Unterstützt von Capgemini

iX extra April 2023
Cloud

Eine Sonderveröffentlichung der Heise Medien GmbH & Co. KG

Souveräne europäische Clouds

iX extra zum Nachschlagen:
www.ix.de/extra

Souveräne europäische Hyperscaler-Alternativen

Das Thema digitale Souveränität als Hype abzutun, gefährdet schlimmstenfalls die Existenz des eigenen Unternehmens. Wer die Vorteile der Cloud nutzen möchte, ohne die Kontrolle über seine Daten komplett aufzugeben, muss besonnen agieren und gut informiert sein.

Wer die Dienste eines Cloud-Providers nutzt, tritt die Herrschaft über die eigenen Daten immer ab – zumindest bis zu einem gewissen Grad. Technisch ist das anders nicht möglich. Umso wichtiger ist es für Unternehmen wie Behörden, sich Gedanken zu machen, wem sie zumindest einen Teil ihrer Daten überantworten und was das bedeutet, falls eine einst gut funktionierende Partnerschaft mit einem Lieferanten aus welchen Gründen auch immer in die Brüche geht. Dabei spielt auch die Politik eine Rolle: Welche Gerichtsstände sind vereinbart, welche internationalen Gesetze spielen eine Rolle, welche Fallback-Mechanismen existieren und wie lassen sich Probleme möglichst a priori vermeiden?

Genau das steckt hinter dem Schlagwort der digitalen Souveränität. Es beschreibt die grundlegenden Probleme des Cloud-Ansatzes und macht Vorschläge, wie sich ein hoher Grad an Souveränität trotz der Nutzung von Diensten Dritter erhalten lässt. iX stellt vor, worauf Unternehmen und Behörden achten müssen und welche Anbieter am Markt existieren, die mit souveränen Angeboten um die Gunst der Nutzer buhlen.

Der Weg in die Cloud

Die Welt ist in den vergangenen Jahren ein gutes Stück komplizierter geworden. Für quasi in Stein gemeißelt gehaltene politische Grundsätze stellen sich als doch nicht so zuverlässig heraus. In Europa tobt ein blutiger Angriffskrieg, und vermeintlich längst zugeschüttete politische Gräben entpuppen sich nicht nur als noch immer existent, sondern als tiefer denn je. Das hat freilich Auswirkungen auch auf die digitale Welt. Während manche die Realität bis heute in analog und digital einteilen, verschwimmen die Grenzen gerade bei jüngeren Generationen. Digitale Dienste, sei es zur Kommunikation, zum Austausch von Dokumenten oder für nahezu jede andere Aufgabe, nehmen in der Geschäftswelt der Gegenwart wie im Privatleben vieler Menschen heute einen zentralen Platz ein. Für den Einzelnen kommt es dabei gar nicht so sehr darauf an, wie oder warum die genutzten digitalen Dienste genau funktionieren – solange sie eben funktionieren.

Der unkomplizierten Nutzung von IT-Diensten entgegen steht die Tatsache, dass diese auf der technischen Seite irgendwie umgesetzt sein wollen. Hier hat in den vergangenen Jahren das Cloud-Computing Fakten geschaffen. Ohne AWS, GCP und Azure, also die großen US-Hyperscaler, wäre das Netz in unseren Breitengraden heute nicht das, was es eben ist. Andernorts gibt es diesen Effekt ebenso. Der chinesische Cloud-Anbieter Alibaba gehört heute zu den größten und zugleich wertvollsten IT-Unternehmen der Welt. Wohin man also auch schaut: Die Cloud ist aus dem Alltag der Menschen kaum wegzudenken.

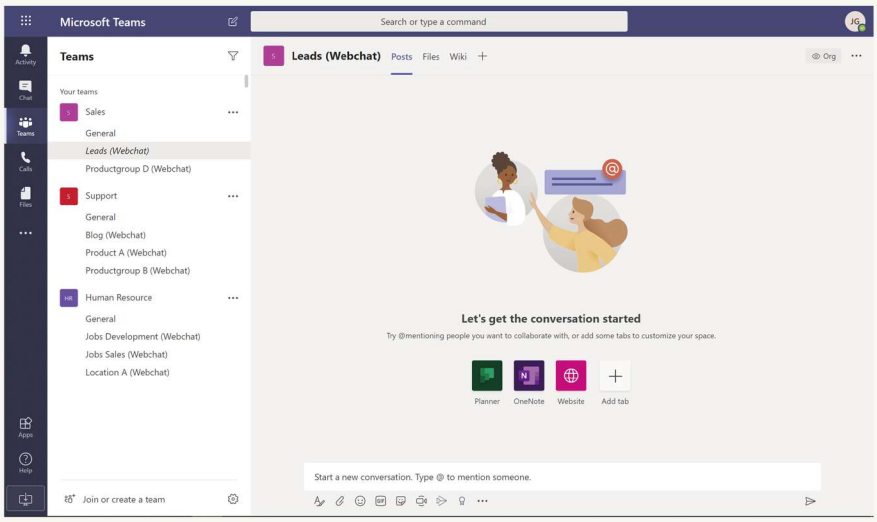
Bessere Technik, aber weniger Budget

Für Unternehmen einerseits, andererseits aber auch für Behörden und Bürger geht das mit handfesten Herausforderungen einher. Weder Unternehmen noch Behörden kommen heute ohne digitale Dienste zurecht. Dass jede Firma heute irgendwie auch eine IT-Firma ist, ist längst bekannt, und ohne Computer und EDV könnten auch Behörden auf allen Ebenen die anliegende Arbeitslast realistisch nicht mehr stemmen.

Wie aber erfolgt die Nutzung digitaler Dienste sinnvoll, und was bedeutet „sinnvoll“ eigentlich? In der Vergangenheit war die Antwort auf diese Frage meist recht eindeutig: Fast immer ging es darum, irgendwo eigene Infrastruktur zu betreiben oder betreiben zu lassen, zum Teil bis hinunter auf die Gemeindeebene. Obwohl Villa Riba und Villa Bajo also direkt nebeneinanderliegen, konnte es vorkommen, dass beide ihre digitalen Agenden völlig unabhängig voneinander abwickelten, dabei auf andere Anbieter setzten und zum Teil auch völlig unterschiedliche Preise bezahlten. Dasselbe Prinzip ist in der freien Wirtschaft ohnehin normal, hier steht es schließlich jedem Anbieter frei, mit jedem potenziellen Kunden freie Vertragsverhältnisse auszumachen.

Das Problem dabei: Der Betrieb eigener IT-Infrastruktur ist teuer. Und die Dienstleister, die mit ihren Angeboten bei Firmen wie Behörden auf Kundenfang gingen, strichen für ihre Arbeit viel Geld ein. Vielerorts sind Lösungen, die vor 15 und mehr Jahren installiert worden sind, noch immer im Einsatz und verschlingen nicht zuletzt durch mehrfach künstlich verlängerte Supportverträge riesige Summen – so viel Geld, dass mancherorts aus der IT einer Kommune ein Politikum wird.

Was erschwerend hinzukommt: Heute muss die digitale Infrastruktur von Firmen wie von Unternehmen viel mehr leisten und viel besser funktionieren als früher. Corona hat deutlich gemacht, dass gute Systeme für



Quelle: Microsoft

Dienste wie Microsoft Teams sind schnell ausgerollt und in Betrieb genommen, doch entstehen hier Abhängigkeiten in mehrere Richtungen, die digitaler Souveränität im Wege stehen (Abb. 1).

