Raus aus der Abhängigkeit

CLOUD-EXIT: WIE UNTERNEHMEN IHRE DIGITALE SOUVERÄNITÄT ZURÜCKGEWINNEN

US-Hyperscaler dominieren den Cloud-Markt, doch für europäische Unternehmen wachsen die Risiken. Unsere Autoren zeigen, wie sich Exit-Strategien und souveräne Cloud-Architekturen risikobasiert entwickeln lassen: von bewährten Portabilitäts-Mustern über Multi- und Sovereign-Cloud-Modelle bis hin zu durchdachten Governance-Mechanismen, die Sicherheit, Compliance und unternehmerische Handlungsfähigkeit miteinander verknüpfen.

Die Nutzung von Cloud-Diensten großer US-Anbieter entwickelt sich für europäische Unternehmen und Behörden zunehmend zum Problem. Geopolitische Spannungen, gesetzliche Zugriffsmöglichkeiten wie der Cloud Act und strenge Datenschutz-Vorgaben machen deutlich: Cloud bedeutet nicht mehr nur Skalierbarkeit und Effizienz, sondern auch Kontrollverlust.

Digitale Souveränität wird damit zur Schlüsselanforderung. Organisationen müssen sicherstellen, dass sie über ihre Daten und Infrastruktur selbstbestimmt verfügen können – unabhängig von externen politischen oder regulatorischen Einflüssen.

RECHTLICHE RAHMENBEDINGUNGEN VERSCHÄRFEN DEN DRUCK

Die rechtliche Lage im Cloud-Umfeld hat sich in den vergangenen Jahren mehrfach verschoben. Besonders das Schrems-II-Urteil sorgt bis heute für Unsicherheit: Mit dem Beschluss hob der Europäische Gerichtshof das frühere Privacy Shield auf. Standardvertragsklauseln bleiben zwar ein wichtiges Instrument, verlangen jedoch zusätzliche technische und organisatorische Schutzmaßnahmen. In der Folge führen das EU-US Data Privacy Framework und die Executive Order 14086 neue Garantien ein – etwa Redress-Mechanismen (Beschwerdeverfahren) und Grundsätze der Verhältnismäßigkeit bei Geheimdienstzugriffen. Diese Regelungen mindern Risiken, schaffen aber keine vollständige Rechtssicherheit und ersetzen keine individuelle Prüfung einzelner Workloads.

Weiterhin bleibt der CLOUD Act ein zentraler Unsicherheitsfaktor: US-Behörden dürfen unter bestimmten Bedingungen auf Daten von US-Anbietern zugreifen, auch wenn diese physisch in der EU liegen. Entscheidend dafür sind Besitz, Verwahrung oder Kontrolle. Gleichzeitig erhöhen NIS-2 und DORA den Druck auf Unternehmen: Beide Regularien verschärfen die Anforderungen an Governance, Lieferkettenmanagement und Drittparteikontrolle sowie an Exit-Fähigkeit und Resilienz – vor allem für Betreiber kritischer Infrastrukturen und Akteure im Finanzsektor.

WENN TRANSPARENZ AN GRENZEN STÖßT

Die Nutzung von US-Hyperscalern schafft vor allem für Betreiber kritischer Infrastrukturen eine komplexe Risikolandschaft. Politische und regulatorische Unsicherheiten – etwa durch den CLOUD Act oder mögliche Handelsrestriktionen – können dazu führen, dass Behörden auf Daten zugreifen oder Cloud-Dienste eingeschränkt werden, selbst wenn die Informationen physisch in Europa liegen. Solche extraterritorialen Zugriffspflichten untergraben die Rechtssicherheit und gefährden die Integrität sensibler Systeme.

Ein Beispiel aus der Praxis: Ein europäisches Unternehmen betreibt geschäftskritische Anwendungen in der Public Cloud eines großen US-Anbieters. Zwar liegt eine Testierung nach dem Cloud Computing Compliance Criteria Catalogue (C5) – eine Testierung nach ISAE-3000-Auditstandard des Bundesamts für Sicherheit in der Informationstechnik (BSI), keine Zertifizierung im engeren Sinne – vor und belegt definierte Sicherheits- und Compliance-Kontrollen, doch die tatsächliche Transparenz bleibt begrenzt. Der Katalog bestätigt das Vorhandensein definierter Kontrollen, ersetzt jedoch nicht die individuelle Einsicht in Betriebsprozesse oder Speicherorte. Für hochsensible Workloads braucht es deshalb einen eigenen Transparenz- und Evidenzpfad – mit Nachweisen zu Replikation, Zugriffsketten und eingebundenen Drittparteien.

