ISSN 1864-0907
SEPTEMBER 2026

IT-BUSINESS

CHANNEL GUIDE

DIE CLOUD

VOGEL IT MEDIEN

Souveränität als Spektrum

Die Debatte um Digitale Souveränität pendelt zwischen berechtigten Warnungen vor zu großen Abhängigkeiten und antiamerikanischen Beißreflexen. Dabei geht die entscheidende Frage unter: Nicht ob ein US-Anbieter souverän sein kann, sondern welcher Grad an Souveränität für welchen Workload nötig ist. AWS, Google und Microsoft beantworten sie mit drei unterschiedlichen Ansätzen.

Europa braucht eigene souveräne Cloud-Infrastrukturen – in diesem Punkt sind sich IT-Branche und Digitalpolitik weitgehend einig. Zu groß sei die Gefahr, dass in einer geopolitischen Krise jemand den Stecker zieht oder den berüchtigten Kill Switch betätigt. So weit der Konsens. Danach geraten wirtschaftspolitische Wunschbilder und unternehmerische Realitäten durcheinander, und die Debatte schrumpft schnell auf eine simple Formel: gute europäische Cloud, böse US-Cloud. Wer nachfragt, bekommt das Stichwort CLOUD Act serviert – oder ein ganz persönliches Unbehagen über Donald Trumps Zoll- und Außenpolitik.

Zwei Beispiele gefällig? Christian Scholz, VP Health & Energy bei Stackit, kommt in einem Blog zu dem Schluss, dass „US-IT-Firmen für europäische Unternehmen zum Geschäftsrisiko“ geworden sind. Benjamin Schilz, CEO des Messengerdienstes Wire, lässt US-Präsident Trump in einem LinkedIn-Post gleich per Panzer über Europa rollen. Das Kettenfahrzeug trägt dabei die Logos von AWS, Google und Microsoft. Wie sich das mit den eigenen US-Partnerschaften der Schwarz-Gruppe – etwa Zscaler oder Crowdstrike – und den unzähligen Hard- und Softwareabhängigkeiten Europas verträgt, müssen die Beteiligten selbst beantworten.

Solche Zuspitzungen zeigen vor allem eines: Bei der Differenzierung ist Luft nach oben. Und genau die brauchen Kunden, um eine tragfähige Multicloud-Strategie zu entwickeln. „Viele Kunden ordnen die Regulatorik, der sie unterliegen, gar nicht richtig ein und versteifen sich aus Angst auf einen bestimmten Weg“, sagt Pascal Reddig, Head of Google Cloud beim IT-Dienstleister Adesso. Der Kill Switch ist ein starkes Bild. Wahrscheinlicher ist der Alltag: Sanktionen gegen Einzelpersonen, Exportkontrollen, geänderte Lizenzbedingungen. Das trifft andere Workloads – und verlangt andere Antworten.

AWS, Microsoft und Google haben den europäischen Bedarf bei Datensouveränität, Compliance und Governance längst erkannt, ihre Portfolios entsprechend ausgebaut und insbesondere Deutschland als Schlüsselmarkt identifiziert. Ihre gemeinsame Botschaft: Digitale Souveränität ist für sie eine weitere Wahlmöglichkeit, keine europäische Autarkie. Eine allgemeingültige Definition des Begriffs gibt es ohnehin nicht. Die Hyper-

BILD: MIDJOURNEY / KI-GENERIERT

scaler behandeln ihn deshalb als eine Art Spektrum und bauen ihre Angebote entsprechend auf. „Wir differenzieren je nach Sensitivitätsgrad des Workloads und empfehlen das entsprechende Souveränitätsmodell“, sagt Guido Massfeller, Head of Sovereignty DACH bei Google Cloud. „Das hat natürlich auch Auswirkungen auf die Funktionen, die Ausformung der Souveränität und letztlich auf den Preis. Wenn ein Unternehmen nur Datensouveränität anstrebt, benötigt es keine operationale Souveränität.“