Videotelefonie heute ein Muss sind, keine nette Ergänzung. Sollen Schulen in Deutschland in Sachen Digitalisierung vorankommen, brauchen sie bessere Systeme für das digitale Lernen und so weiter – die Liste lässt sich beliebig fortführen. Und während der erwartete Featureumfang digitaler Dienste immer größer wird, steht immer weniger Geld dafür zur Verfügung. Es ist keinesfalls ungewöhnlich, dass Kunden heute in Verhandlungen mit ihrem IT-Dienstleister gehen, die einen Budget-Cut von 25 Prozent pro Jahr und mehr vorsehen. Schließlich sei Automatisierung ja Standard und überhaupt habe die immer weiter um sich greifende Standardisierung und Automatisierung dafür gesorgt, dass der Betrieb von IT-Infrastruktur heute leichter und billiger sei als vor zehn Jahren.

Sichere Datenspeicher aus der Cloud

Anbieter	Produkt	URL
doubleSlash	Business Filemanager	www.business-filemanager.de/softwareloesung/
DRACOON	DRACOON	page.dracoon.com/sichere-cloud
Dropbox	Dropbox Business	www.dropbox.com/business
DSwiss	SecureSafe	www.securesafe.com/de/geschaeftskunden/uebersicht
idgard	virtueller Datenraum	www.idgard.com/de/produkt/datenraum
leitzcloud by vBoxx	leitzcloud	leitz-cloud.com/funktionen
Nextcloud	Nextcloud Enterprise	nextcloud.com/de/enterprise/
ownCloud	ownCloud.online	owncloud.online/
pCloud	pCloud	www.pcloud.com/de/
Strato	HiDrive Business	www.strato.de/cloud-speicher/hidrive-business/
TeamDrive	Secure Office	teamdrive.com/komponenten#secure
Telekom	MagentaCLOUD	cloud.telekom-dienste.de/
Tresorit	Tresorit Enterprise	tresorit.com/de/enterprise
Your Secure Cloud	Your Secure Cloud	www.yoursecurecloud.de/geschaeftskunden/features.html

Die Cloud als Allheilmittel?

Hier laufen die beiden Diskussionsfäden dieses Artikels zusammen. Denn ein zentrales Versprechen der Cloud-Anbieter war und ist es, den Kunden Ersparnisse durch Automation und Standardisierung zu ermöglichen. Der Deal geht in etwa so: Weil AWS, Azure, GCP und die vielen anderen Anbieter alles automatisieren, profitieren sie massiv von der „Economy of Scale“. Es genügt, ein Produkt einmal teuer zu entwickeln, um es danach beliebig oft nicht gar so teuer weiterzuverkaufen – irgendwann ist der Break Even erreicht, und ab da druckt das jeweilige Produkt quasi Geld für den Anbieter.

Das funktioniert zudem auf allen Ebenen. Ganz gleich, ob Infrastructure as a Service – also virtuelle Instanzen zum Einmieten, in denen Kunden ihre Produkte selbst betreiben – oder Platform as a Service / Software as a Service: Immer soll die Herstellung eines durch den Kunden nutzbaren Produktes in der Cloud so günstig sein, dass er dasselbe Produkt selbst für dasselbe Geld nicht herstellen kann. Kunden haben so weniger Arbeit, zahlen geringere Preise und kriegen insgesamt eine deutlich bessere Dienstleistung, während der Anbieter der Lösung im Geld schwimmt.

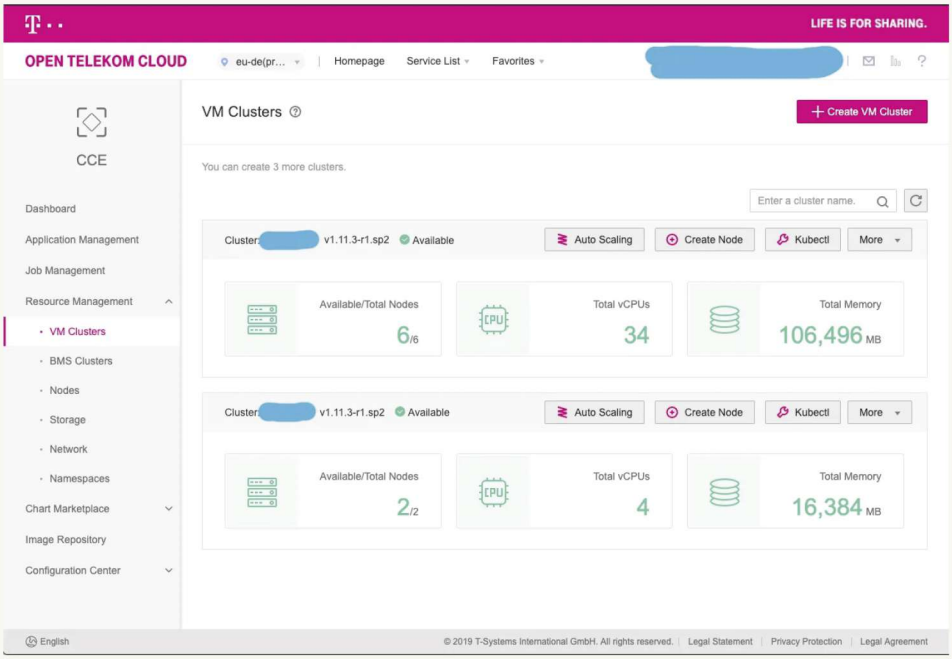
Rechtliche Bedenken

Das funktioniert aber nur, solange grundlegende rechtliche und politische Themen zwischen allen Beteiligten einvernehmlich gelöst sind und bleiben. Und weil digitale Dienste heute Teil des Alltags sind, kommen geopolitische Themen oder nationale Interessen schneller ins Spiel, als es manchem lieb ist.

Ein einfaches Beispiel macht das schnell deutlich. Das Thema Datenschutz spielt innerhalb der Europäischen Union eine große Rolle. Die Mitglieder der EU haben sich deshalb auf die DSGVO geeinigt, die die zentralen Prinzipien des Datenschutzes in der EU definiert. In anderen Rechtsräumen gelten andere Regeln, in den USA beispielsweise der CLOUD Act. Der aber steht der DSGVO diametral entgegen – denn der CLOUD Act verpflichtet US-Firmen, US-Ermittlern Zugriff auf Daten einzuräumen, selbst wenn diese außerhalb der USA liegen, die entsprechenden Maschinen aber einem US-Unternehmen gehören. Wer Dienste von Azure, GCP und Co. nutzt, befindet sich mithin rechtlich zumindest in einer Grauzone, denn die DSGVO bleibt trotzdem gültig. Zwar gibt es eine theoretische Hintertür: Betroffene Länder können mit den USA ein bilaterales Abkommen

Souveräne Clouds auch für den öffentlichen Sektor

Anbieter	Produkt	URL	Anmerkungen
ACI	ASP by ACI	aci-edv.de/cloud-loesungen	für Steuerberater, Rechtsanwälte und KMU, eigenes RZ in Hamburg
arvato Systems	souveräne Cloud-Plattform für den öffentlichen Sektor	www.arvato-systems.de/branchen/branchen-im-ueberblick/oeffentlicher-sektor/souveraene-cloud-plattform-fuer-den-oeffentlichen-sektor	Azure als technische Basis, Kooperation mit SAP
Atos	OneCloud	atos.net/de/lp/verwaltungscloud	Open Source und Red Hat
Bechtle	Zukunftspakete Digitale Souveränität	www.bechtle.com/public-sector/digitale-souveraenitaet-loesungen-europa	Dienstleister, arbeitet mit IONOS und plusserver zusammen
Dataport	sichere Cloud-Services	www.dataport.de/was-wir-bewegen/thema/deutsche-verwaltungscloud/	Mitarbeit bei der deutschen Verwaltungscloud, eigene BSI-zertifizierte RZs
Delos	Delos Cloud	discover.sap.com/delos-cloud/de-de/index.html	SAP-Tochter, Testbetrieb
Hundertserver	Hundertserver Cloud	www.hundertserver.de/	Linux und Open Source
]init[	Private Cloud	www.init.de/thema/souveraene-verwaltungscloud	Dienstleister
METRO CLOUD Provider	Metro Cloud	metro-cloud.de/managed-cloud/	technische Basis: VMware HCI
noris network	noris Enterprise Cloud Private	www.noris.de/it-services/cloud-services/iaas/noris-enterprise-cloud-private-nec/	technische Basis: VMware HCI
noris network	Wavestack Cloud	www.noris.de/wacestack-cloud/	SCS-Basis, Betastadium
Oracle	Sovereign Cloud Regions for the EU	www.oracle.com/security/saas-security/data-sovereignty/european-union-restricted-access/	angekündigt, Verfügbarkeit 2023
STACKIT	STACKIT CLOUD	www.stackit.de/de/cloud/vorteile/	IaaS, PaaS, eigene RZs
T-Systems	Sovereign Cloud powered by Google Cloud	www.t-systems.com/de/de/cloud-services/managed-platform-services/souveraene-cloud/sovereign-cloud-powered-by-google-cloud	technische Basis Google Cloud in T-Systems-eigenen RZs



