Europa auf dem Weg zur souveränen Cloud

Frischer Antrieb für Digitalisierung?

T Systems

Let's power
higher performance

In Kooperation mit

intel

Inhalt

Der jüngste Spross des Cloud-Universums: die Sovereign Cloud

Seit Jahren befinden sich verstärkt Themen wie Digitalisierung und Cloud auf den politischen Agenden wieder. So ist die Cloud einer der Kernaspekte der europäischen Digitalstrategie, doch auch viele europäische Länder haben umfangreiche Programme für Digitalisierung etabliert. Zuletzt publizierten u.a. Italien (September 2021) und Frankreich neue Cloud-Strategien – die im Zusammenhang mit der europäischen Initiative GAIA-X gesehen werden können.

So stellte im Mai 2021 [1, 2, 3] Bruno Le Maire, Minister für Wirtschaft, Finanzen und Wiederaufbau, eine Strategie vor, mit der die Cloud-Einführung in Frankreich beschleunigt werden soll. In dem skizzierten Szenario sollen Regierungen weltweit unter der Kontrolle von nationalen Anbietern führende Cloud-Technologien nutzen – ein weiterer Beitrag zur anhaltenden und verstärkt auch emotional geführten Diskussion um souveräne Clouds.

Häufig stehen geopolitische Aspekte im Mittelpunkt der Diskussion um souveräne Clouds und behindern – wie in den Anfangstagen der Cloud – die Suche nach einer einheitlichen Definition und Wahrnehmung. Dabei bietet die Verfügbarkeit von souveränen Clouds auch Organisationen jenseits der öffentlichen Hand und regulierter Branchen interessante Perspektiven. Viele Unternehmen verbinden mit souveränen Clouds die Hoffnung, dass sie die Möglichkeiten von Public Clouds in einem compliance-konformen Rahmen vorkonfektioniert nutzen können.

Aber was steckt hinter dem Konzept von souveränen Clouds und welche Herausforderungen können sie lösen? Dieses White Paper ist ein weiterer Diskussionsbeitrag, um das Phänomen besser zu verstehen und zeigt die konkrete Realisierung einer Sovereign Cloud im Detail auf.

Alles begann mit der Cloud

Anfangs kritisch beäugt, hat sich die Cloud in den letzten Jahren einen festen Platz auf den Agenden der meisten Unternehmen in Europa erobert. Auch die öffentliche Hand hat die Potenziale der Sourcing-Alternative erkannt. Cloud Computing hat mit seiner einfachen und dynamischen Verfügbarkeit in Verbindung mit den passenden Abrechnungsmodellen das Outsourcing revolutioniert und flexibilisiert.

Im Rahmen ihrer Strategien verfolgen Unternehmen und Organisationen sehr unterschiedliche Ansätze beim Einsatz der Cloud – nur wenige Unternehmen setzen auf einen „All-in“-Ansatz. Weitaus häufiger sind hybride Modelle, in denen Private und Public Cloud On-Premises-Ressourcen beigefügt werden oder in denen vor allem neue Geschäftsideen in der Public Cloud realisiert werden, während etablierte Workloads in Bestandssystemen verbleiben. Cloud-Strategien berücksichtigen sehr häufig auch Aspekte des Investitionsschutzes – sind also nicht nur vor dem Hintergrund von Geschäftsentwicklung und Innovation, sondern auch vor dem Hintergrund betriebswirtschaftlicher Facetten zu entwickeln.

Nichtsdestoweniger sind die Vorteile der Cloud weithin anerkannt. Sie ermöglicht Unternehmen schnellere Reaktionen auf Marktentwicklungen, die risikoärmere Entwicklung von neuen Services und Geschäftsideen sowie die Einführung agiler Entwicklungsmethoden (DevOps). Dabei setzen Unternehmen verstärkt auf vorkonfigurierte Services, die aus den Ökosystemen der großen Hyperscaler bereitgestellt werden. Ein typisches Beispiel dafür ist die Nutzung von Plattform-Diensten für die Entwicklung von Künstlichen Intelligenzen (AI PaaS) oder für Datenanalytik (z.B. Big Query in der Google Cloud). Insbesondere Entwicklungsprojekte profitieren in hohem Maße von der Cloud: Sie bietet den temporären Zugriff auf umfangreiche Rechen- und Speicher-Ressourcen (beispielsweise für das Training von KIs) in Verbindung mit nutzungsbasierten Preismodellen.

Die Skalierbarkeit der Cloud bietet weitere Vorteile für die Abfederung von Lastspitzen, in Burst-Szenarien oder für die (internationale) Expansion von Services. In solch dynamischen Szenarien kann sie auch ihre Vorteile in puncto Kosteneffizienz ausspielen. Gleichzeitig befreit der Cloud-Einsatz Inhouse-Teams von Infrastruktur-Management-Aufwänden bis hin zum Betrieb eigener Rechenzentren. Darüber hinaus erzielt das Sourcing-Modell Beiträge, um den Carbon Footprint von Unternehmen nachhaltig zu reduzieren.

Die Cloud bietet damit eine perfekte Basis, um die zukünftigen digitalen Märkte in nahezu allen Branchen zu gestalten. Auch die öffentliche Hand hat die Perspektiven für moderne Verwaltungsprozesse und E-Government erkannt.

Die Cloud – die perfekte Lösung für alles?

Die Akzeptanz der Cloud zeigt sich im kontinuierlichen Wachstum des Marktes für Cloud-Services. IDC prognostiziert für den europäischen Markt (Public Cloud) ein Volumen von 105 Mrd. US$ 2022, IaaS und PaaS werden dabei um ca. 30 Prozent wachsen. In ihren Top 10 Predictions für 2022 erwarten die Analysten, dass bis 2024 etwa zwei Drittel der Legacy-Applikationen mit Cloud Services angereichert werden.[4]

Trotz des Wachstums zeigt aber die Realität, dass mitnichten alle Workloads in die Cloud verlagert werden. Dafür gibt es verschiedene Gründe, die sich an den konkreten Workloads, Applikationen und Daten orientieren.

