Schluss mit dem Wirrwarr

Cloud-Modell und Datensouveränität beachten

Stand: Februar 2022

Uptime IT GmbH

Süderstraße 282 – 288

20537 Hamburg

www.uptime.de

service@uptime.de

Inhaltsverzeichnis

1 Verantwortungsvoll eine Cloud-Strategie entwickeln

Wird das Internet jetzt Cloud genannt? Wieso beeinflusst das Cloud-Modell Ihre Datensouveränität? Zwei Fragen, deren Antworten einen wichtigen Einfluss auf die Digitalisierungsstrategie Ihres Unternehmens haben.

Um die Zusammenhänge zu verstehen und die erste Frage zu beantworten, ist es wichtig, zwischen Cloud-Infrastruktur und Cloud-Services zu unterscheiden, denn eine Cloud ist nicht mit dem gesamten Internet gleichzusetzen.

Cloud-Services umschreiben die mit Cloud-Technologie bereitgestellten Services wie Webshops, Mail-Postfächer, Dateiablagesysteme, Datenbanken usw. Moderne Bereitstellungsmodelle sind heutzutage cloudbasiert.

Unter Cloud-Infrastruktur versteht man im engeren Sinne das Bereitstellen von Server- und Speichergruppen, die über ein gemeinsames Web-Interface buch- und managebar sind. Dies geht in der Regel mit einer Virtualisierung von Hardware einher, kann aber auch dedizierte Hardware und Mischformen von beidem beinhalten. Wichtig sind die gemeinsame Bereitstellung und das Management in einer Anwendungsoberfläche.

Cloud-Services laufen üblicherweise auf Cloud-Infrastruktur, auf der aber auch andere Anwendungen laufen können, die keine Cloud-Eigenschaften haben. Der Begriff Cloud-Computing ist der Oberbegriff zu Cloud-Services und -Infrastruktur.

Der Prozess der Beschaffung, Bereitstellung und des Managements der verschiedenen Cloud-Produkte beruht meistens auf einer Web-Schnittstelle, die entweder von Menschen oder Maschinen bedient wird. Ebenso kommunizieren Cloud-Produkte in der Regel über Web-Schnittstellen mit Menschen und Maschinen (Machine-To-Machine oder Internet of things).

Für die Cloud-Strategie ist es wichtig, zu entscheiden, ob man seine Datensouveränität erhalten möchte oder es dem eigenen Unternehmen gleichgültig ist, wenn die Daten von Dritten mitgelesenen werden können.

2 Datensouveränität behalten

Die verschiedenen Spielarten des Cloud-Computings beziehen sich maßgeblich auf den Bereitstellungsort und die Managementverantwortung für Infrastruktur und Services. Diese beiden Parameter haben wesentlichen Einfluss hinsichtlich der Datensouveränität eines Unternehmens und damit auf den Schutz der Betriebsgeheimnisse und den Datenschutz; aber auch auf die Flexibilität hinsichtlich eines eventuellen Anbieterwechsels.

Tabelle 1 zeigt die grundlegenden Faktoren, die zum Erhalt der Datensouveränität beitragen. Man unterscheidet zwischen ruhenden Daten, der Datenübertragung und der Datenverarbeitung. Die Verschlüsselung von ruhenden Daten und Übertragungswegen gilt als Mindeststandard. Die Datenverarbeitung erfolgt technisch bedingt im RAM und in der CPU immer unverschlüsselt. Daher benötigt es hierbei ein besonderes Vertrauensverhältnis zum jeweiligen Dienstleister. Es ist weiterhin wichtig, den jeweiligen Rechtsraum des Providers zu beachten.

Tabelle 1: Der für einen Provider geltende Rechtsraum und die Verschlüsselung von Daten beeinflussen die Datensouveränität bei Cloud-Lösungen.

	Für den Provider geltender Rechtsraum	Verschlüsselung
Ruhende Daten	Für Datensouveränität zwingend zu beachten, z.B. bei Providern mit US-amerikanischen Wurzeln gelten auch in Deutschland US-Gesetze, wie z.B. der US-Cloud-Act	ja
Datenübertragung	-	ja
Verarbeitungsort	Für Datensouveränität zwingend zu beachten, z.B. bei Providern mit US-amerikanischen Wurzeln gelten auch in Deutschland US-Gesetze, wie z.B. der US-Cloud-Act	Verschlüsselung ist technisch noch nicht realisierbar. Daher ist ein uneingeschränktes Vertrauensverhältnis zum Provider Voraussetzung

3 Die Private Cloud im B2B-Umfeld

Im Unternehmenskontext spielen vier Varianten der Private Cloud eine Rolle, die im Folgenden skizziert werden. Alle Varianten zeichnen sich durch die uneingeschränkte Datensouveränität des Unternehmens aus.