Quelle: T-Systems

Die Open Telekom Cloud von T-Systems basiert auf OpenStack-APIs und kommt als rein europäische Cloud daher, die Kunden Souveränität sowohl im technischen wie auch im rechtlichen Kontext erlaubt (Abb. 2).

eingehen, das für solche Fälle ein Einspruchsrecht vorsieht, doch ein solches Abkommen hat bisher nur Großbritannien geschlossen.

Für Firmen ist das bereits ein großes Problem – für Behörden oder andere öffentliche Einrichtungen wie Schulen ist der Zustand in Summe indiskutabel. Cloudbasierte Dienste wie MS Teams (Abbildung 1) oder Microsoft 365 dürfen deshalb in einigen Bundesländern in Schulen bereits nicht mehr zum Einsatz kommen – was groteskerweise dazu führt, dass etwa die Eltern betroffener Kinder ihre Wut an den jeweiligen Bildungseinrichtungen auslassen, diese gar als Digitalisierungsbremse und als unbelehrbar bezeichnen. Die Verantwortlichen in solchen Konstrukten können kaum gewinnen: Entweder verstoßen sie gegen geltendes Recht oder sie ziehen den Groll derer auf sich, denen Datenschutz nicht so wichtig ist und die lieber „Fortschritt first“ auf den Fahnen tragen.

Digitale Souveränität als Ausweg

Deshalb sollen öffentliche Initiativen von Bund, Ländern und zum Teil der Kommunen die Öffentlichkeit für die „digitale Souveränität“ sensibilisieren. Darunter versteht die Politik heute im Wesentlichen sämtliche Maßnahmen, die digitale Dienste in einzelnen Mitgliedsstaaten der Europäischen Union, besser aber noch unter den Regeln derselben ermöglichen – mit einheitlicher Rechtsgrundlage und erhöhten Garantien für alle Mitgliedsstaaten. Laut dem Beauftragen der Bundesregierung für Informationstechnik (Bundes-CIO) meint digitale Souveränität „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“ (siehe ix.de/zyem). Im Kontext digitaler Dienste mit Cloud-Bezug ist das, so schön es klingt, ein echtes Brett.

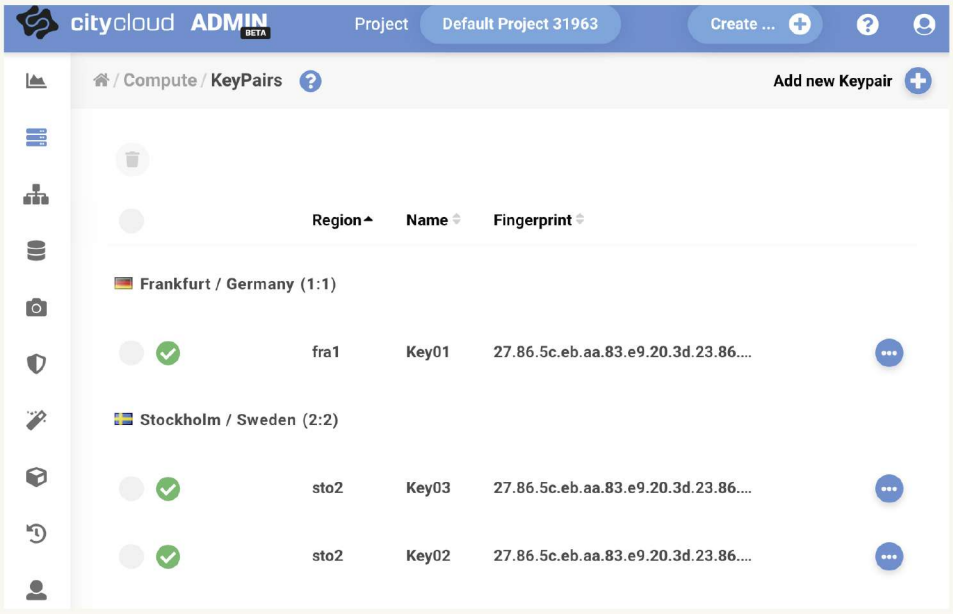
Es lohnt sich an dieser Stelle, zunächst einen genaueren Blick auf die Arten von Diensten zu werfen, die infrage kommen, und auf die Art und Weise, wie deren Nutzung die digitale Souveränität einer Firma oder einer Behörde möglicherweise einschränkt. Auch die Open Source Business Alliance (OSBA) befasst sich in ihrer Arbeitsgruppe Public Affairs ausgiebig mit dem Thema digitale Souveränität und hat Mindestanforderungen für Cloud-Angebote zusammengestellt (siehe ix.de/zyem).

Problem 1: Daten

Das erste Problem ist die Sicherheit von Daten mit Personenbezug, die zur Nutzung von Cloud-Diensten erhoben werden. Hier geht die Nutzung fremder Infrastruktur implizit immer damit einher, dass man die Kontrolle über die eigenen Daten zumindest zum Teil aufgibt. Gerade Institutionen und öffentliche Stellen können das aber eigentlich nur tun, wenn der um das Konstrukt herumgebaute rechtliche Rahmen absolut wasserdicht ist.

Hinzu kommt, dass die eigenen Daten in den falschen Händen zu einer realen Gefahr werden können. Ist es wirklich sinnvoll, dass Microsoft eine Liste sämtlicher Schüler einer Schule in Deutschland besitzt, da diese samt und sonders mit MS-Teams-Accounts ausgerüstet sind? Aus dem Bauch heraus würden diese Frage die meisten Beobachter wohl eher mit Nein beantworten. Digitale Souveränität muss die sie praktizierenden Unternehmen und Behörden also in die Lage versetzen, anhand geltender europäischer Rechtsstandards Daten so zu handhaben, dass sie nicht unfreiwillig an Dritte abfließen.

Zusätzlich spielt die Möglichkeit, auf die eigenen Daten zuzugreifen, eine bedeutsame



Quelle: Cleura

Cleura kommt aus Schweden und spielt damit nach den Regeln europäischer ISPs: Es verspricht Kunden souveräne und mit gängigen Compliancestandards kompatible Lösungen ohne Vendor Lock-in (Abb. 3).

Cloud-Transformation im Public Sector

Digitale Souveränität hat im Public Sector einen hohen Stellenwert. Das betrifft auch Cloud-Computing. Capgemini berät öffentliche Auftraggeber auf ihrem Weg zur souveränen Cloud.