KOSTENGRÜNDE Flexibilität hat ihren Preis. Pay-as-you-go-Modelle für die Cloud realisieren große finanzielle Vorteile für Adhoc oder temporäre Einsatzszenarien. Für den Dauerbetrieb von Anwendungen bieten Hyperscaler häufig rabattierte Reserved-Kontingente an. Da Unternehmen meist über keine TCO-Analyse ihrer Istkosten verfügen, wirken die Dauerkosten für den Public-Cloud-Einsatz höher als die Kosten für das traditionelle Hosting. Hinzu kommt die Notwendigkeit für eine Financial Governance der Cloud-Ressourcen, beispielsweise das aktive Abschalten von ungenutzten Ressourcen. Kostenkontrolle für Cloud-Ressourcen ist aktuell eine der größten Herausforderungen für Unternehmen.

TECHNISCHE LIMITS Im Produktionsumfeld mit seinen Echtzeit-Ansprüchen können die Latenzen bei einer Datenverarbeitung in der Cloud inakzeptable Verzögerungen auslösen, beispielsweise beim Einsatz von Virtual- oder Augmented-Reality-Applikationen. Für Echtzeit- oder echtzeitnahe Datenverarbeitung werden Cloud-Infrastrukturen daher mit Edge-Computing-Ressourcen angereichert.

FEHLENDE DATENSOUVERÄNITÄT Unternehmensinterne Daten repräsentieren das Know-how und die Errungenschaften der Geschäftstätigkeit. Unternehmen fordern zurecht, dass ihre Daten in der Cloud zuverlässig verfügbar und sicher gegen unberechtigte Zugriffe aufbewahrt werden. Sie müssen Gewissheit haben, dass ihre Daten nicht zweckentfremdet eingesetzt (beispielsweise für das Training von KIs) oder manipuliert werden. Darüber hinaus muss die Ablage der Daten nicht nur internen Vorgaben genügen (bspw. dem Schutz geistigen Eigentums): Viele Daten sind speziell durch externe Regularien geschützt (bspw. personenbezogene Daten nach der EU-DSGVO) und dürfen spezifische Rechtsräume nicht verlassen. Verstöße gegen die (in den Ländern der Geschäftstätigkeit unterschiedlichen) Regularien können in Strafzahlungen und Imageverlusten münden.

KOMPLEXE MIGRATION Viele Unternehmen mit langjähriger Marktpräsenz unterhalten komplexe Legacy-Anwendungen, die ihre Business-Prozesse zuverlässig unterstützen. Die Migration solcher Anwendungen ist aufwändig, die Abhängigkeiten von Infrastrukturen sind hoch. Ihre Migration erfordert häufig Neuimplementierungen, bspw. den Umstieg auf Microservices, um die Vorteile der Cloud zu nutzen. Betriebswirtschaftliche Gründe, der Schutz der getätigten Investitionen und die Ausschöpfung des erworbenen Know-hows, favorisieren häufig den weiteren Betrieb derartiger Applikationen im „As-is“-Modus.

ABHÄNGIGKEIT VOM CLOUD-PROVIDER Die Entscheidung für eine Technologie oder einen Provider bedeutet in der Regel eine langfristige Bindung und mündet damit in einer Vertrauensfrage. Wie wird der Cloud-Provider seine Plattform technisch weiterentwickeln? Welchen Einfluss haben Nutzer auf die Entwicklung? Welche Entwicklungen können die Unterstützung der Unternehmensprozesse in Zukunft erschweren?

Nutzer müssen sich darauf verlassen können, dass die Plattform auch in den Folgejahren ihre Erwartungen bspw. an Sicherheit, Innovationskraft, Kosten etc. erfüllen wird. Dazu kommt, dass die Integration von Plattform-Mehrwert-Diensten in eigene Applikationen den Export der Workloads auf andere Plattformen komplizierter macht – der Vendor Lock-in verstärkt sich.

Abhilfe schaffen Applikationen, die plattformunabhängig konzipiert und entwickelt werden oder Open Source nutzen. Auch der Einsatz von Containern ist eine wichtige Komponente. Viele Unternehmen setzen auch Massenspeicher in der Cloud ein, um Daten langfristig abzulegen. Die dabei entstehenden Datenmengen lassen sich nicht immer schnell und einfach von der jeweiligen Plattform abziehen.

Compliance-Vorbehalte als Hemmschuh für den Cloud-Einsatz

Compliance-Vorbehalte sind einer der Hauptgründe für das Zögern gegenüber dem Cloud-Einsatz in europäischen Unternehmen – und damit auch ein Hindernis für die Realisierung von Digitalisierungsprojekten. Das bestätigt auch der Cloud-Monitor des Branchenverbands Bitkom aus dem Jahr 2021 für den deutschen Markt. Hier artikulieren 75 Prozent der Befragten, dass sie beim Public-Cloud-Einsatz einen Zugriff Unberechtigter auf sensible Unternehmensdaten befürchten. 67 Prozent äußern Unklarheiten hinsichtlich der Rechtslage; 60 Prozent halten fest, dass rechtliche und regulatorische Bestimmungen gegen einen Public-Cloud-Einsatz sprechen.

Datenschutz und Datensicherheit machen häufig Sorgen

Inwieweit treffen die folgenden Aussagen für Ihr Unternehmen zu bzw. nicht zu?

