bm
bank und markt

54. Jahrgang | Fritz Knapp Verlag | die-digitale-bank.de

11

15. November 2025

DIE DIGITALE BANK

Digitaler Sonderdruck

TECHNOLOGIE IM BANKING

Cloud-Strategie – europäische Souveränität statt US-Abhängigkeit

Björn Berg

Foto: AdobeStock/MdNazim

Cloud-Strategie – europäische Souveränität statt US-Abhängigkeit

Von Björn Berg

Foto: Brian Penny auf Pixabay

Die Cloud bildet das Rückgrat der modernen digitalen Finanzwelt – und ist Achillesferse zugleich. Denn sie macht Finanzinstitute zunehmend abhängig von großen US-Hyperscalern wie Amazon, Google oder Microsoft. Geopolitische Risiken, regulatorische Vorgaben und steigende Preise treiben die Institute nun dazu, über Alternativen nachzudenken und europäische Partner in den Blick zu nehmen. Gute Anbieter gibt es längst. Doch zum Durchbruch fehlt laut Björn Berg noch der Schulterschluss der Branche. Red.

„Wir wollen ein digital souveränes Deutschland." So steht es im aktuellen Koalitionsvertrag. Dies betrifft nicht nur Politik und Wirtschaft im Allgemeinen, sondern ist auch für Banken und Kapitalverwaltungsgesellschaften von Bedeutung. Denn digitale Souveränität bedeutet, die Kontrolle über Daten und Infrastruktur zu behalten, statt sie internationalen Anbietern zu überlassen.

Im Zentrum steht dabei die Cloud. Sie ist Motor und Risiko zugleich: Einerseits ermöglicht sie schnelle Innovation und skalierbare Services, andererseits schafft sie ein Abhängigkeitsverhältnis. Und genau dieses Abhängigkeitsverhältnis wird zunehmend kritisch gesehen – insbesondere, da die Dominanz der US-amerikanischen Hyperscaler Amazon Web Services (AWS), Microsoft Azure und Google Cloud immer spürbarer wird und Fragen bezüglich Regulierung, Datenschutz, Kosten und Kontrolle aufwirft.

Vor allem der im Jahr 2018 verabschiedete US Cloud Act zwingt Finanzinstitute dazu, ihre Strategien zu überdenken. Das Gesetz erlaubt es US-Behörden, auf Daten zuzugreifen, die von amerikanischen Unternehmen gespeichert oder verarbeitet werden – unabhängig davon, in welchem Land sich die Server befinden. Selbst Daten in deutschen Rechenzentren können davon betroffen sein. Für Unternehmen bedeutet dies ein unkalkulierbares Risiko, da sie vom Goodwill der US-Politik abhängig sind.

Dass geopolitische Konflikte unmittelbare und auch drastische Auswirkungen auf den Finanzsektor haben können, zeigte sich am Beispiel der Amsterdam Trade Bank (ATB): Das Amtsgericht Amsterdam erklärte die Bank im April 2022 für insolvent, nachdem sie aufgrund von Sanktionen gegen ihre russische Eigentümergruppe zeitweise von internationalen Zahlungsinfrastrukturen abgeschnitten war. Die ATB zählte vor der Insolvenz rund 23 000 Privatkunden, von denen knapp 6 000 ihren Wohnsitz in Deutschland hatten. Der Fall zeigt, dass Eigentümer- und Sanktionsrisiken den Zugang zu Zahlungsverkehr und Marktinfrastrukturen abrupt kappen können.

Parallel dazu erhöhen europäische Vorschriften wie der Digital Operational Resilience Act (DORA), die Network and Information Security Directive 2 (NIS2), die Leitlinien der Europäischen Bankenaufsichtsbehörde zu Outsourcing-Vereinbarungen und der EU AI Act den Druck. Sie verlangen, dass kritische Funktionen auch bei Ausfällen Dritter aufrechterhalten werden können. Viele Finanzinstitute behandeln dieses Thema noch stiefmütterlich, dabei ist klar: Resilienz ist keine Option mehr, sondern eine regulatorische Pflicht.

