CLOUD COMPUTING

Digitale Souveränität im öffentlichen Sektor

CIO

SPONSORED BY OVHcloud

Auch der öffentliche Sektor setzt vermehrt auf die Vorteile von Cloud Computing. Die geopolitischen Entwicklungen zeigen, dass digitale Souveränität für IT-Verantwortliche in diesen Organisationen das wichtigste Kriterium bei der Providerwahl sein sollte. Dieses Whitepaper ist eine aktuelle Bestandsaufnahme des Themas und bietet Lösungen sowie konkrete Handlungsempfehlungen für IT-Entscheidungsträger in der öffentlichen Verwaltung.

Executive Summary

Cloud Computing hat sich auf breiter Front durchgesetzt. Laut einer Bitkom-Umfrage[1] wären 62 Prozent der deutschen Unternehmen ohne ihre Cloud-Dienste nicht mehr funktionsfähig. Auch für die öffentliche Verwaltung ist Cloud Computing inzwischen unverzichtbar. Bislang kommen vielerorts US-basierte Hyperscaler zum Einsatz, doch das wird wegen der geltenden Rechtslage zunehmend problematisch. Dabei stellen europäische Cloud-Provider eine echte Alternative dar. Sie erfüllen alle Anforderungen hinsichtlich des europäischen und deutschen Datenschutzes, sind zumeist günstiger, verursachen keinen Vendor Lock-in und bieten langfristige Planungssicherheit.

Erfahren Sie in vier Punkten worauf die CIOs von öffentlichen Einrichtungen und Behörden unbedingt achten müssen, damit sie einerseits die vielen Vorteile des Cloud-Computings nutzen können, ohne andererseits das Risiko eines Datenmissbrauchs durch fremde Regierungen zu riskieren.

Einleitung

Die neue Wirtschaftspolitik der USA hat zur Folge, dass sich viele deutsche Cloud-Anwender nach Alternativen außerhalb der USA umsehen. In einem Gartner-Bericht[2] heißt es dazu: „Verschärfte Datenschutzbestimmungen und geopolitische Spannungen treiben die Nachfrage nach souveränen Cloud-Diensten voran. Unternehmen werden zunehmend aufgefordert, Daten, Infrastruktur und kritische Workloads vor der Kontrolle durch externe Jurisdiktionen und dem Zugriff ausländischer Regierungen zu schützen."

Dieses Whitepaper erläutert die aktuelle Situation, die potenziellen Konsequenzen und zeigt geeignete Lösungswege speziell für Behörden und öffentliche Einrichtungen auf.

IT im öffentlichen Sektor: Gefangen zwischen Wunsch und Wirklichkeit

Der öffentliche Sektor steht vor mehreren Herausforderungen: Er soll die Digitalisierung konsequent vorantreiben, denn man erwartet heute moderne und reibungslos funktionierende digitale Verwaltungsangebote. Das darf aber nicht zu Lasten des Datenschutzes, der Datensicherheit und der Compliance gehen. Hinzu kommen knappe Budgets und Ressourcen. Cloud Computing kann viele dieser Anforderungen sehr wirtschaftlich erfüllen. Doch es war lange zweifelhaft, ob öffentliche Einrichtungen überhaupt eine Public Cloud nutzen dürfen. Mit den jüngsten Regelungen wie NIS2[3] und dem Digital Operational Resilience Act (DORA[4]) sind die Anforderungen weiter gestiegen.

> Es gibt **keine Garantie** dafür, dass Microsoft EU-Daten nicht an die US-Regierung weitergibt.
>
> – **Anton Carniaux**,
> Chefjustiziar bei Microsoft Frankreich.

Jetzt muss genau belegt werden, wo die Daten gespeichert sind und wer darauf zugreifen darf.