Selbst detaillierte Audit-Anfragen stoßen in der Praxis an Grenzen, wenn Anbieter nur standardisierte Reports bereitstellen und keine tieferen technischen Details offenlegen. Diese Intransparenz erschwert es, die Einhaltung europäischer Datenschutzanforderungen vollständig zu prüfen und Risiken aus extraterritorialen Gesetzen realistisch zu bewerten. Gleichzeitig drohen Lock-in-Effekte: Proprietäre Schnittstellen und enge Dienstabhängigkeiten machen den Anbieterwechsel aufwendig und riskant. Im Ernstfall – etwa bei geopolitischen Konflikten oder regulatorischen Änderungen – kann das die Geschäftskontinuität unmittelbar gefährden.

Ohne eigene Architekturentscheidungen bleibt „digitale Souveränität“ ein theoretisches Konzept, kein praktischer Vorteil.

Die Kombination aus politischem Druck, rechtlichen Unsicherheiten und technologischen Abhängigkeiten macht deutlich: Strategische Exit-Optionen und souveräne Cloud-Architekturen sind keine theoretische Überlegung, sondern eine sicherheitsrelevante Notwendigkeit für Organisationen, die kritische Dienste bereitstellen.

EXIT-STRATEGIE IM KONTEXT DIGITALER SOUVERÄNITÄT

Eine Exit-Strategie bedeutet nicht die sofortige Migration aller Systeme, sondern die Fähigkeit, jederzeit handlungsfähig zu sein. Sie schafft die Grundlage, um im Fall regulatorischer Änderungen, geopolitischer Spannungen oder technischer Risiken schnell reagieren zu können.

Ohne eine definierte Exit-Option bleibt Entscheidungsfreiheit häufig theoretisch, da technische und organisatorische Abhängigkeiten den Wechsel erschweren. Erst die aktive Vorbereitung – etwa durch Migrationspläne, Daten- und Log-Portabilität sowie Notfallkonzepte – macht Souveränität praktisch umsetzbar. Ein Missverständnis ist, „Exit" mit passivem Abwarten gleichzusetzen. Wirksam ist nur ein proaktiver Ansatz: Analyse der Workloads, Identifikation von Lock-in-Risiken und Aufbau alternativer Plattformen.

Open-Source-basierte und standardisierte Komponenten sowie containerbasierte Portabilität senken Wechselkosten und verringern Abhängigkeiten. Dadurch lassen sich Workloads flexibel auf Hyperscalern, europäischen Cloud-Plattformen oder auf unternehmenseigenen Infrastrukturen (On-Premises) betreiben. Ergänzend sichern vertragliche Exit-Optionen – etwa die Portabilität von Daten und Protokollen, klare Service Level Agreements (SLA) und festgelegte Audit-Rechte – die Handlungsfähigkeit langfristig ab.

PRAGMATISCHER ANSATZ ZUR WORKLOAD-KLASSIFIKATION

Ein entscheidendes Element für jede Exit-Strategie ist die Priorisierung der Workloads. Ein bewährter Weg ist die Klassifikation nach Daten- und Systemkritikalität:

- **Unternehmenskritisch:** Systeme, deren Ausfall die Geschäftskontinuität unmittelbar gefährdet, zum Beispiel Enterprise Resource Planning (ERP) oder Produktionssteuerung
- **Kritisch:** Anwendungen mit hohem Einfluss auf Compliance oder Sicherheit, aber ohne sofortige Betriebsunterbrechung, zum Beispiel Human-Resources-(HR)-Systeme oder die Finanzbuchhaltung
- **Intern:** Workloads für interne Prozesse mit begrenztem Risiko, zum Beispiel Kollaborationstools
- **Öffentlich:** Systeme mit offenen Daten oder geringer Sensibilität, zum Beispiel Marketing-Websites

Diese Klassifikation ermöglicht eine schrittweise Exit-Planung: Zuerst Backups und Disaster-Recovery für unternehmenskritische Workloads, dann Migration kritischer Systeme, während weniger sensible Anwendungen später folgen. So entsteht ein realistischer, priorisierter Migrationspfad, der Handlungsfähigkeit sichert, ohne operative Stabilität zu gefährden. Ergänzend sollte je Klasse der Schutzbedarf – also Vertraulichkeit, Integrität, Verfügbarkeit und rechtliche Anforderungen – sowie die Exit-Tiefe (von reinen Sicherungskopien bis zu vollständig redundanten Disaster-Recovery- und aktiv-aktiv-Szenarien) mit konkreten Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) verknüpft werden.

