Hintergrundinformation Safe Harbor

Oktober 2015

Zwei Fliegen mit einer Klappe

Gesetzeskonforme Lösung für die hybride Cloud: So entsprechen Unternehmen dem Datenschutz

Wer heute die Public Clouds großer US-amerikanischer Anbieter für operative Unternehmensdaten verwenden möchte, wird schnell durch die Vorgaben des deutschen Datenschutzes ausgebremst. Durch Nutzung von Colocation-Rechenzentren und Datenmanagement-Software von NetApp sind CIOs in der Lage, Multi-Cloud-Umgebungen zu realisieren und gleichzeitig die volle Datenkontrolle zu behalten.

Der CIO muss bei Nutzung der Cloud neben den rechtlichen Rahmenbedingungen auch die technisch-organisatorischen Schutzmaßnahmen sowie eine jederzeit verfügbare und hoch performante Systemleistung sicherstellen. Problematisch ist hierbei, dass beim klassischen Outsourcing-Modell die Daten in der Cloud verarbeitet werden und nicht aus der Cloud. Der Unterschied von „in“ und „aus“ kann hierbei rechtlich relevant sein. So ist die Weitergabe von Daten in die USA – hier sitzen die Betreiber der großen Public Clouds – als „unsicheres Drittland“ im datenschutzrechtlichen Sinne nur zulässig, wenn bei der Empfängerstelle ein angemessenes Datenschutzniveau hergestellt wird und dies durch die entsprechende Zertifizierung bestätigt wird. Die hierzu konzipierte Safe Harbor-Zertifizierung gilt jedoch in ihrer aktuellen Ausformung als nicht mehr geeignet, ein angemessenes Datenschutzniveau zu gewährleisten. Nachdem zuletzt auf der Ebene der nationalen Datenschutzbehörden massive Zweifel an der Effektivität des Safe Harbor-Prinzips aufgekommen waren, hat auch der Europäische Gerichtshof (EuGH) mit Urteil vom 06.10.2015 diese Regelung zum Austausch von Daten zwischen den USA und der EU für ungültig erklärt.

Ein CIO sollte daher den Outsourcing-Prozess mit Blick auf das strenge rechtliche Rahmenwerk für die Übermittlung bestimmter Datenkategorien in Clouds außerhalb des EU-Raumes umkehren. Haben Unternehmen ihre Daten allerdings bereits in die Cloud verschoben, stehen sie oftmals vor dem Problem, diese wieder auf effiziente Art ins eigene Rechenzentrum zu holen. Gleiches gilt für die zwingend gebotene Löschbarkeit der in die Cloud ausgelagerter Daten, die – trotz Zusicherungen durch den Cloud-Anbieter – oftmals de facto nicht gegeben ist.

Verarbeitung von Workloads in der Cloud

Mit einer (privaten) „Cloud an der Cloud“ lassen sich bestimmte Services in die Cloud hinein erweitern. Hierzu betreibt das Unternehmen in einem Colocation-Rechenzentrum ein eigenes Storage-System, auf dem sich operative Daten befinden. Das Rechenzentrum befindet sich in unmittelbarer geografischer Nähe zu den großen Public Cloud-Anbietern, wodurch sehr niedrige Latenzzeiten und somit hohe Zugriffsraten auf Netzwerkebene möglich werden. Solche Colocation-Angebote unterstützen eine Trennung von Storage und Compute. So realisieren Unternehmen eine neue Art von hybrider Cloud: Während die großen Datenmengen in On-Premise Storage-Systemen verbleiben, können Fachabteilungen ihre Workloads (Rechenleistung) flexibel und nach Bedarf in die Cloud auslagern.

Hybride Cloud ermöglicht Unternehmen Kontrolle über Daten

Mit der so realisierten Cloud findet eine Datenverarbeitung statt, ohne dass die operativen Daten in die Public Cloud des Anbieters verschoben werden. Dieses Modell gibt in datenschutzrechtlicher Hinsicht Anlass zu einer Neubewertung gegenüber den klassischen Modellen der Datenübermittlung und kann wesentlich weitere Spielräume für die Nutzung von globalen Clouds eröffnen. Mit einer solchen Lösung müssen Unternehmen die eigentlichen Daten nicht bewegen. Diese bleiben stattdessen in einem Storage-System unter der Kontrolle des Unternehmens gespeichert. Die gebuchten Public Cloud-Services (Rechenleistung, Applikationen und weitere „as a“-Services) greifen dann zu bestimmten Zeiten auf diese Daten zu. Mit Abschluss der Datenverarbeitung melden sich die Services wieder ab und ziehen sich aus den Datenbeständen zurück. Die Anwendungen können die Daten verarbeiten und ändern, auf deren Basis Ergebnisse erzeugen und Auswertungen erstellen. Dabei nimmt das Unternehmen jedoch lediglich den Vorgang des „Computing“ selbst, aber keine Speicherressourcen der Cloud an sich in Anspruch. Im Rechtssinne findet daher zu keinem Zeitpunkt eine „Datenübermittlung“ in die Cloud statt. Die Daten bleiben hierbei stets auf dem im Unternehmen stehenden Server.