Das Problem mit den Hyperscalern

Alle Daten in US-basierten Clouds unterliegen dem CLOUD Act[5] oder FISA 702[6]. Diese Regelungen erlauben amerikanischen Behörden den Zugriff auch dann, wenn die Daten physisch in Europa gespeichert sind. Das davon betroffene Unternehmen muss nicht einmal über einen solchen Datenzugriff informiert werden. In einer Anhörung[7] vor dem französischen Parlament sagte Microsofts Chefjustiziar Anton Carniaux jüngst unter Eid, dass es „keine Garantie dafür gibt, dass Microsoft EU-Daten nicht an die US-Regierung weitergibt“. Damit bestätigte er die Verunsicherung beim Einsatz von US-Cloud-Diensten. Befürchtet werden dabei nicht nur Datenübermittlungen, sondern auch aktive Maßnahmen, wie das Abschalten von Cloud-Diensten für die EU. Dass das im krassen Widerspruch zur DSGVO und zu speziellen Auflagen in vielen Branchen steht, ist offensichtlich.

Die Lösung: Souveräne Cloud aus Europa

Die europäischen IT-Chefs haben die Signale gehört. So sagen die Analysten von Gartner[2], dass bis 2029 die Hälfte aller Organisationen über digitale Souveränitätsstrategien verfügen werden – heute sind es weniger als zehn Prozent. „Unternehmen richten ihre Cloud-Strategien proaktiv an den Anforderungen digitaler Souveränität aus“, sagt Joe Rogus, Director Advisory bei Gartner. Vor allem die öffentlichen Einrichtungen erkennen inzwischen, dass digitale Souveränität keine theoretische Debatte ist, sondern eine strategische Notwendigkeit.

Wann ist eine Organisation „digital souverän“?

Digitale Souveränität besteht aus drei Ebenen: Datensouveränität, technischer Souveränität und operationaler Souveränität. Datensouveränität bedeutet, dass die Daten vor extraterritorialen Zugriffen geschützt sind. Technische Souveränität bezieht sich auf den physischen Ort der Datenspeicherung und -Verarbeitung. Hierzu gehört auch die Wahlfreiheit der Infrastruktur – also kein sogenanntes Vendor Lock-in, bei dem man nur schwer oder gar nicht die Plattform wechseln kann. Die operative Souveränität umfasst zuletzt den Betriebsbereich: Wo sitzen die Support-Mitarbeiter – in Indien, China oder den USA?

Doch Vorsicht ist geboten: Nicht alles, was als „souverän“ angeboten wird, erfüllt die Auflagen. Große US-Anbieter behaupten beispielsweise, dass sie digitale Souveränität bieten – was aber nicht stimmt. In Anlehnung an das Wort Green-Washing hat sich dafür der Begriff „Souveränitäts-Washing“ etabliert. Das ist sehr gefährlich, weil es vortäuscht, dass die Anwender unabhängig und geschützt sind – während in Wahrheit weiterhin Abhängigkeiten und fremde Zugriffsrisiken bestehen. Besonders für kritische Infrastrukturen und öffentliche Verwaltungen ist das ein sehr ernstzunehmendes Thema.

Zertifizierungen: Der Unterbau der digitalen Souveränität

Um die Souveränitäts-Vorgaben teilweise mess- und nachvollziehbar zu machen, wurden detaillierte Vorgaben erstellt. So hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) einen umfangreichen Katalog[8] erstellt, in dem festgelegt ist, welche Kriterien ein Cloud-Provider

zu erfüllen hat, um nach dem aktuellen Stand der Technologie als sicher zu gelten. Der Kriterienkatalog heißt „C5“ (Cloud Computing Compliance Criteria Catalogue) und spezifiziert die Mindestanforderungen an ein sicheres Cloud Computing. Seit 2020 dürfen bei öffentlichen Einrichtungen und Behörden nur noch C5-geprüfte Provider zum Einsatz kommen.