3.1 On-Premises

Hierbei befinden sich die Cloud-Infrastruktur und/oder die Cloud-Services auf eigenen Servern und auf dem eigenen Firmengelände. Die Vorteile: Ein Unternehmen betreibt beide Komponenten für sich selbst, ist also der Besitzer und hat die volle Datensouveränität. Nachteile bestehen in Hinblick auf die Administration, die Investitionen und Skalierbarkeit sowie auf die vielfältigen Aspekte rund um das Gebäude- und Zutrittsmanagement.

3.2 Hosted Private Cloud

Bei diesem Modell steht Ihre eigene Hardware bei einem Provider oder wird bei einem Provider ausschließlich an ein Unternehmen vermietet oder bereitgestellt.

Vorteile: Bei diesem Modell spart man den gesamten Gebäudeaufwand, beginnend bei Fläche, Klima, Strom und Zutrittssteuerung und Internetanbindung.

Nachteile: Durch eigene Hardware und darauf zu installierende und betreibende Services bleibt der Aufwand dafür mit allen Folgen weiterhin in Eigenverantwortung.

3.3 Leased Private Cloud

Dieses Modell ist dem der Hosted Private Cloud sehr ähnlich. Die Hardware gehört jedoch dem Provider und liegt meistens in einer vom Provider vorgegebenen genormten Konfiguration vor.

Vorteile: Der Kunde ist alleiniger Nutzer der Hardware. Durch die providerseitige Normung gibt es zwar technische Begrenzungen, allerdings auch Qualitäts- und Preisvorteile bei Bereitstellung und Management. In der Regel können in diesem Modell auch die Zertifizierungen und Prüfungen des Providers auf die bezogene Leistung angewandt und anerkannt werden.

Nachteile: Im Vergleich zur Virtual Private Cloud verzichtet ein Kunde auf kaufmännische Vorteile, meistens ohne dafür einen technologischen Mehrwert zu erhalten.

3.4 Virtual Private Cloud

Bei dieser Dienstleistung wird ein Provider oder externer Dienstleister mit dem Management des Cloud-Computings beauftragt. Zu diesem sollte ein angemessenes Vertrauensverhältnis bestehen, denn bei der Verarbeitung von Daten liegen diese unverschlüsselt in den Anwendungen vor.

Dieses Cloud-Model basiert darauf, dass die Hardware dem Provider gehört und der Kunde eine darauf virtualisierte IT-Infrastruktur nutzt. Mittels Hypervisors der Virtualisierungssoftware und vLAN-Netzwerk findet eine verlässliche Abgrenzung der jeweiligen Kundeninstallationen statt. Die heutzutage dafür eingesetzten Technologien sind so gut, dass es allgemein anerkannt ist, dass eine dedizierte Hardware wie bei der Leased Cloud keinen Vorteil mehr bezüglich der Datensouveränität gegenüber der Virtual Private Cloud bietet.

Vorteile: Der Kunde profitiert von einer vereinheitlichten, auf dem aktuellen Stand der Technologie befindlichen Infrastruktur unter Ausnutzung von Skaleneffekten, einfacher Bereitstellungsmethoden, geringer Providerbindung und kontinuierlicher Technologieentwicklung. Kapitalbindende Investitionen entfallen vollständig.

Nachteile: Der Kunde verliert die Möglichkeit der vollständigen Individualisierung (das kann aber auch ein Vorteil sein!).

Aufgrund der großen Marktbedeutung bezeichnet man heutzutage diese Variante auch verallgemeinernd mit „Private Cloud“.

Tabelle 2 Übersicht der wichtigsten Private Cloud Modelle

	Beschreibung	Vorteile	Nachteile
On-Premises	Cloud-Infrastruktur und/oder Cloud-Services befinden sich auf eigenen Servern und auf dem eigenen Firmengelände.	Unternehmen betreibt Cloud-Infrastruktur und -Services für sich selbst, ist also der Besitzer und hat die volle Datensouveränität.	Nachteile ergeben sich in Hinblick auf die Administration, die Investitionen und Skalierbarkeit sowie auf die vielfältigen Aspekte rund um das Gebäude- und Zutrittsmanagement.
Hosted Private Cloud	Unternehmenseigene Hardware steht beim Provider oder wird bei einem Provider ausschließlich an einen Kunden vermietet oder ihm bereitgestellt.	Einsparungen am gesamten Gebäudeaufwand, beginnend bei Fläche, Klima, Strom und Zutrittssteuerung und Internetanbindung. Volle Datensouveränität.	Durch eigene Hardware und darauf zu installierende und betreibende Services bleibt der Aufwand dafür mit allen Folgen weiterhin in Eigenverantwortung.