Google Cloud baut drei Sovereign-Modelle auf, bei denen den Partnern eine entscheidende Rolle zukommt. Die Wahl besteht zwischen Data Boundary, Cloud Dedicated und einer Air-Gapped-Lösung. „Unternehmen sollten Kontakt mit uns aufnehmen, wenn sie nicht an One-Size-Fits-All glauben“, so Massfeller. Für das häufig vorgebrachte Argument eines US-Zugriffs über den CLOUD Act zeigt er Verständnis: „Unsere Public-Cloud-Services unterliegen dem CLOUD Act. Das muss man klar sagen. Deswegen prägt diese Realität unsere Strategie im Souveränitätsumfeld: Wir stellen diese Angebote ausschließlich zusammen mit nationalen Partnern zur Verfügung.“

Die erste Stufe, Data Boundary, adressiert reine Datensouveränität: Kunden bestimmen, wo ihre Daten regional gespeichert und verarbeitet werden, die Schlüsselverwaltung liegt außerhalb der Google-Infrastruktur. Die Bereitstellung des Schlüssels, der permanent verfügbar sein muss, kann in dem Modell über T-Systems erfolgen.

Wem das nicht reicht, für den greift das zweite Modell: Cloud Dedicated. Hier wandert ein großer Teil der Verantwortung in die Hände eines Partners. Das französische Unternehmen Thales baut dazu eine neue, rechtlich und operativ von Google Cloud unabhängige Gesellschaft in Deutschland auf, die die Infrastruktur ausschließlich mit deutschem Personal betreibt. „Wir übergeben praktisch eine Kopie des Google-Cloud-Universums in die Hände eines Partners – in Deutschland in die Hände von Thales“, erklärt Massfeller. „Thales ist der operationale Partner dieser Cloud, zieht einen Käfig um diesen dedizierten Teil und managt alles, was rein- und rausgeht. Google ist der Technologiepartner, die Bereitstellung obliegt aber komplett dem Partner.“

Angst vor fremden Zugriffen im Support begegnet Massfeller so: „Sollte es einen Supportfall geben, bei dem Google ins Rechenzentrum müsste, kämen wir dort nur eskortiert rein und raus. Das ist genau das wesentliche Unterscheidungsmerkmal unseres Souveränitätsangebots. Der Partner ist der operative Owner dieser Cloud-Infrastruktur und legal wie technisch unabhängig.“ Für besonders strenge Anforderungen bleibt die Air-Gapped-Lösung. „Google hat weder physikalischen noch virtuellen Zugang zu diesen Systemen und Daten“, erklärt Reddig. Medial bekannt wurde die Lösung im vergangenen Jahr als Teil der Multicloud-Strategie der Bundeswehr; im Einsatz ist sie unter anderem im Joint Analysis, Training and Education Centre der NATO.

Microsoft bündelt sein Angebot unter der Microsoft Sovereign Cloud – ebenfalls in drei Bereitstellungsmodellen. Der konzeptionelle Unterschied zu Google Cloud liegt im Ausgangspunkt: Microsoft betrachtet digitale Souveränität in erster Linie als in die Plattform integrierte Funktion. In der Sovereign Public Cloud nutzen Unternehmen Cloud- und KI-Dienste mit souveränen Kontrollen aus der öffentlichen Microsoft-Cloud heraus; Betrieb und Zugriff

BILD: GOOGLE CLOUD

Guido Massfeller, Head of Sovereignty DACH bei Google Cloud

„Unternehmen sollten Kontakt mit uns aufnehmen, wenn sie nicht an One-Size-Fits-All glauben. Wir differenzieren je nach Sensitivitätsgrad des Workloads und empfehlen das entsprechende Souveränitätsmodell.“

BILD: AWS

Stéphane Israël, Managing Director bei AWS European Sovereign Cloud

„Kunden wollen das Beste aus beiden Welten – sie möchten die komplette Palette der fortschrittlichen Cloud- und KI-Services von AWS nutzen können und gleichzeitig sicherstellen, dass sie strengste Souveränitätsanforderungen erfüllen können.“

BILD: MICROSOFT

Ralf Wigand, National Security & IT-Compliance Officer bei Microsoft Deutschland

„Bei Microsoft verstehen wir Digitale Souveränität als Spektrum: Wir stellen die Optionen bereit, mit denen jeder Kunde die Wahlfreiheit hat, nach seinen Vorgaben und Wünschen das passende Maß an lokaler Verarbeitung, Kontrollmöglichkeiten und Leistungsfähigkeit zu wählen."

werden von europäischem Personal kontrolliert, die Verschlüsselung liegt laut Ralf Wigand, National Security & IT-Compliance Officer bei Microsoft Deutschland, vollständig beim Kunden. „Organisationen müssen dafür nicht in eine separate Cloud wechseln oder ihre Architektur ändern, sondern können die Souveränitätskontrollen innerhalb der Umgebung anwenden, die sie bereits betreiben."