GRAFIK: OVHCLOUD

OVHcloud: Europäischer Marktführer im Bereich Cloud Computing

Als Vorreiter im Bereich digitaler Souveränität und einer vertrauenswürdigen Cloud mit dem besten Preis-Leistungs-Verhältnis setzt OVHcloud[9] seit mehr als 20 Jahren auf ein integriertes Modell, mit dem es die volle Kontrolle über seine Wertschöpfungskette hat – von der Herstellung seiner eigenen Server über die Orchestrierung seines Glasfasernetzwerks mit einer Bandbreite von bis zu 20 Tbit/s bis hin zur Errichtung und Verwaltung seiner Rechenzentren.

OVHcloud ist offiziell beim BSI als Betreiber Kritischer Infrastrukturen (KRITIS) in Deutschland registriert. Damit erfüllt OVHcloud die Anforderungen des BSI an Unternehmen, deren Dienste von besonderer Bedeutung für das Gemeinwohl und die Versorgungssicherheit sind. Dies wiederum beinhaltet die Einführung und Aufrechterhaltung eines wirksamen Informationssicherheitsmanagementsystems (ISMS) oder auch physische und logische Zugangskontrollen zu Rechenzentren und Systemen. Die Nachweise und entsprechende Dokumentation müssen dem BSI alle zwei Jahre in einem Audit vorgelegt werden. Weitere „Prüfsiegel“[10] der OVHcloud sind u.a. die ISO 27001/27017/27018 und 27701-Zertifizierungen sowie der CSA Star (eine Selbstbewertung nach dem Verfahren der Cloud Security Alliance Level 1).

Die Public Cloud von OVHcloud basiert komplett auf Open-Source-Technologie – somit ist ein Vendor Lock-in ausgeschlossen. Sie wird ausschließlich in Europa gehostet und bietet den Kunden eine kompromisslose digitale Souveränität. Ganz neu bietet OVHcloud auch eine On-Premise-Cloud-Plattform[11] (OPCP) an. OPCP ist eine Privat-Cloud-Umgebung, die nach

BILDQUELLE: SHUTTERSTOCK.COM/DW LABS INCORPORATED

Vorgaben des Kunden konfiguriert ist und im Hoheitsbereich des Kunden betrieben wird. Das heißt, der Kunde bekommt die komplette Hard- und Software vorinstalliert geliefert – nur den Strom und das Internet muss er noch bereitstellen. Das Management der Infrastruktur kann durch OVHcloud, den Kunden oder einem Mix aus beiden erfolgen. Die Lösung wird bereits von der Luxemburgischen Post eingesetzt.

Namhafte Referenzen

OVHcloud ist als Anbieter im öffentlichen Sektor fest etabliert und kann auf viele erfolgreiche Kunden und Projekte als Referenz verweisen.

Ein Beispiel dafür, ist die Bundespolizei[12], die bei der Digitalisierung ihrer E-Learning-Angebote auf das Videokonferenzsystem Visavid der Auctores GmbH, und auf die hochsicheren Cloud-Dienste von OVHcloud setzt. Auctores ist spezialisiert auf digitale Kommunikationslösungen für Behörden, Bildungseinrichtungen und Unternehmen. Mit Visavid betreibt der OVHcloud-Partner eines der wenigen vollständig DSGVO-konformen Videokonferenzsysteme aus Deutschland. Das Ergebnis ist eine datenschutz-konforme, leistungsfähige und zukunftssichere Lösung, die exakt auf die besonderen Anforderungen von Bundesbehörden zugeschnitten ist. Der Hostingauftrag

wurde im Mai 2025 vom Beschaffungsamt des Bundesministeriums des Innern für eine Laufzeit von fünf Jahren vergeben. „Durch unsere ausgereifte Softwarelösung Visavid sowie der Unterstützung unseres Rechenzentrumspartners OVHcloud können wir unserem neuen Kunden eine erstklassige Lösung für dessen Anforderungen bieten“, sagt Daniel Hausner, Projektverantwortlicher für Visavid bei Auctores.

> **Durch unsere ausgereifte Softwarelösung Visavid** sowie der Unterstützung unseres Rechenzentrumspartners OVHcloud können wir unserem neuen Kunden eine erstklassige Lösung für dessen Anforderungen bieten.
>
> – **Daniel Hausner**,
> Projektverantwortlicher für Visavid bei Auctores.