Schwachstellen der Hyperscaler-Abhängigkeit

Neben geopolitischen Risiken nimmt auch die technische und organisa-

Foto: Cofinpro

Björn Berg, Senior Manager,
Cofinpro AG,
Frankfurt am Main

torische Komplexität zu. Multi-Cloud-Umgebungen, die Public-Cloud-Dienste, Private-Cloud- und On-Premises-Lösungen kombinieren, erfordern ein aufwendiges Governance- und Architekturmanagement. Außerdem kämpfen die Nutzer mit Performance-Problemen bei großen Workloads, Schwankungen in Hochlastphasen und inkonsistenter Echtzeitverarbeitung.

Hinzu kommen die Sicherheitsrisiken: Selbst etablierte Cloud-Betreiber verzeichnen regelmäßig Vorfälle. So wurde beispielsweise im Jahr 2023 bei Microsoft ein Master Signing Key gestohlen, wodurch Angreifer Zugriff auf Regierungs- und Unternehmensdaten erhielten (siehe Kasten). Dieser Vorfall verdeutlicht die Gefahren einer systemischen Abhängigkeit. Proprietäre Technologien erhöhen zudem das Risiko sogenannter Vendor-Lock-ins, also der Bindung an einen Anbieter.

Auf regulatorischer Ebene wird diesen Gefahren zunehmend entgegengewirkt. Sowohl DORA als auch der EU AI Act schreiben eine resiliente Sicherheitsarchitektur, dokumentierte Ausstiegsstrategien sowie umfassende Nachvollziehbarkeit vor – also genau jene Bausteine, die eine souveräne Cloud-Strategie ausmachen. Vor diesem Hintergrund gewinnen rechtliche Unsicherheiten beim transatlantischen Datentransfer an Brisanz, während die europäische Datenhoheit zu einem strategischen Imperativ wird.

Europäische Alternativen gewinnen an Profil

Europäische Anbieter haben auf die jüngsten Turbulenzen reagiert und befinden sich nun im Aufbruch. Unter anderem positionieren sich:

OVHcloud (Frankreich): Marktführer in Europa, mit Fokus auf EU-Datenhoheit, breiter Produktpalette und zertifizierten Sicherheitsarchitekturen.

Open Telekom Cloud (Deutsche Telekom, Deutschland): Einer der europäischen Benchmark-Leader für Souveränität und Compliance, beliebt in regulierten Branchen.

Stackit (Schwarz Gruppe, Deutschland): Innovative hyperscalefähige Cloud-Lösung mit starker Präsenz im Handel und in der Industrie.

IONOS (Deutschland): Auch als IONOS Cloud bekannt, bietet skalierbare Lösungen, klare Preismodelle und garantiertes EU-Hosting.

Scaleway (Frankreich): Starke Entwicklerorientierung, vollständige EU-Datenhoheit, hohe Innovationsdynamik bei KI-, Serverless- und Kubernetes-Lösungen.

Cleura (Schweden): Managed Cloud- und Infrastrukturservices, mit Fokus auf Datenschutz und Nutzung ausschließlich in Europa ansässiger Rechenzentren.

Sie alle setzen auf offene Standards und Technologien wie die Containerisierung, um Handlungsfreiheit zu gewährleisten. Doch der Markt bleibt fragmentiert. Nationale Anbieter arbeiten noch zu wenig zusammen, sodass Europa bei Serverless-Architekturen oder KI-Diensten hinterherhinkt. Initiativen wie Gaia-X, eine europäische Initiative zur Schaffung einer offenen, vernetzten und vertrauenswürdigen Cloud- und Dateninfrastruktur, sowie der künftige EUCS-Standard (European Cloud Services Standard) sollen die Interoperabilität und das Vertrauen stärken. Dieser Prozess wird nicht nur in Deutschland, sondern auch in Frankreich, den Niederlanden und Skandinavien zunehmend politisch gefördert.