Ergänzend gibt es die Sovereign Private Cloud. „Damit können Kunden Microsoft-Lösungen auch auf kundenseitig kontrollierter Infrastruktur betreiben – in hybriden oder auch vollständig getrennten Umgebungen. Das ist insbesondere für regulierte Branchen, den öffentlichen Sektor sowie sensible Umgebungen und unternehmenskritische Workloads relevant, bei denen regulatorische, Sicherheits- oder Resilienzanforderungen eine stärkere Isolation voraussetzen", so Wigand. Das dritte Modell setzt auf Partner: Die National Partner Clouds sind unabhängig betriebene Umgebungen für spezifische regulatorische Anforderungen. „Sie basieren technisch auf Azure, werden aber von nationalen Partnern unabhängig betrieben. In Deutschland etwa betreiben SAP und Arvato gemeinsam die Partner-Cloud Delos."

AWS geht hingegen einen anderen Weg und baut eine eigene souveräne Cloud-Region neben den bestehenden auf. Im Januar folgte der offizielle Launch der AWS European Sovereign Cloud in Brandenburg. Rund 7,8 Milliarden Euro will AWS bis 2040 in die Region investieren. Technologisch setzt AWS auch hier auf das Nitro-System. Entscheidend ist aber die Abgrenzung: Die ESC bildet eine eigene Partition (eusc-de-east-1), die physisch und logisch von der globalen AWS-Cloud getrennt ist. Für die Nutzung sind separate Accounts sowie eine eigenständige Tooling- und Management-Konfiguration erforderlich. Ergänzt wird das Angebot durch Verschlüsselungs-, Schlüsselverwaltungs- und Compliance-Mechanismen sowie ein eigenes Sovereign Reference Framework. Es dient Kunden als formalisierter Nachweisrahmen gegenüber Aufsichtsbehörden und Auditoren, um die Einhaltung ihrer Souveränitätsanforderungen belegen zu können. Zum Start stehen mehr als 90 AWS-Services bereit – eine Feature-Parität mit der globalen AWS-Cloud wird angestrebt. Auch AWS hat für die ESC eine in Deutschland ansässige Holding gegründet. Die ESC soll im schlimmsten Fall, etwa bei einem Kill-Switch-Szenario, einen unabhängigen Betrieb auf unbestimmte Zeit ermöglichen.

Auch die Politik wünscht sich anscheinend eine Koexistenz europäischer und amerikanischer Wettbewerber – formuliert dafür aber Bedingungen. „Um mit digitalen Innovationen Schritt zu halten und gleichzeitig digitale Souveränität zu ermöglichen, verfolgt das BSI eine Doppelstrategie", erklärte BSI-Präsidentin Claudia Plattner im Januar. „Erstens: Der europäische Markt und die hiesige Digitalindustrie müssen gestärkt werden. Zweitens: Außereuropäische globale Produkte müssen so angepasst und eingebettet werden, dass eine sichere und selbstbestimmte Nutzung möglich wird. Voraussetzung dafür sind im Bereich Cloud-Computing innovative Angebote, die als europäische Instanzen sowohl technisch als auch organisatorisch unabhängig betrieben werden."

Digitale Souveränität ist kein Zustand, den manabhakt, sondern eine unternehmerische Entscheidung – pro Workload, im Abgleich von Kontrolle, Risiko, Leistungsfähigkeit und Kosten. Die entscheidende Frage lautet nicht „Europa oder USA?", sondern: Wie viel Souveränität brauchen wir – und was sind wir bereit, dafür zu bezahlen? Liefern müssen darauf beide Seiten. Europäische Anbieter wären gut beraten, die US-Hyperscaler auch in stark regulierten Branchen als Konkurrenten im Wettbewerb wahrzunehmen statt als Gegner in einem Kulturkampf. Die Hyperscaler hingegen müssen Souveränität trotz aller Vorbehalte aus dem Marketing in die Realität holen, denn ein Versprechen hält genauso lange, wie es niemandem wehtut.

Mehr unter:
https://voge.ly/vglF9J3/

Autor:
Alexander Siegert