Die Nutzung von Souveräner Cloud ist ein wirksamer Hebel für die digitale Transformation im Public Sector. Deshalb ziehen öffentliche Auftraggeber Technologieberater wie Capgemini als sogenannte Cloud Integratoren hinzu. Cloud Projekte beginnen oft mit der Beratung zur strategischen Auswahl von Cloud-Service-Providern und dem richtigen Cloud Deployment-Modell (Public, Private oder Multi Cloud). Die Unterstützung bei der Implementierung von Cloud-Services bis hin zum Betrieb ist eine weitere Kernaufgabe eines Cloud Integrators. So werden öffentliche Institutionen auf ihrem Weg zur Nutzung von Cloud-Lösungen begleitet.

Voraussetzungen für die Souveräne Public Cloud

Prinzipiell erfüllen die Public Clouds der Hyperscaler die meisten Anforderungen an Cloud-Souveränität. Doch außereuropäische Staaten können globale Cloud-Anbieter verpflichten, Daten von europäischen Kunden herauszugeben, ohne dass EU-Recht Anwendung findet. Provider, die in der EU ansässig sind und ausschließlich hier operieren, sind vor solchen Zugriffen geschützt. Deshalb stellen einige Hyperscaler ihre Technologie europäischen Partnern zur Verfügung, die als Treuhänder oder Betreiber der Plattform und aller Kundendaten auftreten. Daneben gibt es technologische Souveränitäts-Optionen, bei denen beispielsweise Organisationen ihre Clouddaten verschlüsseln und den dazugehörigen Schlüssel selbst verwalten. Auf diese Weise behalten sie ihre Datensouveränität in eigener Hand.

Cloud-Transformation zwischen Innovation und Souveränität

Cloud-Souveränität entsteht dann, wenn Cloud-Nutzung Kontrolle, Wahlmöglichkeiten und Autonomie über Daten, Systeme und Cloud Services erlaubt. Allein die nutzenden öffentlichen Institutionen bestimmen, wo Daten liegen, verarbeitet werden und wer darauf zugreift (Datensouveränität). Darüber hinaus können sie jederzeit nachvollziehen, ob die operative Nutzung von Cloud Services mit geltendem Recht und Regularien übereinstimmt und eine Betriebskontinuität gewährleistet ist (Operative Souveränität). Zuletzt bedeutet Souveränität, dass keine kritischen Abhängigkeiten zu Technologien eines Cloud-Providers bestehen und Workloads z. B. migrierbar sind (Technologische Souveränität).

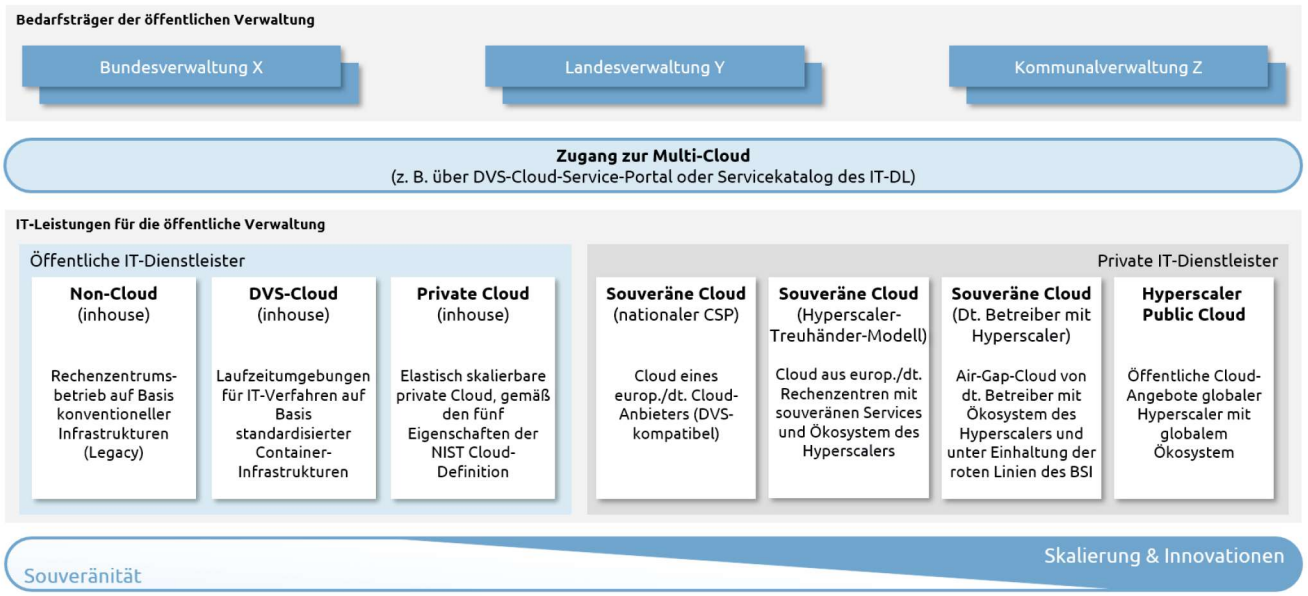
Hyperscaler entwickeln ihre Cloud-Angebote schnell weiter und erschließen neue Anwendungsfelder. Wurden Souveräne Cloud-Lösungen anfangs von Cloud-Providern aus der EU angeboten, arbeiten jetzt auch Hyperscaler an Angeboten zu Souveräner Cloud (siehe Infokasten). Im Wettbewerb zwischen europäischen Anbietern und den US-amerikanischen Hyperscalern entstehen Cloud-Angebote, die eine Balance zwischen Selbstbestimmung, Kontrolle und Modernisierung erlauben. Auch für den ökologisch nachhaltigen Einsatz von IT kann eine an den aktuellen Bedarf angepasste Nutzung von Cloud einen wesentlichen Beitrag leisten. Geliefert aus modernen Cloud-Rechenzentren kann der Einsatz von Public Cloud die IT öffentlicher Institutionen darin unterstützen, Vorgaben für Nachhaltigkeit und Klimaschutz zu erfüllen. Innovative Fachverfahren in der Cloud können Millionen Bürger*innen eine konkrete Erleichterung bieten: in der digitalen Kommunikation mit Behörden, bei der Digitalisierung des Schulunterrichts und bei zahlreichen anderen öffentlichen Dienstleistungen. Expert*innen von Capgemini tragen entscheidend dazu bei und gestalten die Digitalisierung maßgeblich mit.

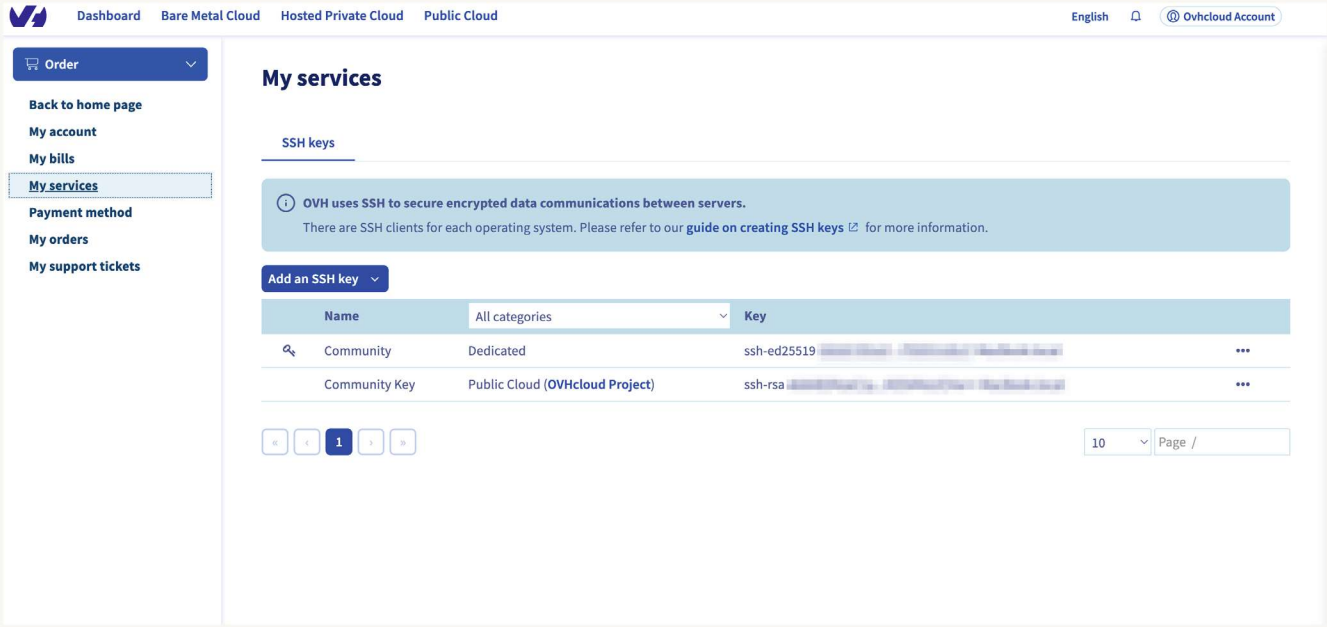
Cloud Integratoren arbeiten interdisziplinär