ERFOLGSFAKTOREN FÜR DEN STRATEGISCHEN EXIT

Eine wirksame Exit-Strategie verlangt mehr als technische Maßnahmen. Sie beginnt mit einer klaren strategischen Ausrichtung und endet in einer umsetzbaren Praxis. Eine einheitliche Lösung gibt es jedoch nicht. Der konkrete Weg hängt immer vom Geschäftsmodell, von regulatorischen Anforderungen und von der technischen Ausgangslage ab. Fünf Faktoren bestimmen, ob eine Exit-Strategie in der Praxis trägt:

- **Strategische Verankerung:** Jede Exit-Strategie braucht Rückendeckung aus der Geschäftsleitung. Sie ist Teil der Risiko- und Compliance-Strategie und muss in die Unternehmensplanung integriert sein.
- **Transparenz und Analyse:** Abhängigkeiten müssen sichtbar werden. Das gelingt durch Abstraktionsschichten zwischen Anwendung und Plattformdiensten sowie durch die konsequente Vermeidung proprietärer Schnittstellen.
- **Offenheit und Portabilität:** Offene Standards und containerbasierte Architekturen bilden das Rückgrat einer souveränen Cloud-Strategie. Organisationen sollten früh festlegen, welche Kernkomponenten portabel und interoperabel bleiben müssen.
- **Wirtschaftlichkeit:** Eine realistische Kalkulation entscheidet über den Erfolg. Investitionen in Migration, neue Plattformen und Schulungen müssen den Gesamtbetriebskosten (Total Cost of Ownership, TCO) gegenübergestellt werden. Der Wettbewerb zwischen Anbietern wirkt dabei als Optimierungshebel.
- **Architektonische Absicherung:** Schlüsselherrschaft, Zugriffsentkopplung, Datenlokalisierung und die regelmäßige Testbarkeit der Zielplattform schaffen technische Flexibilität und organisatorische Resilienz.

ARCHITEKTURPRINZIPIEN FÜR SOUVERÄNE CLOUD-UMGEBUNGEN

Darüber hinaus gilt es, die technische Architektur konsequent auf Portabilität auszurichten. Ein zentrales Prinzip lautet Portability by Design: Standardisierte Containerformate nach Open Container Initiative (OCI), Infrastruktur als Code und automatisierte Plattformtests gewährleisten, dass Workloads unabhängig von einzelnen Anbietern betrieben werden können.

Ebenso wichtig ist eine konsequente Kryptografie- und Schlüsselherrschaft. Unternehmen sollten ihre Schlüssel selbst kontrollieren – etwa über Hardware-Sicherheitsmodule (HSM) oder externe Key-Management-Systeme (KMS) – und deren Rotation dokumentieren. Masterkeys dürfen dabei grundsätzlich nicht exportierbar sein.

Auch die Zugriffsentkopplung spielt eine zentrale Rolle. Strikte Least-Privilege-Modelle, getrennte Administrator-Domänen, Just-in-Time-Berechtigungen und revisionssichere Protokollierung in einer separaten Vertrauensdomäne erhöhen die Sicherheit und Nachvollziehbarkeit.

Nicht zuletzt trägt eine klare Datenlokalisierung zur Souveränität bei: Sensible Workloads sollten ausschließlich innerhalb der Europäischen Union verarbeitet werden. Remote-Administrationszugriffe von außerhalb des europäischen Rechtsraums sind bei kritischen Infrastrukturen (KRITIS) zu vermeiden.

Ergänzend gehört zu einer souveränen Cloud-Architektur ein durchgängiger Transparenz- und Audit-Pfad. Vertraglich zugesicherte Auskunfts- und Prüfungsrechte, klar definierte Disclosure-Prozesse und technische Nachweise – etwa in

Reifegrad	Merkmale
Basic	Backups vorhanden, kein dokumentierter Migrationspfad, minimaler Portabilitätsnachweis
Prepared	Restore-/Migrationstests dokumentiert, getrennte Admin-Domänen und Schlüsselhaltung, Verträge mit Portabilitätsklauseln
Portable	automatisierte Migration auf Alternativplattformen, Container/Infrastrucure-as-Code, externe Schlüsselherrschaft etabliert
Resilient	regelmäßige Trockenübungen, nachweisbares Full-Failover, Logs in separater Trust-Domäne, definierte und geprüfte RTO/RPO-Ziele

Tabelle 1: Checkliste Reifegradmodell Exit-Fähigkeit

Form von Attestierungen oder Protokollen – ermöglichen eine unabhängige Überprüfung, ohne Betriebsgeheimnisse zu gefährden.

Abschließend gilt: Ein Exit bleibt nur dann wirksam, wenn er regelmäßig getestet wird. Organisationen sollten Wiederherstellungs- und Migrationsübungen fest einplanen, Zielplattform-Runbooks dokumentieren und messbare Kennzahlen für Wiederanlaufzeiten und Datenverluste definieren. Nur so lässt sich die Exit-Fähigkeit im Ernstfall verlässlich nachweisen.