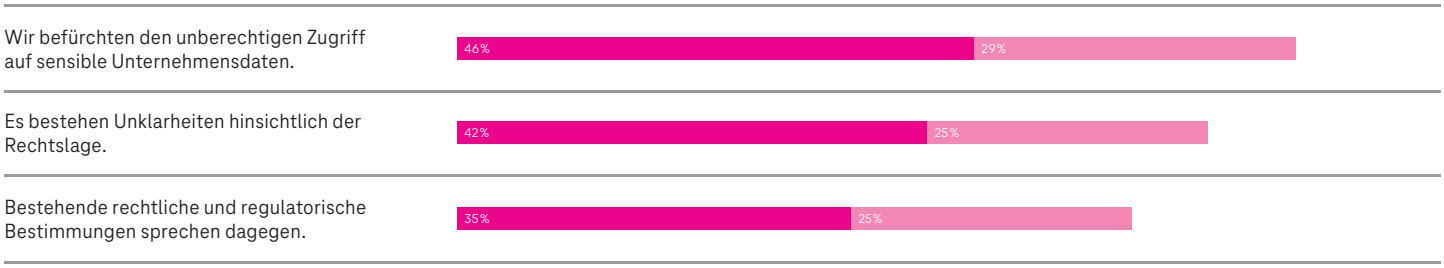


Abb. 1. Auszug der Ergebnisse des Bitkom/KPMG Cloud Monitors 2021 . Befragung von Unternehmen, die keinen Public-Cloud-Einsatz planen. Magenta: trifft voll und ganz zu, transparent: trifft eher zu.

Initiativen zur Sicherheits- und Datenschutzbewertung von Cloud-Diensten (European Data Protection Board, in Schweden und den Niederlanden) legen nahe, dass in anderen Ländern ähnliche Vorbehalte gegen die Public Cloud bestehen. Public-Cloud-Angebote werden durch US-amerikanische und chinesische Anbieter geprägt. Vertragliche Regelungen zwischen dem Anbieter und dem Nutzer verschaffen europäischen Unternehmen nur bedingt Sicherheit. Im Zweifelsfall hebeln nationale Regelungen wie der US-Cloud Act das geltende Vertragsrecht aus. Die Diskrepanz hinsichtlich des Schutzes von Daten in unterschiedlichen Rechtsräumen (zwischen Anbieter und Nutzer) bleibt bestehen.

Zusammengefasst: Private Unternehmen und Organisationen der öffentlichen Hand haben die Bedeutung von Cloud Computing für die Zukunft erkannt und wollen die Vorteile im Wettbewerb bzw. für den Bürgerservice nutzen. Diesem Wunsch stehen aber regulatorische Hindernisse im Weg. Diese lassen sich sehr wohl im Rahmen von Einführungsprojekten beseitigen. Aber dies erfordert fallbezogen hohe Aufwände für die Implementierung von Compliance- und Sicherheitslösungen (unter denen bisweilen letzten Endes auch die User Experience leidet).

Cloud ja – aber im Einklang mit europäischen Regelungen

Mit den Forderungen nach einer souveränen Cloud wollen die europäischen Länder das Dilemma Cloud vs. Compliance lösen. Die souveräne Cloud soll Unternehmen die Funktionalität der Public Cloud bereitstellen und zugleich die in Europa geltenden Regularien erfüllen. Damit wird die Sovereign Cloud zwar kein Cloud-Allheilmittel, könnte aber in einem bestimmten Marktsegment eine interessante Sourcing-Alternative werden, beispielsweise für regulierte Branchen, die öffentliche Verwaltung oder überall dort, wo Nutzer ein Höchstmaß an Vertrauen für den Umgang mit ihren Daten und Diensten einfordern. Eine mögliche Definition einer souveränen Cloud spiegelt die Ansprüche der Nutzer wider:

> Eine souveräne Cloud stellt ein Cloud-Dienste-Ökosystem bereit, welche keine Anbieterabhängigkeiten erzeugt („Vendor Lock-In“). Die angebotenen Dienste sind entweder auch Open Source verfügbar oder es existiert ein entsprechendes anbieterunabhängiges Äquivalent, so dass jede Funktionalität unabhängig vom Anbieter zu jedem Zeitpunkt genutzt werden kann. Sie erfüllt die Anforderungen in Bezug auf Regulatorik und Gesetzgebung, so dass die Daten und deren Nutzbarkeit zu jedem Zeitpunkt beim Nutzer verbleiben.
>
> **Dr. André Engelbertz (VP Cloud Services Strategy & CTO, T-Systems International GmbH)**

Nicht definitionsrelevant, aber wichtig für eine Business-Entscheidung über die Nutzung einer souveränen Cloud sind zudem zwei Aspekte:

1 Die Erwartungen von Nutzern an eine Cloud umfassen auch ein leistungsfähiges Ökosystem von Zusatzdiensten – die Bereitstellung eines einfachen IaaS wird den aktuellen Business-Anforderungen nicht gerecht.

2 Regulatorische und Souveränitätsanforderungen werden durch den klassischen Eigenbetrieb, das Outsourcing und die Private Cloud seit Jahrzehnten zuverlässig abgebildet. Diese Sourcings dienen als Maßstab für die Souveränität einer Sovereign Cloud auf Basis einer Public Cloud. In der Realität können so beim Design einer Sovereign Cloud – je nach Souveränitätsniveau – Abstriche an der Architektur einer Public Cloud notwendig sein (beispielsweise die Limitierung der Skalierbarkeit, die Verfügbarkeit von Diensten oder höhere Kosten).