Cloud-Architekt*innen bei Capgemini beginnen eine digitale Transformation mit einer Analyse der Verfahrenslandschaft und Prozesse: Wo startet die Cloud-Transformation, welche konkreten Modernisierungsschritte sind angestrebt? Im Zuge der Modernisierung transformiert Capgemini in enger Abstimmung mit der nutzenden Institution und den Cloud-Service-Providern als Technologiepartner die Verfahrenslandschaft.

Erfolgreicher Einsatz moderner Cloud-Technologien geht mit einem grundlegenden Wandel der Arbeitsweise in der IT einher. Capgemini begleitet öffentliche Institutionen deshalb auch auf der Organisationsebene, um den größtmöglichen Nutzen einer Cloud-Einführung zu erreichen. Capgemini Berater*innen unterstützen bei der Modernisierung der Governance und bei Veränderungen der internen Kultur. Entsprechend vielfältig sind die Fähigkeiten der Cloud-Expert*innen: Sie verstehen institutionelle Strukturen, gestalten effektive und effiziente Prozesse und Cloud-Infrastruktur. Im Sinne des DevOps-Ansatzes arbeiten Plattform- und Software-Engineers eng in interdisziplinären Teams zusammen. Dabei ergeben sich auch neue Rollenprofile für Mitarbeiter*innen bei Capgemini, die im Laufe ihrer Karriere in allen Bereichen – Beratung, Entwicklung, Architektur – fachliche Spezialisierungen wählen oder den Weg der Generalist*innen einschlagen.

Erfahren Sie mehr über Karrieremöglichkeiten bei Capgemini:
www.capgemini.de/karriere





Quelle: OVH

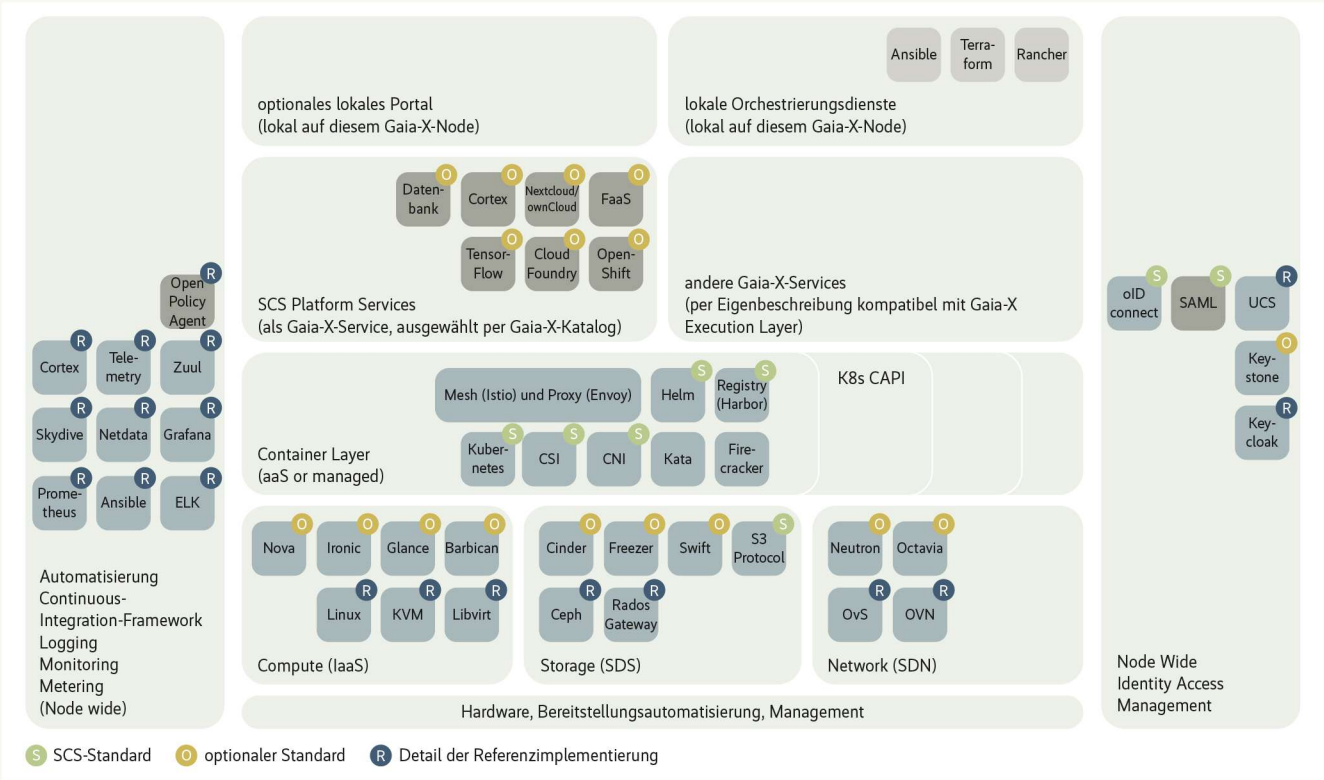
Auch OVHcloud geht mit einer auf OpenStack-APIs basierenden Cloud an den Start und spielt nach europäischen Regeln (Abb. 4).

Rolle. Blockiert ein fremder Internetanbieter den Zugriff auf Daten, sodass die eigene Applikation nicht mehr zu verwenden ist, kann das Firmen in Gefahr bringen – oder die öffentliche Ordnung in ganzen Ländern.

Problem 2: Dienste

Nicht minder wichtig ist die Verfügbarkeit von Diensten im Kontext des Lock-in-Effekts. PaaS, SaaS und Co. machen es spielend einfach, bestehende On-Premises-Dienste in die Cloud zu verlagern, etwa wenn eine Kommune eine Uralt-Installation von MS Exchange loswerden muss. Natürlich hat Microsoft entsprechende Migrationswerkzeuge, um bestehende On-Premises-Set-ups gleich in Azure zu übernehmen. Die Behörde zahlt hinterher vermutlich weniger Geld für diesen Dienst als für die On-Premises-uralt-Variante, genießt höhere Verfügbarkeit durch implizite Features für HA im Azure-Kontext und erspart sich zugleich den Betrieb eigener Infrastruktur.

Doch wer seine E-Mails in Microsoft 365 integriert – und bei den Konkurrenzprodukten von Google und anderen Anbietern ist es nicht anders –, bekommt nicht nur ein DSGVO-Problem, sondern macht sich vom gebuchten Dienst auch komplett abhängig.



Quelle: SCS

Der Sovereign Cloud Stack versteht sich als Werkzeugkasten für Unternehmen, die eine private oder öffentliche Cloud auf Basis offener Standards so bauen wollen, dass Kunden darin echte Souveränität genießen können (Abb. 5).