Leased Private Cloud	Die von einem Kunden zu mietende Hardware gehört dem Provider und liegt meistens in einer vom ihm vorgegebenen genormten Konfiguration vor. Der Kunde ist alleiniger Nutzer der Hardware.	Durch die providerseitige Normung gibt es zwar technische Begrenzungen, allerdings auch Qualitäts- und Preisvorteile bei Bereitstellung und Management. In der Regel können in diesem Modell auch die Zertifizierungen und Prüfungen des Providers auf die bezogene Leistung angewandt und anerkannt werden. Volle Datensouveränität.	Im Vergleich zur Virtual Private Cloud verzichtet ein Kunde auf kaufmännische Vorteile, meistens ohne dafür einen technologischen Mehrwert zu erhalten.
Virtual Private Cloud	Provider wird mit dem Management des Cloud-Computings beauftragt. Zu diesem sollte ein angemessenes Vertrauensverhältnis bestehen, denn die Daten liegen unverschlüsselt in den Anwendungen vor. Der Kund betreibt auf der Hardware seine virtualisierte IT-Infrastruktur.	Vereinheitlichte, auf dem aktuellen Stand der Technologie befindliche Infrastruktur, Ausnutzung von Skaleneffekten, einfache Bereitstellungsmethoden, geringer Providerbindung und kontinuierlicher Technologieentwicklung. Kapitalbindende Investitionen entfallen vollständig. Volle Datensouveränität	Der Kunde verliert die Möglichkeit der vollständigen Individualisierung (das kann aber auch ein Vorteil sein!).

3.5 Gemeinsamkeiten aller Private Cloud Lösungen

Alle Kundenserver und -Workstations sind kundenspezifisch. Auch wenn es sich um virtuelle Maschinen handelt, sind die Betriebssysteme die Betriebssysteme eines einzigen Kunden. Das Gleiche gilt für die jeweiligen Netzwerke, die diese Systeme verbinden. Diese sind so voneinander getrennt, dass andere Kunden den Datenverkehr nicht sehen können. Ebenso sind in der Konsequenz auch alle Datenhaltungssysteme kundenindividuell, speziell Dateisysteme und Datenbanken. Insbesondere gibt es keinerlei Datenbanken, die von mehreren Kunden gleichzeitig verwendet werden. Dies beginnt bei Authentifizierungssystemen, wie z.B. Active Directory, und geht bis hin zu Monitoring und Managementsystemen.

Kurzum: Alle Lösungen werden individuell bereitgestellt und mit keinem anderen Kunden geteilt.

4 Herausforderungen für die Datensouveränität: Public Cloud

Bei Public-Cloud-Services stehen die gemeinsame Bereitstellung und Verwendung im Vordergrund. Beispiele: In einem Active Directory wird das gesamte Anmeldeverfahren sämtlicher Kunden eines Großanbieters abgebildet, auf einem SQL-Server werden für alle Kunden gemeinsam Instanzen und Platz vermietet, und von einem anderen Cloud-Anbieter wird Speicherplatz vermietet. Die Cloud-Applikationen werden also nicht für jeweils einen Kunden installiert.

In einer Public Cloud stellt der Provider zentrale Applikationsdienste bereit, in denen alle Kunden ihre Daten speichern und verarbeiten. Die Abgrenzung zwischen den Kunden findet nicht auf Basis von (virtueller) Hardware und Netzwerken statt, sondern alleine durch die Applikation des Providers selbst.

Dieses Modell verlangt vom Kunden Vertrauen nicht nur zum Provider und seiner Organisation, sondern auch zu den Fähigkeiten des Providers, diese Abgrenzungen mit den jeweiligen Entwickler- und Wartungsmannschaften lückenlos zu erstellen.

Vorteile: Das Bereitstellungsmodell ist schneller, einfacher und skaliert hervorragend. Da der Service als Public Cloud Service vorhanden ist und der Kunde nur die Teilnahme bucht, entfällt die Bereitstellung von Netzen, Betriebssystemen und Anwendungen. Der Kunde bucht den Service mit Qualität und Menge, kann in der Regel die Menge beliebig mehren und mindern und bekommt den tatsächlichen Verbrauch abgerechnet.

Nachteile: Die Public Cloud Services sind auch dann, wenn sie auf quelloffenen Lösungen basieren, fast immer Einzellösungen vom jeweiligen Anbieter. Ebenso finden bei den großen Anbietern „Verbesserungen“ an den allgemein zugänglichen Lösungen statt, die zu individuellen Schnittstellen-implementierungen und Lösungsverhalten führen.