Dies illustriert anschaulich, dass die Sovereign-Cloud-Diskussion von zwei Gegenpolen beherrscht wird:

1. dem Wunsch nach maximaler Souveränität, der zu einer Abkehr von Cloud-Prinzipien führt und
2. der Zufriedenheit der Nutzer mit einem Souveränitätsniveau, das „gut genug“ ist, aber volle Cloud-Funktionalität bietet.

In anderen Worten: **Sind Unternehmen bzw. Nutzer bereit, für Souveränität Abstriche gegenüber dem Leistungsportfolio führender Cloud-Ökosysteme hinzunehmen – bei höheren Kosten?**

Auf dem Weg zur Sovereign Cloud

Theoretisch existieren verschiedene Wege, mit denen diese Souveränität realisiert werden soll – und wie weit die Souveränität und die damit verbundene Unabhängigkeit gehen soll.

Aufbau einer europäischen Cloud

Im naheliegendsten Fall baut Europa eine eigene Kontinental-Cloud bzw. europäische Staaten initiieren nationale Clouds. Doch wie weit soll beim Design einer eigenen souveränen Cloud die Wertschöpfungstiefe gehen? Sollen beispielsweise auch Chips und Netzwerkkomponenten aus europäischer Produktion stammen? In der Ära global vernetzter Wertschöpfungsketten undenkbar. Die wenigsten Unternehmen stellen Software und Hardware selbst her. Sie greifen auf am Markt etablierte Produkte zurück, die von US-Software-Anbietern wie Microsoft oder Hardware-Herstellern wie Intel geliefert werden. Souveränität, also komplette Kontrolle, endet hier an der detaillierten Kenntnis des Codes oder der Hardware-Architektur.

Nutzung eines lokalen Anbieters

Ein einfacher Weg zu einer souveränen Cloud ist die Nutzung eines etablierten europäischen Providers. Da diese ebenfalls dem europäischen Regelwerk genügen müssen, löst sich die Diskrepanz unterschiedlicher Kulturen und Rechtsräume in der Geschäftsbeziehung auf. Allerdings nehmen Nutzer mit diesem Ansatz deutliche Abstriche an der Funktionalität des Cloud-Ökosystems hin. Kein europäischer Provider kann auch nur annähernd die Funktionsfülle der Hyperscaler-Ökosysteme anbieten.

Integration vorhandener europäischer Infrastrukturen

Mit Structura-X entstand im November 2021 eine weitere Initiative zum Aufbau einer (souveränen) GAIA-X-kompatiblen Infrastruktur. Hierbei soll eine souveräne europäische Cloud auf Basis bestehender Infrastrukturen europäischer Firmen entstehen. Die Teilnehmer der Initiative bringen ihre (dem europäischen Recht bzw. den GAIA-X-Vorgaben genügenden) Dienste ein und stimmen gleichermaßen zu Open-Source-Technologie zu verwenden. Damit werden über eine logische Steuerungsebene des Infrastruktur-Verbunds Cloud-Föderierungs-Dienste nutzbar – und mit ihnen Interoperabilität, Sicherheit und Datenschutz „by Design“.

Nutzung eines etablierten, leistungsfähigen Cloud-Ökosystems

Nicht umsonst haben sich die Hyperscaler ihren Platz an der Sonne erobert. Die Kapazitäten ihrer Clouds sowohl in Präsenz, Skalierbarkeit und Service-Portfolio bieten herausragende Möglichkeiten. Souveränitätsansätze, die von Hyperscalern ausgehen, setzen auf zusätzliche technische Souveränitätskontrollen, die in die Plattform eingebaut werden. Alternativ können Nutzer eigene Souveränitätskontrollen oberhalb der Plattform in ihre eigenen Landing Zones einbauen. Zu den üblichen plattform-immanenten Souveränitätskontrollen gehören die Nutzung von Hardware für Confidential Computing oder zusätzliche Verschlüsselungsverfahren.

Etabliertes Cloud-Ökosystem unter der Kontrolle/dem Betrieb eines nationalen Providers

In einer weiteren Variante bietet der Hyperscaler spezifische Cloud-Ressourcen innerhalb und für einen Rechtsraum an. Er übergibt die Kontrolle über die Ressourcen an einen lokalen Partner, der auch die Verträge mit den Kunden abschließt – auf Basis des lokalen Rechts. Der Zugriff des Hyperscalers auf die Cloud-Ressourcen wird gekappt oder zumindest streng durch den lokalen Partner kontrolliert. Der Partner erhält umfassende technische und physische Kontrollrechte – dies kann so weit gehen, dass die Cloud-Ressourcen innerhalb des Partner-Rechenzentrums allokiert werden. Dieses Vorgehen verbindet die Stärken und die Leistungsfähigkeit der existierenden Cloud-Ökosysteme mit den Anforderungen an Kontrolle und Rechtskonformität – ein optimaler Kompromiss, der eine schnelle und pragmatische Realisierung eines Sovereign-Cloud-Angebots ermöglicht. Im DACH-Raum ist bislang ein derartiges Angebot am Markt verfügbar: die T-Systems Sovereign Cloud powered by Google Cloud.

Exkurs Confidential Computing

Die Auslagerung von Rechenleistung bringt zwar viele Vorteile mit sich, erfordert aber auch ein bedeutendes Maß an Vertrauen. Verschlüsselung wird oft als die Antwort angesehen, um dieses Maß an Vertrauen zu erreichen. Denn in einer Welt, in der Unternehmen ständig sensible Daten speichern, konsumieren und weitergeben – von Kreditkartendaten bis hin zu Krankenakten, von Finanzunterlagen bis hin zu Geolokalisierungsdaten – ist der Schutz sensibler Daten wichtiger denn je.