Das ist im Alltag gegebenenfalls ein Ärgernis, wenn Funktionen wegfallen oder Updates anstehen, für die man eigentlich keinen Bedarf oder keine Zeit hat. Kritisch wird die Situation jedoch, wenn durch Eingriffe der Politik solche Abhängigkeitsszenarien ausgenutzt werden, um die Infrastruktur der Behörden anderer Länder zu boykottieren und sogar auszuschalten. Wenn einzelne Behörden eines Landes etwa nicht mehr miteinander kommunizieren können, weil der gemeinsame Mailprovider den Stecker gezogen hat, ist das kaum im Sinne des Erfinders.

Zu allem Überfluss ist es in solchen Situationen regelmäßig unmöglich, „mal eben" von einem Anbieter zu einem anderen zu migrieren: Bestimmte Features und Funktionen bauen die großen Hyperscaler nämlich auch und gerade deshalb ein, um das zu verhindern. Wer beispielsweise als Unternehmen eine Internetplattform betreibt und dafür auf eine der skalierbaren Datenbanken der Hyperscaler zugreift, findet bei der Konkurrenz nicht schnell mal eine kompatible Alternative. Umbauten an der jeweiligen Anwendung wären unumgänglich, würden aber viel Zeit kosten. Diese Zeit haben im Zweifelsfall weder Firmen noch Behörden.

Umgehen lässt sich das Problem letztlich nur durch die Definition und Nutzung offener Standards. Wer das Prinzip aber richtig angeht, setzt dazu auf Open-Source-Software und offene Standards und verhindert so von vornherein, dass der Lock-in-Effekt überhaupt eintritt.

Souveräne Clouds in Europa

Digitale Souveränität klingt zunächst wie eine Floskel. Dann wird es schnell konkret: Wie man die eigene IT-Landschaft konstruiert, von wem man sich im Falle eines Falles abhängig macht und wie man sich technisch absichert, das entscheidet unter Umständen durchaus über Wohl oder Wehe eines ganzen Unternehmens oder kritischer staatlicher Infrastruktur.

Etliche Unternehmen in Europa haben das erkannt und wollen zum Gegengewicht zu AWS, Azure und Co. werden. Auch die Politik ist nicht untätig: Gaia-X halten die meisten Beobachter heute zwar für gescheitert, doch das Projekt existiert noch und es schafft noch immer technische Standards, die ein wichtiger Beitrag zu digitaler Souveränität sein können. Doch stehen Projekte wie Gaia-X nicht an vorderster Front. Diese Aufgabe kommt hierzulande stattdessen Internetanbietern zu, die den Betrieb digitaler Infrastruktur oft seit Jahrzehnten erfolgreich praktizieren. Sie nehmen für sich in Anspruch, an die europäische Rechtsordnung gebunden zu sein, sodass viele rechtliche Probleme, mit denen Unternehmen sich bei den Hyperscalern herumschlagen, gar nicht erst entstehen. „Cloud made in Europe" ist hier also mehr als ein Werbeslogan. Im Folgenden stellt dieser Artikel einige Produkte namhafter Hersteller vor und erläutert deren Ansätze.

Magenta-T mit der Open Telekom Cloud

Dass man den Markt verstanden hat und in der Lage ist, ihn mit qualitativ hochwertigen und innovativen Produkten zu bespielen, das demonstriert die Telekom seit einigen Jahren mit schöner Regelmäßigkeit. Lange bevor die digitale Souveränität in der Diskussion vorkam, konnte T-Systems in Form der Open Telekom Cloud (OTC, siehe Abbildung 2) bereits liefern.

Die OTC war dabei von Anfang an als Alternative zu AWS, Azure und Co. für den hiesigen Markt konzipiert und warb mit Faktoren

wie „Datenschutz made in Germany“. Für alle Belange in der Open Telekom Cloud übernimmt T-Systems die volle betriebliche Verantwortung, Vertragspartner ist ausschließlich die T-Systems International (TSI), und wer will, speichert seine Daten ausschließlich auf Servern im Hoheitsgebiet der Bundesrepublik Deutschland.

Gerade in den vergangenen Jahren hat die Open Telekom Cloud auch technisch einen erheblichen Sprung in die richtige Richtung gemacht: Noch immer basiert das Produkt im Kern auf OpenStack, setzt also auf freie APIs und standardisierte Werkzeuge. Neben dem klassischen Infrastructure-as-a-Service-Geschäft (IaaS) bietet T-Systems heute auf der OTC aber auch viele PaaS- und SaaS-Dienste an. Mit AWS aufnehmen kann man es dabei zwar im Sachen Quantität nicht, aber das dürfte für die meisten Kunden hierzulande kaum notwendig sein. Mittlerweile darf die Open Telekom Cloud etliche Zertifikate und Freigaben ihr Eigen nennen; so ist die Plattform offiziell zertifiziert für Dienste, die Amtsgeheimnisse verarbeiten. ISO27001 und diverse andere Audits gehören ebenfalls zum Zertifizierungspaket.

Nicht zuletzt nutzt die Telekom ihre Open Telekom Cloud als Vehikel für eigene Produkte: Einige PaaS- und SaaS-Dienste werden gar nicht im Kontext der OTC beworben, greifen im Hintergrund aber auf diese zurück.

In Summe ist die Open Telekom Cloud mithin ein schönes Beispiel dafür, wie es mit der digitalen Souveränität klappen kann: Sie hat ein starkes Unternehmen im Rücken, setzt bei sämtlichen Schnittstellen auf offene Standards und ist transparent bei Ort sowie Art und Weise der Datenhaltung. Falls Kunden aus irgendwelchen Gründen genug von Magenta-T haben, stehen ihnen Auswege offen. Weil die OpenStack-APIs bei der OTC zum Einsatz kommen, lassen Workloads sich zumindest grundsätzlich in andere Clouds auf OpenStack-Basis verschieben.

