvoraussetzung, um Workloads souverän und risikoadäquat platzieren zu können.

2. Prozesslandschaft und Transparenz

Unternehmen müssen wissen, wo welche Prozesse laufen, welche Systeme voneinander abhängen und wo Daten mit hoher „Data Gravity“ liegen, also von vielen Systemen intensiv genutzt werden. Tools zur Inventarisierung, Discovery Center, CMDB-Integration und Security-Analysen schaffen ein möglichst vollständiges Bild über Software, Infrastruktur, Auslastungsspitzen und Datenflüsse. Erst diese Transparenz ermöglicht es, Workloads in sinnvollen Clustern zu migrieren – statt in einem risikoreichen Big-Bang-Ansatz.

3. Organisatorische Reife und Fähigkeiten

Cloud-Architekturen erfordern andere Fähigkeiten als klassische Rechenzentren: Automatisierung, Infrastructure as Code, Container-Orchestrierung, Zero-Trust-Security sowie kontinuierliches Kosten- und Risikomanagement. Wer souverän handeln will, muss diese Kompetenzen im eigenen Haus aufbauen oder gezielt durch Partner ergänzen – inklusive klarer Governance-Modelle, Rollen und Verantwortlichkeiten.

Selbstbestimmung als Zielbild

Erst vor diesem Hintergrund wird die Frage nach dem jeweils „richtigen“ Provider sinnvoll. Marktvielfalt ist prinzipiell ein Vorteil: Hyperscaler, europäische Anbieter, spezialisierte Sovereign-Cloud-Angebote und eigene Rechenzentren lassen sich kombinieren. In der Praxis hat sich gezeigt, dass ein Mix aus wenigen, bewusst ausgewählten Plattformen, idealerweise nicht mehr als drei, die Handhabbarkeit wahrt und gleichzeitig ausreichend Wahlfreiheit ermöglicht.

Das größte Risiko liegt weniger in der Nutzung einzelner Hyperscaler, sondern in ungesteuert gewachsenen Cloud-Landschaften ohne klares Regelwerk: Schatten-IT, redundante Services, widersprüchliche Sicherheitsniveaus und fehlende Exit-Strategien untergraben jede Form von Souveränität.

Wer dagegen technologische Vielfalt aktiv orchestriert, schafft sich echte Selbstbestimmung: Daten mit hohem Schutzbedarf können in souveränen oder lokal/regional verankerten Umgebungen verarbeitet werden, während hochskalierende KI- oder Analyse-Workloads in globalen Plattformen laufen. Entscheidend ist, dass diese Entscheidungen bewusst getroffen werden – auf Basis klar definierter Ziele, belastbarer Risikoanalysen und transparenter Architekturprinzipien.

Abhängigkeiten kennen

Digitale Souveränität bedeutet in diesem Verständnis nicht, ohne Abhängigkeiten zu sein. Sie bedeutet, Abhängigkeiten zu kennen, zu bewerten und aktiv zu steuern. Unternehmen, die ihre Cloud-Strategie heute unter diesem Blickwinkel neu ausrichten, machen sich unabhängiger von geo- und marktpolitischen Verwerfungen – und sichern sich zugleich die Innovationsfähigkeit, die sie für die Herausforderungen der nächsten Jahre benötigen.

Pragmatisches Vorgehen

Ein pragmatisches Vorgehen folgt dabei drei Schritten: Bestandsaufnahme von Workloads, Daten und Abhängigkeiten, Bewertung der Souveränitätsanforderungen und Risiken – und darauf aufbauend die Definition einer Zielarchitektur mit klaren Governance-Regeln und Exit-Szenarien. So wird digitale Souveränität vom Buzzword zur gelebten Handlungsfähigkeit.

Wer schreibt:

Als Business Area Lead for Cloud Solutions bei der BTC AG spielt **Alena Mattfeldt** eine zentrale Rolle in der Entwicklung und Umsetzung der Cloud-Aktivitäten. Sie hat maßgeblich am Aufbau der Cloud-Unit als agile IT-Service-Organisation mitgewirkt, die heute das Fundament sämtlicher Cloud-Aktivitäten bei BTC bildet.

Als Senior Cloud Consultant bei der BTC AG gestaltet **Frauke Harms** die strategische Weiterentwicklung von Azure Infrastructure- und Security-Lösungen. Sie verbindet Marktanforderungen mit Portfolio- und Innovationsinitiativen und trägt zur nachhaltigen Positionierung der Cloud-Services bei. ◄