Kryptografie wird heute häufig eingesetzt, um sowohl die Vertraulichkeit von Daten (Verhindern der unbefugten Einsicht) als auch die Datenintegrität (Verhindern oder Erkennen nicht autorisierter Änderungen) zu gewährleisten. Während Techniken zum Schutz von Daten während der Übertragung („in transit“) und im Ruhezustand („in rest“) allgemein genutzt werden, ist der dritte Zustand – der Schutz von Daten, die verarbeitet werden – eine weitere Herausforderung für Sovereign Clouds. Wenn Unternehmen ihre Daten in einer Sovereign Cloud nutzen möchten, müssen sie das Problem lösen, wie sie verschlüsselte Datensätze in großem Maßstab sicher verarbeiten können.

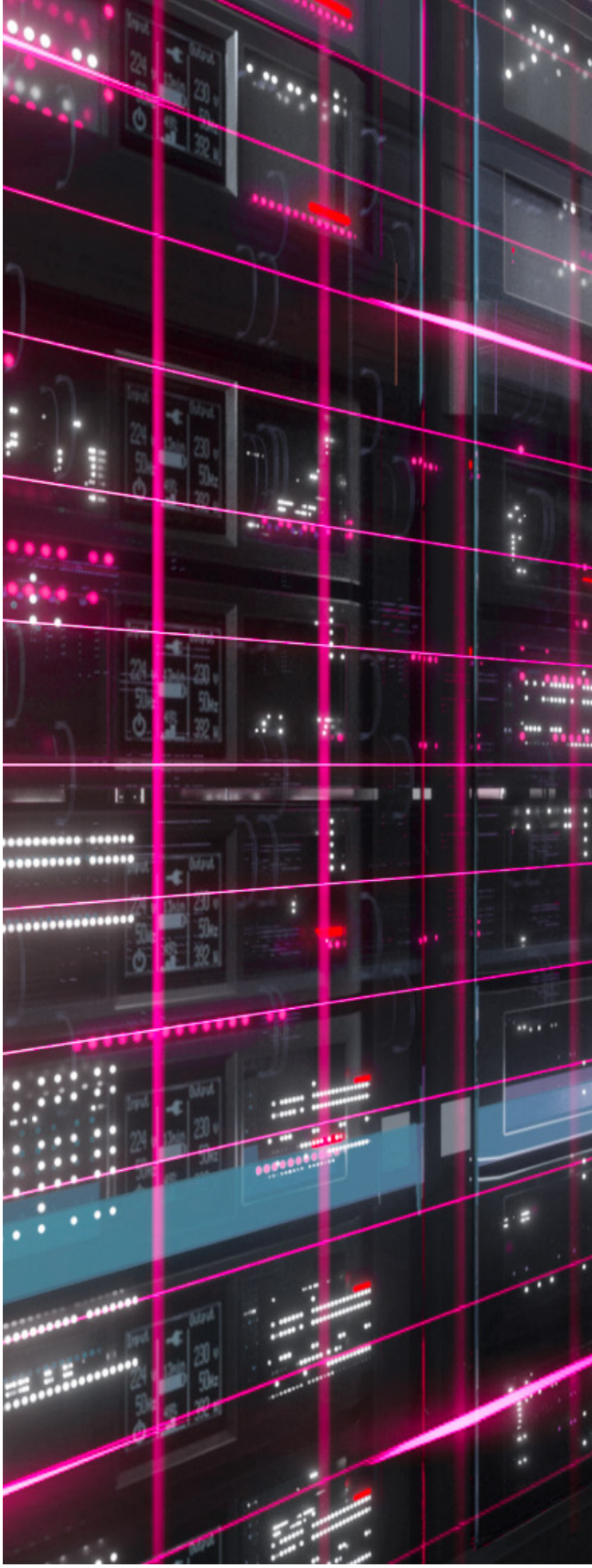
Confidential Computing hilft bei der Lösung dieses Problems. Es schützt die verwendeten Daten, indem Berechnungen in einer hardwarebasierten Trusted Execution Umgebung (wie der Intel® Software Guard Extension – Intel® SGX) erfolgen. Diese sicheren und isolierten Umgebungen verhindern den unbefugten Zugriff oder die Änderung von Anwendungen und Daten während der Nutzung. Das Sicherheitsniveau von Organisationen, die sensible und regulierte Daten verwalten, erhöht sich. Intel® SGX bietet zudem das Konzept der Remote Attestation. Sie garantiert die Integrität der Computerumgebung und des Codes, der auf die Datensätze zugreift. Damit wird sichergestellt, dass der Dateneigentümer immer die Kontrolle über seine Daten behält.

Das Confidential Computing unterstützt damit die Ziele einer Sovereign Cloud. Es erlaubt den Schutz sensibler Daten während ihrer Verarbeitung. Nicht nur sensible Daten im Sinne der Gesetzgebung lassen sich schützen, sondern auch geistiges Eigentum, das für das jeweilige Unternehmen einen hohen Wert darstellt. Confidential Computing schützt damit auch proprietäre Geschäftslogiken, Analysefunktionen, maschinelle Lernalgorithmen oder komplette Anwendungen. Es kann den Zugriff des Algorithmus auf Datensätze überwachen und eine Genehmigung zur Ausführung der gewünschten Funktionen sicherstellen. Moderne Frameworks für maschinelles Lernen wie TensorFlow können so auf vertrauliche Weise auf einer souveränen Cloud genutzt werden. Confidential Computing kann ebenfalls für die sichere Zusammenarbeit von Partnern in der Cloud eingesetzt werden. So können beispielsweise verschlüsselte Daten aus verschiedenen Quellen kombiniert werden, um vertrauliche Analysen zu fertigen, beispielsweise in der Geldwäschebekämpfung oder in der klinischen Forschung.