Das Ziel der Finanzindustrie sollte darin bestehen, ihre Systeme portierbar zu gestalten und das Risiko von Vendor-Lock-ins zu minimieren. Ein vielversprechender Ansatz ist der Einsatz Cloud-agnostischer Architekturen, da diese Migration und Flexibilität ermöglichen. Container-Technologien wie Kubernetes oder Docker erlauben den plattformunabhängigen Betrieb von Anwendungen. Infrastructure as Code (IaC) automatisiert die Bereitstellung und Migration von Workloads und reduziert Abhängigkeiten zusätzlich.

Zentral ist dabei eine konsequente Multi-Cloud-Strategie, bei der Daten und Services über mehrere Anbieter verteilt werden, um Ausfallsicherheit zu gewährleisten. Ebenso entscheidend sind regelmäßige Datenreplikationen und On-Premises-Fallbacks, um im Krisenfall handlungsfähig zu bleiben. Viele Banken haben diesen Schritt allerdings noch nicht vollzogen: Sie betreiben Multi-Cloud oft lediglich nominell, ohne echte Redundanz zu schaffen.

US-Anbieter: Defizite bei Kostentransparenz

Trotz detaillierter Kostenaufstellungen und persönlicher Ansprechpartner bei den großen US-Anbietern bleibt die Preisstruktur für Finanzinstitute oft komplex und schwer vorhersehbar. Ein Beispiel: Microsoft kündigte im März 2024 eine kurzfristige Preisanpassung von bis zu 11 Prozent für Cloud-Produkte in Europa an, ohne eine ausreichende Begründung oder Vorlaufzeit zu nennen. Insgesamt ist die Preisstruktur vieler Hyperscaler undurchsichtig. Verschärft wird diese Problematik durch die geplante EU-Digitalsteuer, die transatlantische Cloud-Dienste zusätzlich verteuern könnte.

Der Microsoft-Master-Key-Vorfall

Beim Master-Signing-Key-Vorfall nutzten Angreifer einen gestohlenen Signaturschlüssel, um Zugriff auf E-Mail-Konten von US-Behörden und Unternehmen zu erlangen. Aufgrund einer internen Fehlkonfiguration konnte der Schlüssel auch für Unternehmens-Tokens verwendet werden – ein gravierender Architekturfehler. Microsoft veröffentlichte erste Untersuchungsergebnisse am 11. Juli 2023 und erklärte die Analyse am 6. September 2023 für abgeschlossen. Rückwirkend wurden unautorisierte Zugriffe ab Mitte Mai 2023 nachgewiesen. Die Aufarbeitung wurde durch fehlende Logdaten erschwert, was Fragen zur Transparenz und Sicherheitskultur aufwarf. Kritisiert wurde vor allem die späte und unvollständige Information der Kunden – erst Wochen später wurde bekannt, dass auch Azure-Dienste betroffen sein konnten, sofern sie dem kompromittierten Schlüssel vertrauten.

Europäische Anbieter setzen dagegen häufig auf pauschalierte oder planbare Preismodelle, die Budgetsicherheit gewährleisten. Besonders bei stabilen Workloads sind sie wettbewerbsfähig, auch wenn ihr Portfolio an Zusatzservices eingeschränkter ausfällt. Für eine fundierte Entscheidung ist jedoch vollständige Transparenz unerlässlich, denn nur eine realistische Betrachtung der Total Cost of Ownership – einschließlich Personal-, Sicherheits- und Governance-Aufwand – ermöglicht eine verlässliche Kosteneinschätzung.

Europas Weg zur Cloud-Souveränität

Angesichts dieser vielschichtigen Herausforderungen wird deutlich, dass europäische Banken Cloud-Infrastrukturen benötigen, die technologisch leistungsfähig, regulatorisch konform und strategisch unabhängig sind. Der Weg dorthin erfordert eine koordinierte Transformation, die alle Akteure einbindet und Standards harmonisiert:

Finanzinstitute müssen ihre Souveränität aktiv gestalten. Sie sollten Pilotprojekte mit europäischen Anbietern initiieren und Erfahrungen austauschen, anstatt auf regulatorischen Druck zu warten. Nur gemeinsames Handeln schafft Marktmacht und Glaubwürdigkeit.