REIFEGRADMODELL ALS ORIENTIERUNG

Um den Stand der eigenen Exit-Fähigkeit bewerten zu können, lässt sich der Fortschritt anhand eines Reifegradmodells mit vier Stufen einordnen (siehe Tabelle 1). Basic steht für die Ausgangsstufe: Backups sind vorhanden, ein dokumentierter Migrationspfad oder belastbarer Nachweis der Portabilität jedoch nicht. Prepared beschreibt Organisationen, die bereits Restore- und Migrationstests dokumentiert haben, getrennte Administrator-Domänen und eine eigene Schlüsselhaltung betreiben sowie über Verträge mit Portabilitätsklauseln verfügen.

Portable kennzeichnet Umgebungen, in denen Workloads automatisiert auf alternative Plattformen migriert werden können – mit containerisierten Anwendungen, Infrastruktur als Code und einer etablierten externen Schlüsselverwaltung. Resilient schließlich bezeichnet die höchste Stufe: Regelmäßige Wiederherstellungsübungen, ein nachweisbares vollständiges Failover, Protokolle in separaten Vertrauensdomänen sowie definierte und geprüfte Wiederanlauf- und Wiederherstellungsziele sichern die Exit-Fähigkeit auch im Ernstfall.

EU DATA ACT SCHAFFT NEUE CHANCEN

Ein deutliches Signal für Überlegungen zu Exit-Szenarien sind neue Rahmenbedingungen, die durch die europäischen Institutionen gesetzt werden. Der EU Data Act (VO (EU) 2023/2854) ist seit 2024 in Kraft; der Großteil der Pflichten gilt ab 12. September 2025 und bringt für Unternehmen einen entscheidenden Vorteil: verbindliche Wechselrechte für Cloud-Kunden. Damit wird der Anbieterwechsel nicht mehr nur eine technische, sondern auch eine rechtlich abgesicherte Option. Ein weiterer Meilenstein folgt bis zum 12. Januar 2027, wenn sogenannte Egress-Gebühren vollständig entfallen müssen – also Entgelte, die Anbieter bislang für das Herausleiten oder Übertragen von Daten an andere Plattformen verlangten.

Diese Regelungen senken die finanziellen Hürden für Datenmigration erheblich und stärken die Position europäischer Unternehmen gegenüber Hyperscalern. Wer jetzt eine Exit-Strategie plant, sollte diese neuen Rechte aktiv nutzen – etwa durch die Aufnahme entsprechender Klauseln in Verträge und die Vorbereitung auf einen Anbieterwechsel ohne zusätzliche Kosten.

Der neue Rechtsrahmen stärkt die digitale Souveränität, doch nur Unternehmen, die frühzeitig handeln und ihre Architektur entsprechend ausrichten, können die Vorteile tatsächlich nutzen.

FAZIT

Für alle Organisationen, die sich mit einem Exit-Szenario beschäftigen, ist digitale Souveränität kein abstraktes Ideal, sondern ein strategischer Imperativ. Wer heute die Kontrolle über Daten, Systeme und Plattformen sichern will, muss den Exit nicht als Rückschritt begreifen, sondern als Gestaltungsoption. Der EU Data Act liefert dafür neue rechtliche Hebel – doch ohne technische und organisatorische Vorbereitung bleiben sie wirkungslos.

Jetzt ist der richtige Zeitpunkt, die Exit-Fähigkeit gezielt zu planen und zu bewerten. Welche Workloads sind kritisch? Wo bestehen Lock-in-Risiken? Welche Architekturentscheidungen ermöglichen echte Portabilität? Wer diese Fragen heute beantwortet, sichert morgen die Handlungsfreiheit seines Unternehmens – und schafft die Grundlage für Resilienz, Innovationsfähigkeit und regulatorische Sicherheit in einer zunehmend fragmentierten digitalen Welt. ■

MICHAEL BERTKO
ist Sales Consultant bei OPITZ CONSULTING und begleitet Unternehmen bei der Entwicklung und Umsetzung ganzheitlicher Cloud- und Infrastrukturstrategien. Sein Schwerpunkt liegt auf digitaler Souveränität, Multi-Cloud-Architekturen und Exit-Szenarien, die Kontrolle, Sicherheit und Wirtschaftlichkeit miteinander verbinden.

JEREMY SMEETS
ist Senior System Engineer und strategischer Technologieberater bei OPITZ CONSULTING. Seit über einem Jahrzehnt begleitet er Unternehmen und öffentliche Institutionen bei der Architektur, Integration und Transformation komplexer Infrastrukturen – mit besonderem Fokus auf digitale Souveränität, Open-Source-Ecosysteme und nachhaltige Plattformstrategien.