Confidential Computing bietet auf der Hardware-Ebene zusätzlich zu den Souveränitätskontrollen die Möglichkeit, Compliance mit technischen Verfahren zu steuern – eine ideale Ergänzung für alle Souveränitätsansätze.

Souveränes Cloud-Ökosystem von T-Systems und Google Cloud

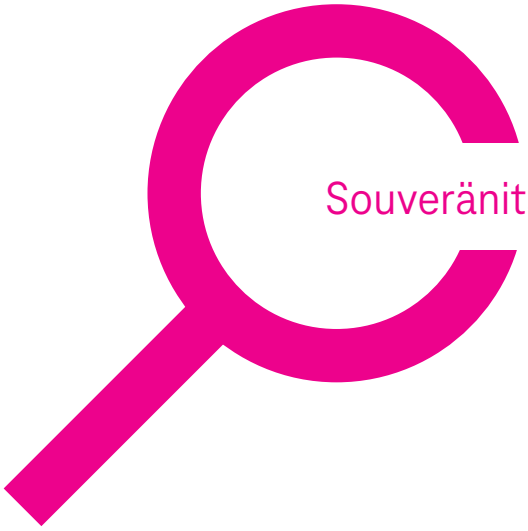
Im April 2022 starteten T-Systems und Google Cloud die T-Systems Sovereign Cloud powered by Google Cloud. Sie bildet ein Ökosystem hochinnovativer und skalierbarer Cloud-Lösungen für unterschiedlichste Souveränitätsanforderungen. Das Angebot verbindet die Open-Source-Expertise von Google Cloud und Sovereign Services von T-Systems. Es richtet sich an alle Unternehmen, den öffentlichen Sektor, das Gesundheitswesen und Kunden mit hoheitlichen Aufgaben in Deutschland, Österreich und der Schweiz, die verschiedene Compliance-Anforderungen, u.a. EU-DSGVO oder Schrems II, erfüllen müssen. Die Cloud wird exklusiv für den DACH-Raum angeboten, kann aber auch von Unternehmen aus anderen Ländern genutzt werden. Google Cloud stellt die technische Plattform bereit, T-Systems steuert die Souveränitätsaspekte bei. Insgesamt werden unter dem Mantel der T-Systems Sovereign Cloud powered by Google Cloud drei verschiedene Clouds für verschiedene Souveränitätsbelange angeboten. Die drei Varianten sind interoperabel, damit werden hybride Szenarien möglich. Die Souveränität der Plattform setzt sich aus drei Komponenten zusammen: Datensouveränität, betriebliche Souveränität und Software-Souveränität.



1 Datensouveränität bedeutet, dass der Eigentümer der Daten die Gewissheit hat, dass seine Daten in der Cloud nicht von Unberechtigten (hierzu zählt auch der Cloud-Betreiber) manipuliert, gelöscht, kopiert oder eingesehen werden. Die Verschlüsselung von Daten erfolgt außerhalb der Cloud-Plattform und die Schlüssel werden in einem externen Key Management verwaltet, so dass der Cloud-Betreiber keinen Zugriff auf die Schlüssel hat.

2 Im Rahmen der betrieblichen oder operationellen Souveränität erhalten Nutzer komplette Transparenz und Kontrolle über die Betriebstätigkeit des Anbieters. Im konkreten Fall erhält T-Systems bspw. die Access Transparency Logs und überwacht auf dieser Basis Google als den Anbieter der Plattform. Der Betreiber/Anbieter der Public-Cloud-Dienste entwickelt den technischen Unterbau der Cloud so weiter, dass die Anpassungen der Plattform das Souveränitätsprinzip nicht untergraben. Damit wird die Zukunftsfähigkeit sowie die volle Leistungsfähigkeit der Plattform sichergestellt.

3 Software-Souveränität markiert eines der wichtigsten Prinzipien der souveränen Cloud: Sie vermeidet, dass Nutzer in Abhängigkeit der Sovereign Cloud geraten (Vendor Lock-in). Applikationen und Dienste bleiben einfach auf eine beliebige andere IT-Infrastruktur (auch in-house) migrierbar. Dies ist auch eine der BaFin-Vorgaben für die Exit-Strategie eines Finanzunternehmens.