Die Schweden-Cloud Cleura

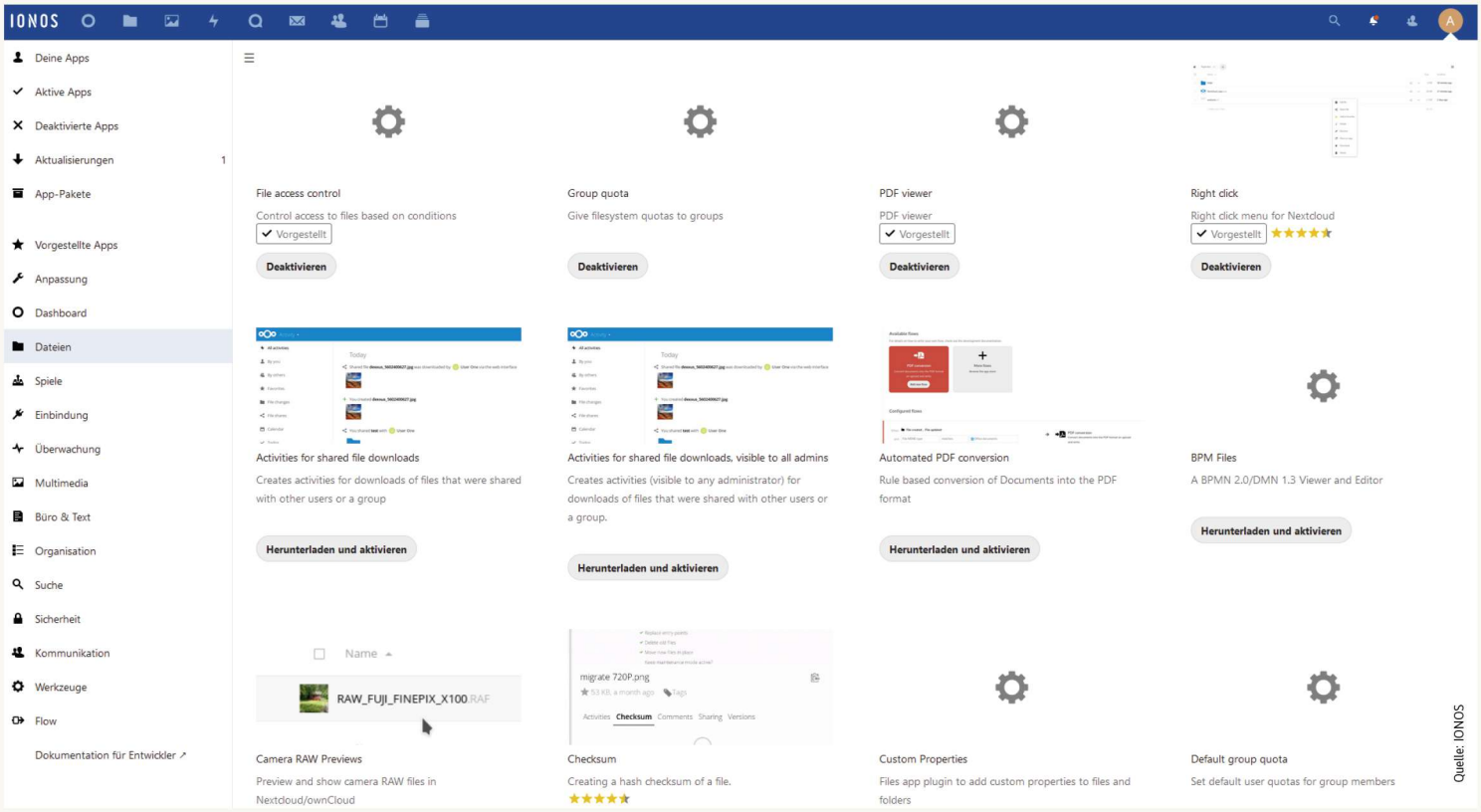
Zu den Public Clouds auf OpenStack-Basis gehört auch Cleura (Abbildung 3). Betreiber ist Iver, das das zuvor City Cloud genannte Produkt 2020 samt dessen Anbieter gekauft hat. Mittlerweile gehört Iver als Muttergesellschaft einer britischen Beteiligungsfirma für Wagniskapital. Dass man es auf die Themen digitale Souveränität und internationale Standardisierung abgesehen hat, ergibt sich schon aus der Dokumentation des Produktes: Immer wieder betont diese nämlich, dass Nutzer bei der Wahl der Komponenten der Cloud und bei der Art, wie sie diese einsetzen möchten, völlig freie Hand haben.

Rechtlich sind die Dinge klar: Iver ist ein schwedisches Unternehmen und unterliegt mithin sämtlichen europäischen Regeln und Richtlinien wie etwa auch T-Systems mit seiner OTC. Garantien im Hinblick auf den Speicherort von Daten sind bei Cleura ebenso verfügbar wie bei der Telekom-Cloud. Etwas kleiner gestaltet sich bei der Cleura-Cloud aber die Zahl der zusätzlich zu IaaS verfügbaren Features. Essenzielle Produkte wie Kubernetes stehen jedoch auch hier zur Verfügung.

In Summe präsentiert Cleura sich als zuverlässiger Cloud-Anbieter mit festen Wurzeln im europäischen Rechtskontext, der auch technisch auf der Höhe der Zeit ist. Weil sowohl die OTC als auch Cleura auf OpenStack basieren, sollten sogar hybride Set-ups zwischen den Lösungen möglich sein, auch wenn das etwas Bastelei bedingt. In Sachen Offenheit gelten für Cleura jedenfalls dieselben Vorteile wie für die Open Telekom Cloud auch – selbst wenn man hier aus irgendwelchen Gründen schnell weg muss, lassen sich vorhandene Ressourcen dank der Nutzung offener Standards woanders schnell etablieren.

Die Franzosen-Wolke OVH

Wenn von OpenStack-Clouds die Rede ist, darf der französische Anbieter OVH (Abbildung 4) nicht fehlen. Der ist so lange im Geschäft wie die OTC der Telekom und unterscheidet sich von dieser vor allem dadurch, dass er in Frankreich beheimatet ist



Quelle: IONOS

Als einziger der hier vorgestellten Anbieter setzt IONOS auf eigene APIs und nicht auf die öffentlichen von OpenStack. Im Kontext digitaler Souveränität hat der Anbieter trotzdem einige Pfunde zum Wuchern (Abb. 6).

und nicht in Deutschland. Im Kontext der europäischen Regeln ist das im Grunde aber zu vernachlässigen: Sämtliche Regeln sind für OVH identisch mit jenen von OTC und auch Cleura. Kommerziell gleicht OVH eher der Telekom denn Cleura, schon in Sachen Größe und Unternehmensform (wie die DTAG ist OVH eine in Frankreich an der Börse notierte AG).

Technisch steht man der Konkurrenz aus Deutschland oder aus Schweden in nichts nach: Neben einem umfassenden IaaS-Angebot gehören auch etliche PaaS- und SaaS-Angebote auf Basis von Kubernetes zum OVH-Portfolio. Wieder kommen OpenStack-APIs zum Einsatz, sodass sich mit denselben Werkzeugen, die OTC oder Cleura verwalten, auch Workloads in OVH steuern und kontrollieren lassen. Und wie beschrieben sind auch hier hybride Set-ups möglich, aber mit etwas Bastelei verbunden. Ein Verschieben von Workloads zwischen der OTC, Cleura sowie OVH sollte aber problemlos möglich sein.

Obendrein hat OVH in der Vergangenheit erfolgreich bewiesen, dass es Krisen in den Griff bekommen kann. 2021 brannte ein großes Rechenzentrum des Unternehmens in Straßburg komplett aus – und OVH machte aus der Not eine Tugend, indem es mit seiner Klientel so offen wie möglich kommunizierte: Statt Geheimniskrämerei legte man die Fakten in schöner Regelmäßigkeit auf den Tisch und machte realistische Angaben hinsichtlich der Rettbarkeit von Daten, der Wiederanlaufzeit von Diensten und anderer Faktoren. Auch das kann im Kontext digitaler Souveränität durchaus eine Rolle spielen: Wie transparent ein Anbieter kommuniziert, bestimmt letztlich nämlich, wie souverän und selbstbestimmt ein Kunde eines Unternehmens seine Entscheidungen treffen kann. Hier hat OVH gezeigt, wie es gehen kann.

Und noch mal OpenStack: plusserver

„Just another OpenStack“ einerseits und durchaus eine Besonderheit ist pluscloud open, ein auf OpenStack basierendes Cloud-Produkt von plusserver in Köln. Besonders ist pluscloud vor allem wegen der genutzten Software: Hier kommt keine Eigenentwicklung zum Einsatz, sondern ein unter Leitung von Kurt Garloff, einem Urgestein der deutschen Cloud-Szene, entstandenes Produkt namens Sovereign Cloud Stack (SCS, [1], siehe Abbildung 5). Der SCS will im Kern ein standardisierter Stack aus etlichen verschiedenen Softwarekomponenten sein, mit denen sich Cloud-Workloads transparent und auf Basis offener Standards betreiben lassen. Sämtliche im SCS genutzten Komponenten sind Open-Source-Software und stehen unter einer freien Lizenz. Parallel dazu läuft – siehe oben – das Projekt Open Operations, das SCS-nutzenden Firmen Regeln vorgibt, ihre betrieblichen Abläufe so transparent wie möglich zu handhaben.