Europäische Cloud-Anbieter müssen kundenorientierter und zugänglicher werden. Entscheidend ist es, Angebote zu schaffen, die sich am Vorbild amerikanischer Plattformen orientieren, eine einfache Buchung ermöglichen und niedrige Einstiegshürden aufweisen. OVHcloud zeigt, dass dies gelingen kann: mit klaren Preismodellen, hoher Transparenz und konsequenter europäischer Compliance.

Die Politik kann Anreize setzen und Rahmenbedingungen schaffen, beispielsweise durch die Förderung gemeinsamer Standards und Zertifizierungen. Die eigentliche Verantwortung liegt jedoch bei Wirtschaft und Finanzsektor, denn Souveränität entsteht nicht durch Regulierung, sondern durch Kooperation.

Zahlreiche Projekte treiben aktuell die Implementierung europäischer Cloud-Dienste voran. Auf der Sicherheitsebene entwickelt die ENISA (European Union Agency for Cybersecurity) mit dem EUCS (European Cybersecurity Certification Scheme for Cloud Services) derzeit ein einheitliches Sicherheitszertifikat. Dieses soll Cloud-Dienste anhand abgestufter Vertrauensniveaus vergleichbar machen und Planungssicherheit für Beschaffung und Aufsicht bieten. Parallel dazu arbeitet Europa im Rahmen des IPCEI-CIS (Important Project of Common European Interest – Cloud Infrastructure & Services) mit der Initiative „8ra" an einem Cloud-Edge-Kontinuum auf Basis offener Standards. Das Ziel ist ein vernetztes Ökosystem aus Cloud-Ressourcen und Edge-Knoten quer durch die EU, für das bis 2030 eine Roadmap erstellt werden soll.

Die Vision einer souveränen europäischen Cloud-Infrastruktur nimmt damit zunehmend konkrete Formen an. Dennoch fehlt es weiterhin an übergreifender Zusammenarbeit und einheitlichen Standards. Die US-Hyperscaler haben es früh verstanden, Standards zu setzen und geschlossene Ökosysteme aufzubauen. Genau diese Geschlossenheit muss Europa nun nachholen. Fragmentierte nationale Lösungen reichen nicht aus, erforderlich ist eine koordinierte europäische Antwort.

Branchenweiter Schulterschluss ist notwendig

Entscheidend für den Erfolg ist es, eine kritische Masse zu erreichen. Solange nur einzelne Institute europäische Cloud-Dienste nutzen, bleibt der Markt zersplittert und die Anbieter können die notwendige Skalierung nicht erreichen. Erst wenn eine substanzielle Anzahl von Banken diesen Schritt gemeinsam geht, entsteht eine Marktdynamik, die Innovationen beschleunigt, Preise stabilisiert und die Entwicklung fortschrittlicher Services wie KI- und Serverless-Architekturen vorantreibt.

Hierfür ist ein Schulterschluss zwischen Finanzinstituten, Anbietern und Politik unverzichtbar. Die Finanzinstitute müssen bereit sein, ihre Komfortzone zu verlassen und aktiv in europäische Alternativen zu investieren – gerne aus Idealismus, alternativ aus strategischem Kalkül. Die Anbieter müssen Interoperabilität gewährleisten und ihre Services konsequent auf die Bedürfnisse regulierter Branchen ausrichten. Und die Politik muss verlässliche Rahmenbedingungen schaffen, ohne in Überregulierung zu verfallen.

Erst durch diese orchestrierte Zusammenarbeit kann Europa eine Cloud-Infrastruktur etablieren, die regulatorisch wegweisend, technisch konkurrenzfähig und strategisch unabhängig ist – eine Lösung, mit der Institute, Kunden und Aufsichtsbehörden gleichermaßen zufrieden sind. Die Zeit des Abwartens ist vorbei. Wer jetzt handelt, gestaltet Europas digitale Souveränität aktiv mit. Wer zögert, riskiert dauerhaft in Abhängigkeit zu verbleiben. ■