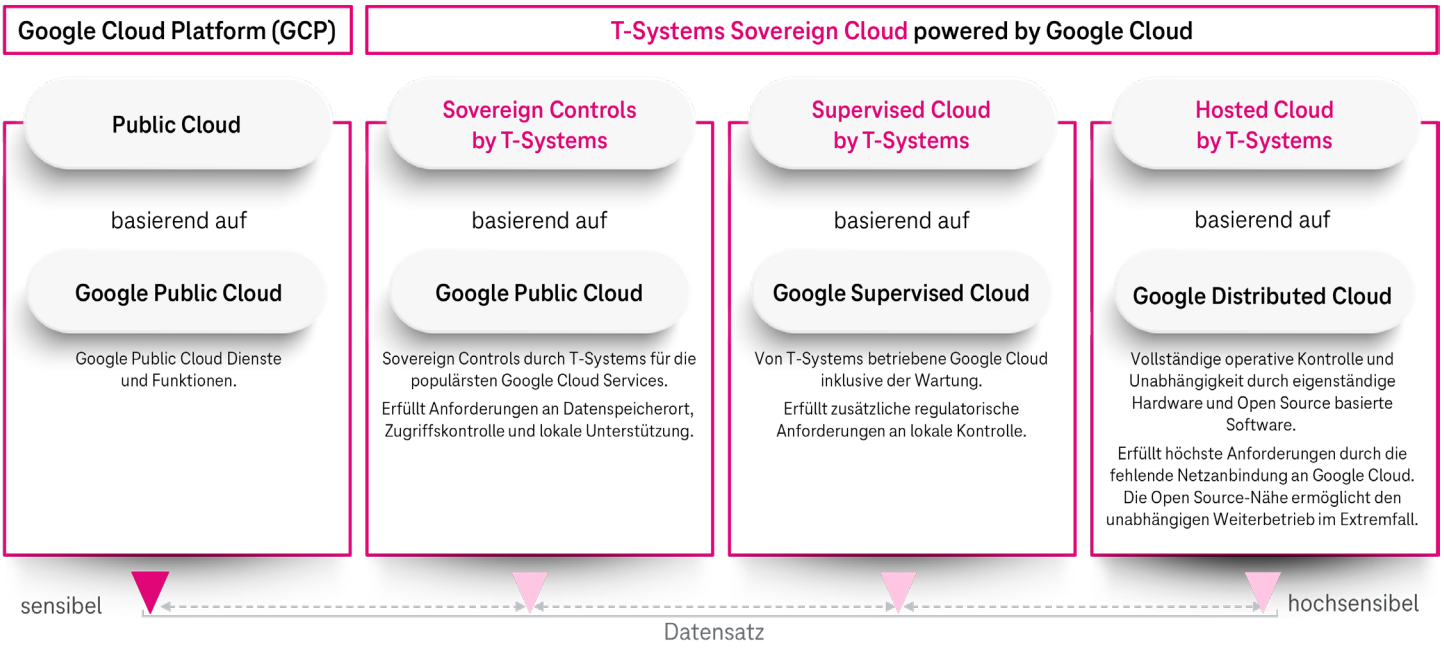
Souveränitätskontrollen

Google Cloud baut für die Sovereign Cloud Souveränitäts-Kontrollpunkte in die Plattform ein und gibt diese Kontrollmöglichkeiten in die Hand von T-Systems. Für den Support der Sovereign Cloud setzt Google nur EU-Mitarbeiter ein. Zu den eingebauten Kontrollpunkten zählen: Zugangskontrolle und -transparenz, Datenresidenz-Kontrolle, Monitoring und externes Schlüsselmanagement (lokal und extern betrieben durch T-Systems). In den späteren Ausbauphasen der Plattform wird zusätzlich das Management der Kundenidentitäten komplett über T-Systems erfolgen. Eine zusätzliche Sicherheitsüberwachung von außerhalb der Plattform wird über ein Security Operations Center (SOC) von T-Systems möglich.

Souveränitätskontrollen im Überblick

Kontrolle der Datenhaltung	Die Daten können nur in Deutschland gespeichert werden.
Lokaler Support und Betrieb	Der Zugriff durch das Personal sowie die Kundenbetreuung erfolgen ausschließlich durch EU-Mitarbeiter mit Sitz in der EU.
Externe Schlüsselverwaltung	Die Schlüssel zur Verschlüsselung der Kundendaten werden von T-Systems gespeichert und verwaltet.
Zugriffskontrolle und -transparenz	Der administrative Zugriff auf Kundendaten und Anwendungen wird protokolliert, geprüft und nur unter vordefinierten Bedingungen freigegeben.
Identitäten-Management	Kundenidentitäten werden von T-Systems verwaltet.
Security Operations Center	T-Systems bietet eine zusätzliche Überwachung des gesamten Cloud-Betriebs.

Varianten der Sovereign Cloud: Die Anforderungen an Souveränität variieren von Branche zu Branche und von Workload zu Workload. Google Cloud und T-Systems werden ein Portfolio von Souveränitätslösungen anbieten. Die T-Systems Sovereign Cloud powered by Google Cloud wird zukünftig neben der bereits heute verfügbaren „Sovereign-Controls"-Basisvariante, die auf der Google Public Cloud beruht, um zwei weitere Varianten mit höherem Souveränitätslevel erweitert.



Mit der **T-Systems Supervised Cloud** bieten die Partner eine Erweiterung der Sovereign Controls um eine physisch getrennte Infrastruktur bei Google Cloud an („Caging").

Die **Hosted Cloud** bietet ein Höchstmaß an Souveränität. Sie richtet sich an Kunden mit höchsten Ansprüchen an sensible Datenhaltung. Sie baut auf der Google Distributed Cloud auf. Diese wiederum basiert auf Google Anthos und garantiert völlige operationelle Kontrolle sowie Unabhängigkeit dank dedizierter Hardware und vollständiger Trennung von der Google Public Cloud („Air Gap"-Fähigkeit). Sie wird von T-Systems betrieben, auf Wunsch auch im Rechenzentrum des Kunden („on premises"). Dank des eingesetzten Open-Source-basierten Software-Stacks erlauben die dort angebotenen Dienste eine Migration auf eine Open-Source-Infrastruktur zu jeder Zeit.

Verfügbare Dienste

Zum Start des Angebots decken die Sovereign Controls zunächst die beliebtesten Google Cloud Services ab:

COMPUTE ENGINE
Im Rechenzentrum von Google laufende virtuelle Maschinen

CLOUD STORAGE
Sicherer, langlebiger, skalierbarer Objektspeicher

KUBERNETES ENGINE
Verwaltete Umgebung für die Ausführung von Container-Anwendungen

CLOUD SQL
Relationale Datenbankdienste für MySQL und PostgreSQL

PERSISTENT DISK
Blockspeicher für VM-Instanzen

Die Sovereign Controls werden kontinuierlich auf weitere Services ausgeweitet. Begonnen wird mit den folgenden aaS-Angeboten:

COMPOSER
Dienst zur Workflow-Orchestrierung auf Basis von Apache Airflow

DATAFLOW
Streaming-Analysen für die Stream- und Batchverarbeitung

DATAPROC
Dienst zum Ausführen von Apache Spark und Hadoop Clustern

PUB/SUB
Messaging-Dienst zum Erfassen und Ermitteln von System-Ereignissen

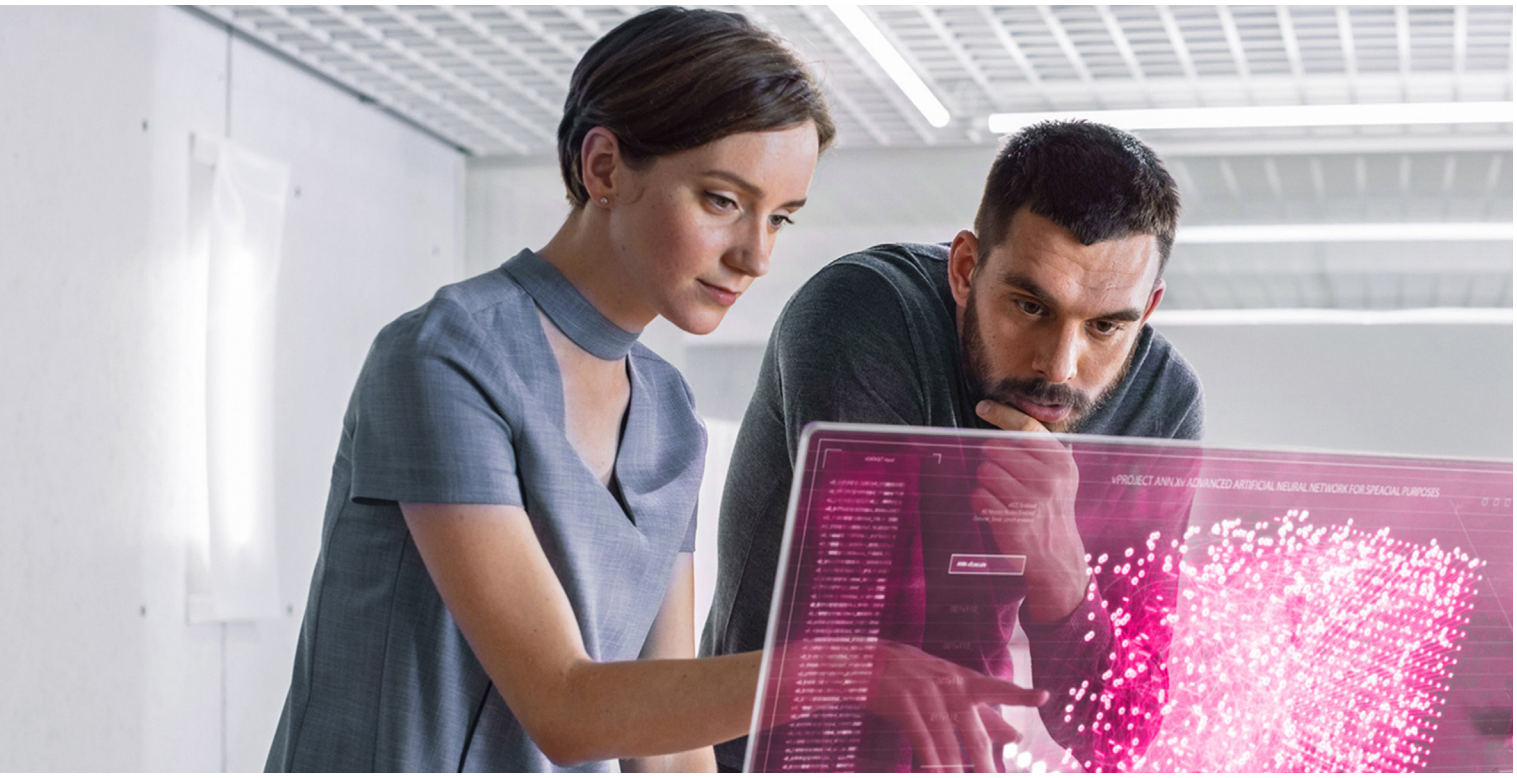
Fazit

Sovereign Clouds versprechen neue Lösungsansätze, bei denen Public Clouds mit der Gesetzgebung und den Regulatorien in spezifischen Märkten verbunden werden. Damit können Sovereign Clouds einen wichtigen Beitrag leisten, um die Digitalisierung in Europa voranzubringen. Die eingebaute Compliance vereinfacht bzw. beschleunigt die Realisierung von Digitalisierungsprojekten und senkt deren Kosten.

Doch wo liegt der Schwerpunkt der Diskussion um souveräne Clouds – auf Seiten der Souveränität oder auf Seiten der Cloud? Wieviel an Mehrkosten, wieviel an Leistungsabstrichen sind Nutzer bereit für garantierte Souveränität hinzunehmen? Und vor allem: Welche Rolle wird die Sovereign Cloud innerhalb einer Multi-Cloud-Welt spielen?

Die T-Systems Sovereign Cloud powered by Google Cloud bietet Unternehmen eine erste Möglichkeit, die Sovereign Cloud zu erproben.

Sie wollen die Möglichkeiten der Sovereign Cloud erkunden?
Sprechen Sie uns an



Quellenangaben

[1] France: Government announces national cloud strategy, May 2021
[2] The Italian Cloud Strategy, September 2021
[3] The European Commission Cloud Strategy, May 2019
[4] IDC FutureScape: Worldwide Cloud 2022 Top 10 Predictions, October 2021

Kontakt

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main, Deutschland

Telefon: 0800 33 09030
E-Mail: info@t-systems.com
Internet: www.t-systems.com

Herausgeber

T-Systems International GmbH
Marketing
Hahnstraße 43d
60528 Frankfurt am Main
Deutschland

T Systems Let's power higher performance