Die Idee: Zwischen Anbietern von Plattformen auf SCS-Basis lassen sich Workloads ohne Probleme verschieben oder aufteilen. Weil überall dieselben Standardkomponenten zum Einsatz kommen, ist das nochmals ein höherer Grad an Souveränität als bei den anderen OpenStack-Clouds in diesem Artikel. Hinzu kommt: Entscheiden sich Unternehmen dafür, auf SCS-Basis eine private Cloud zu bauen, bekommen sie dieselben Vorteile, und zwar sowohl im eigenen RZ als auch im Gespann mit Public-SCS-Clouds in hybriden Set-ups.

Zur Wahrheit gehört aber auch, dass beim Sovereign Cloud Stack noch lange nicht alles perfekt ist. Die Dokumentation lässt an manchen Stellen zu wünschen übrig, die Liste der verfügbaren PaaS- und SaaS-Angebote ist noch übersichtlich und sonderlich viel öffentliche Traktion hat der SCS bisher nicht erreicht. Hier steht kein riesiger Konzern dahinter, sondern eine kleine Truppe von Entwicklern, die von einigen kleineren und mittelgroßen Anbietern unterstützt werden. Vor diesem Hintergrund ist das SCS-Projekt durchaus beeindruckend. Anhand der Beschreibung der souveränen Nutzung von Clouds ist SCS augenblicklich einer der heißesten Kandidaten für höhere Weihen innerhalb der Industrie. Denn SCS zeigt, dass offene Standards und erzwungene Standardisierung viele technische Probleme schon in der Entstehung verhindern.

plusserver darf sich in diesem Kontext auf die Fahnen schreiben, ein Pionier in Sachen digitale Souveränität im deutschen Cloud-Umfeld zu sein. Wer sich für pluscloud open entscheidet, bekommt zwar etwas weniger Lametta als bei der Konkurrenz, dafür aber echte Souveränität nach deutschen Regeln auf deutschem Hoheitsgebiet.

IONOS: auch souverän, aber anders

Der deutsche Cloud-Provider IONOS setzt nicht auf OpenStack oder dessen APIs. Die heutige IONOS-Cloud (Abbildung 6) ist das Ergebnis eines Zukaufs eines proprietären Cloud-Produktes eines Berliner Start-ups. Die IONOS-APIs sind bis heute nicht öffentlich,

Souveräne europäische Clouds

Dienst	Open Telekom Cloud	Cleura	OVHcloud	pluscloud open	IONOS Cloud
Betreiber	T-Systems International	Cleura AB	OVHcloud SAS	PlusServer GmbH	IONOS SE
Unternehmenssitz	Bonn, Deutschland	Stockholm, Schweden	Paris, Frankreich	Köln, Deutschland	Montabaur, Deutschland
URL	open-telekom-cloud.com	cleura.com/services/compliant-cloud/	www.ovhcloud.com/de/	www.plusserver.com/produkte/pluscloud-open	cloud.ionos.de
API-Kompatibilität	OpenStack	OpenStack	OpenStack	OpenStack	OpenStack
IaaS	✓	✓	✓	✓	✓
DBaaS	✓	–	✓	–	✓
LBaaS	✓	✓	✓	✓	✓
weitere PaaS-/SaaS-Angebote	✓	✓	✓	✓	✓
Managed Kubernetes	✓	✓	✓	✓	✓

IONOS ist bei der eigenen Cloud der einzige Anbieter, der sie nutzt. Streng genommen bieten sich Kunden hier also weniger Optionen zur Verwirklichung der digitalen Souveränität, weil es einerseits keine vom Hersteller unabhängigen Werkzeuge gibt und andererseits auch keine weitere Plattform, die diese API unterstützt.

Doch beim Thema digitaler Souveränität kann IONOS auf vielen anderen Ebenen punkten. Die Firma ist eine deutsche AG, die deshalb sämtliche für europäische Unternehmen geltenden Regeln einhalten muss. Wer möchte, kann auch bei IONOS die eigenen Workloads ausschließlich auf Servern innerhalb der Bundesrepublik betreiben. Hinzu kommt: Man beackert das Cloud-Portfolio mit einer großen Anzahl von Entwicklern, sodass neben klassischen IaaS-Angeboten heute auch etliche PaaS- und SaaS-Angebote verfügbar sind. Das nutzt IONOS, um im Kontext der digitalen Souveränität aktiv für sich zu werben: Im Dunstkreis von Gaia-X etwa hat das Unternehmen mehrere Ausschreibungen gewonnen, die technische Plattform für einzelne Gaia-X-Projekte zu stellen.

Die mangelnden Alternativen verfügbarer Clouds mit identischer API kompensiert IONOS zum Teil außerdem dadurch, dass das Unternehmen den eigenen Kunden in Deutschland wie in Europa etliche Regionen für Deployments zur Verfügung stellt. Fällt eine Region aus, lässt sich eine Workload also auch woanders starten, vorausgesetzt, sie ist entsprechend technisch vorbereitet, etwa durch Automatisierung. Zum Teil liegt IONOS hier in Sachen Regionen deutlich vor der Konkurrenz, etwa vor T-Systems mit der OTC.

Fazit

Digitale Souveränität wird als Thema zunehmend an Relevanz gewinnen. Unternehmen wie Behörden können es sich schon heute de facto nicht mehr leisten, ihr digitales Schicksal von einem einzelnen Anbieter abhängig zu machen, der zudem vollständig außerhalb der europäischen Rechtsordnung steht. So sehr Google, Amazon und Co. auch hierzulande Rechenzentren bauen und mit grotesken Konstrukten wie der „Datentreuhänderschaft“ daherkommen, die die Telekom einst für Workloads bei den Hyperscalern übernahm – echte Souveränität bedeutet, tatsächlich unabhängig zu sein, soweit es technisch realisierbar ist.

Etliche Anbieter in Europa bieten dafür heute mannigfaltige Möglichkeiten. Langfristig dürfte das Thema aber auch noch einen weiteren Aspekt vereinnahmen, nämlich die wieder verstärkte Aktivität im Bereich Private Cloud. Wirklich souverän ist, wer die Daten gar nicht erst aus der Hand gibt. Softwareprojekte wie der Sovereign Cloud Stack, aber auch Kollaborations- und Filesharing-Anbieter wie ownCloud oder Nextcloud leisten hier bereits heute wertvolle Beiträge, und werden potenziell noch wichtiger werden. (avr@ix.de)

Quellen

[1] Kurt Garloff; Wolken-Verbund; Mit Souvereign Cloud Stack zu mehr digitaler Souveränität; iX 12/2020, S. 48

[2] Informationen zu den Positionen des Bundes-CIO und der OSBA: ix.de/zyem

In iX extra 5/2023 Hosting: Cloud-Migration als Provider-Service

In Unternehmen wird es zunehmend gängige Praxis, Applikationen über mehrere Clouds zu verteilen: bei einem Serviceprovider, AWS, Azure oder in Colocations. Um der Gefahr unkontrollierten Wildwuchses entgegenzuwirken, sind sorgfältige Planungen und Vorarbeiten nötig. Die eigentliche Migration sollte automatisiert in mehreren Schritten erfolgen. Die Hyperscaler stellen hierfür Tools zur Verfügung und Hoster standardisierte oder individuelle Dienstleistungen. Das iX extra gibt einen Überblick, wie Cloud-Migrationen erfolgreich bewältigt werden können.

Die weiteren iX extras

6/2023	**Storage:** Backup und Archivierung	erscheint am 25.05.2023
7/2023	**Cloud:** Identiy- und Access-Management	erscheint am 29.06.2023
10/2023	**Security:** Neues rund um die it-sa	erscheint am 21.09.2023
11/2023	**Storage:** Objektstorage	erscheint am 19.10.2023
12/2023	**Hosting:** Hochverfügbarkeit auf Bestellung	erscheint am 23.11.2023

Änderungen vorbehalten

MARTIN GERHARD LOSCHWITZ

ist freier Journalist und beackert regelmäßig Themen wie OpenStack, Kubernetes und Ceph.