Dies führt nahezu immer zu einem Provider- oder Vendor-Lock-in (Anbieterbindung). Anders als bei der Virtual Private Cloud ist bei einem Providerwechsel z.B. ein einfacher Umzug durch Down- und Upload der gesamten App mit ihrem Datenbestand ausgeschlossen. Dadurch entstehen Abhängigkeiten mit all ihren Konsequenzen.

Beachtung sollten auch weitere Aspekte finden: Welche Möglichkeiten der Kontrolle und Weisung bestehen gegenüber dem Cloud-Provider? Kann im Bedarfsfall auf Sonderwünsche reagiert werden? Ist der Provider auditfähig, so dass das beauftragende Unternehmen den eigenen qualitativen oder rechtlichen Anforderungen entsprechen kann?

Unter Beachtung dieser Aspekte kann eine solide Entscheidung gefällt werden, ob das Private oder Public Cloud-Modell für ein Unternehmen und den gewünschten Anwendungsfall geeignet ist. Unternehmen, die Betriebsinterna schützen und damit den eigenen wirtschaftlichen Fortbestand bewahren wollen, sind gut beraten, sich auf unabhängige, deutsche Unternehmen zu verlassen.

4.1 Datensouveränität vs. Regierungsinteressen

Die großen Public Cloud Anbieter (Hyperscaler) sind amerikanische oder chinesische Unternehmen, die bezüglich der Datensouveränität – selbst dann, wenn sie deutsche Niederlassungen gegründet haben – den Gesetzen, Weisungen und Interessen ihrer eigenen Regierungen unterworfen sind. Die Wahrung von Geschäftsgeheimnissen obliegt angesichts der weitreichenden Befugnisse von beispielsweise US-Behörden und -Geheimdiensten und dem Datenhunger mancher Anbieter jedem Kundenunternehmen selbst.

Bei Beauftragung von Providern in Drittstaaten mit besonders extensiven Zugriffsrechten durch Behörden ergeben sich aufgrund des Datenschutzniveaus der EU besondere Anforderungen, wobei auch die Beachtung der neuen europäischen Standardvertragsklauseln wohl keinen risikofreien Datentransfer ermöglichen. Hinzu kommen hohe Dokumentations- und Rechtspflichten für den jeweiligen Auftraggeber.

5 Uptime IT

Die Uptime IT GmbH ist ein inhabergeführtes, unabhängiges deutsches Familienunternehmen mit über 30 Jahren Erfahrung in den Bereichen Cloud-Infrastruktur, Managed Hosting und Kubernetes sowie IT-Outsourcing. Ein besonderes Augenmerk legt das umfassend ISO-zertifizierte sowie nach ISAE 3402 Typ 2 geprüfte Unternehmen auf Hochverfügbarkeit, Datensouveränität und -sicherheit.

Unternehmen aus diversen Branchen und verschiedenster Größenordnungen betreiben ihre geschäftskritischen Anwendungen auf der Uptime IT eigenen Infrastruktur. Diese wird georedundant in zwei eigenen Datacentern in Hamburg betrieben. Die erfahrenen Uptime IT Mitarbeiter nutzen weltmarktführende Technologien und sehen sich höchster Qualität und einer partnerschaftlichen Beziehung zu allen Kunden verpflichtet.

6 Tabellarische Zusammenfassung

Tabelle 3 zeigt die Verantwortlichkeiten bei den vorgestellten Cloud-Modellen

		Hardware gehört	Hardware steht bei	Hardware gemanagt von	Betriebssysteme und Datenbanken gemanagt von	Cloud Services	Anwendungen** und Datenspeicher für # Kunden
Private Cloud	On-Premise	Unternehmen	Unternehmen	Unternehmen	Unternehmen	Unternehmen	1
	Hosted	Unternehmen	Provider	Unternehmen	Unternehmen	Unternehmen	1
	Leased	Provider	Provider	Provider	Unternehmen	Unternehmen	1
	Virtual	Provider	Provider	Provider	Unternehmen	Unternehmen	1
Public Cloud*	Public	Provider	Provider	Provider	-	Provider	∞

* Public Cloud im Sinne von Hyperscaler

** Anwendungen in der Public Cloud: z.B. Datenbanken, Dateiablage, Rechenleistung für AI etc., häufig Anbieterbindung

Multi-Cloud bedeutet, dass ein Unternehmen verschiedene Private- und/oder Public-Cloud-Modelle nutzt und diese getrennt voneinander verwaltet. Der Hybrid-Cloud-Ansatz setzt auf eine Verknüpfung zumindest auf der Managementebene der unterschiedlichen Clouds.