Ein weiterer Kunde aus dem öffentlichen Sektor ist die Bundesagentur für Arbeit (BA). Zusammen mit der Deutschen Rentenversicherung (DRV) und der Deutschen Gesetzlichen Unfallversicherung (DGUV) hat sie einen Auftrag für eine Multi-Cloud-Plattform[13] an die Computacenter AG vergeben. Über diese Plattform erhalten die drei Sozialversicherungsträger Zugriff zu Cloud Services von unterschiedlichen Anbietern, darunter auch zu den Services von OVHcloud.

In die Cloud? – Aber sicher!

IT-Verantwortliche in Behörden und öffentlichen Einrichtungen sollten bei ihrer Cloud-Lösung auf diese vier Punkte achten.

1. Digitale Souveränität: Erfüllt der Cloud-Provider diese auf allen drei Souveränitäts-Ebenen?

2. Datenflüsse und Risiken: Welche Daten werden aktuell in ausländischen, insbesondere US-basierten Cloud- und SaaS-Diensten verarbeitet? – Ist das rechtskonform?

3. Hybride Infrastruktur: Der parallele Betrieb von Cloud und On-Prem optimiert die Infrastruktur. – Verletzt eventuell aber die DSGVO oder Compliance-Auflagen.

4. Transparenz und Compliance: die lückenlose Dokumentation der Speicherorte, Zugriffe und Schutzmaßnahmen ist Pflicht, nur so lässt sich nachweisen, dass NIS2, DORA und andere Vorgaben eingehalten werden.

Über OVHcloud

OVHcloud ist ein Global Player im Cloud-Segment und europäischer Marktführer in diesem Bereich. Das Unternehmen betreibt mehr als 450.000 Server in über 40 Rechenzentren auf 4 Kontinenten und bedient 1,6 Millionen Kund:innen in mehr als 140 Ländern.

Als Vorreiter im Bereich der vertrauenswürdigen Cloud und Pionier der nachhaltigen Cloud mit dem besten Preis-Leistungs-Verhältnis setzt das Unternehmen seit mehr als 20 Jahren auf ein integriertes Modell, mit dem es die volle Kontrolle über seine Wertschöpfungskette hat – von der Konzeption seiner eigenen Server über die Orchestrierung seines Glasfasernetzwerks bis hin zur Errichtung und Verwaltung seiner Rechenzentren. Dieser einzigartige Ansatz ermöglicht es OVHcloud nicht nur, alle Verwendungszwecke seiner Kund:innen unabhängig abzudecken, sondern ihnen auch die Vorteile eines umweltverträglichen Modells mit sparsamem Ressourceneinsatz und einem CO_2-Fußabdruck zu bieten, der die besten Werte der Branche erreicht. Heute bietet OVHcloud hochmoderne Lösungen an, die starke Leistung, vorhersehbare Preise und vollkommene Datensouveränität vereinen, um das ungehinderte Wachstum seiner Kund:innen zu unterstützen.

Weitere Informationen über OVHcloud finden Sie hier

Quellen-nachweis

1 Wirtschaft ruft nach einer deutschen Cloud
2 Gartner Identifies the Top Trends Shaping the Future of Cloud
3 NIS2 Directive: securing network and information systems
4 https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
5 Clarifying Lawful Overseas Use of Data Act
6 Erklärungen und Hintergrundinformationen zu FISA Section 702
7 Audition de MM. Anton Carniaux, directeur des affaires publiques et juridiques, et Pierre Lagarde, directeur technique du secteur public, de Microsoft France
8 Kriterienkatalog C5
9 OVHcloud
10 OVHCloud: Compliance und Zertifizierungen
11 On-Prem Cloud Platform
12 Bundespolizei setzt auf Visavid für sicheres E-Learning
13 OVHcloud bringt öffentliche Verwaltung in die Cloud