Datenschützer könnten jetzt argumentieren, dass zwar keine Datenübermittlung gegeben ist, jedoch eine Auftragsdatenverarbeitung. Bei herkömmlicher Cloud-Nutzung trifft dies auch zu, da diese Dienste ähnlich wie ein Outsourcing-Prozess organisiert sind. Das Verfahren mit zwischengeschaltetem Colocation-Anbieter hingegen nutzt die Cloud als eine Verlängerung der eigenen IT-Ressourcen und ohne explizite Übergabe der Daten in eine Drittverantwortung. Es erfolgt eine Art blinde Datenverarbeitung, bei der die IT-Prozesse vom Unternehmen aus gestartet und durchgängig kontrolliert werden. Die Datenverarbeitung erfolgt also mit flüchtigen Prozessen und unter überwiegender Verwendung des Arbeitsspeichers. Dies erlaubt die Betrachtung, dass sich ein Unternehmen die Rechenleistung ins eigene Haus holt und nicht die Cloud als eine Art Outsourcing-Service nutzt.

Entscheidendes Kriterium ist hier die Kontrolle über die Datenverarbeitung. Das Cloud-Rechenzentrum beschränkt sich darauf, für die Einsatzbereitschaft zu sorgen und über die Dauer der Nutzung Buch zu führen. Die Verantwortung für den Datenschutz verbleibt beim Unternehmen.

Fazit

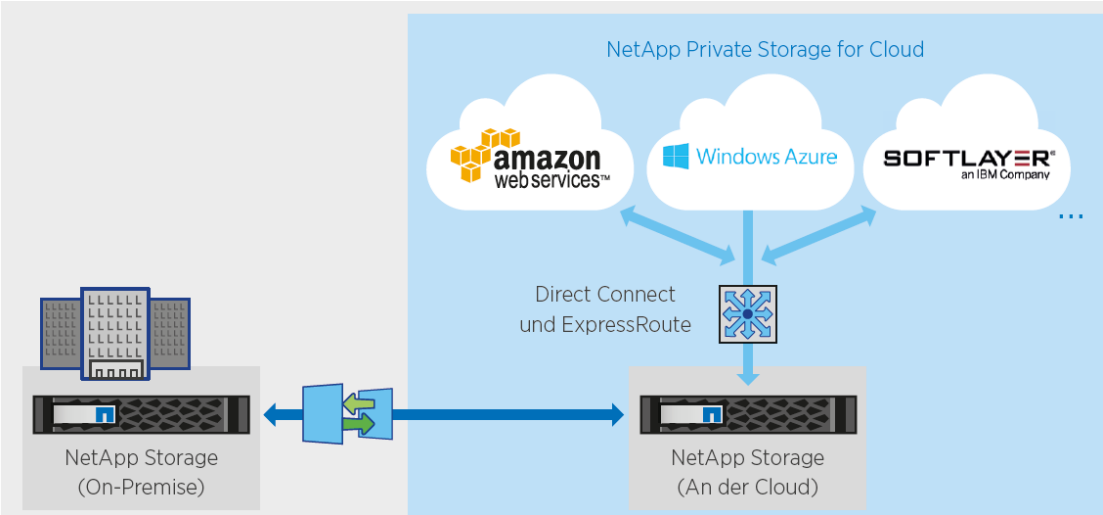
Die Art der hier gezeigten Infrastrukturnutzung gilt daher nicht als Datenübermittlung im eigentlichen Sinn. Sie stellt nicht einmal eine Auftragsdatenverarbeitung dar, wenn das Unternehmen sich lediglich fremder Infrastruktur bedient. Da die Daten auf dem eigenen Storage-System des Unternehmens gespeichert bleiben, ist die vollständige Kontrollhoheit gewährleistet. Diese Konstellation gilt als technische Verlängerung eines unter Eigenkontrolle stehenden IT-Systems. Bei diesem Konzept gelten nicht die strengen Voraussetzungen an eine Datenübermittlung in Drittstaaten. Auch gilt sie nicht als Auftragsdatenverarbeitung in klassischen Sinne, die sonst vertraglich und kontrolltechnisch abzusichern wäre.

Technologie-Briefing

Das Data Fabric-Konzept von NetApp

Das von NetApp entwickelte Data Fabric-Konzept zeigt, wie Unternehmen eine Multi-Cloud-Infrastruktur realisieren. Mit Technologien wie dem Speicherbetriebssystem Data ONTAP behalten Unternehmen bei Nutzung der Public Cloud auch weiterhin die volle Datenkontrolle. IT-Verantwortliche können so ihre Daten unabhängig von Speicherorten wie On-Premise, bei

Service Providern oder in der Public Cloud jederzeit frei verschieben und transparent verwalten.



In einer solchen Multi-Cloud-Umgebung sorgen die Colocation-Center, die mit NetApp Storage-Systemen ausgerüstet sind, dafür, dass kritischen Unternehmensdaten nachhaltig geschützt sind. Durch die Wahl eines Colocation-Centers in Deutschland oder Europa können Unternehmen die jeweils gültigen Datenschutzrichtlinien unterstützen und die entsprechenden Compliance-Anforderungen erfüllen. Bei den Colocation-Anbietern arbeitet NetApp beispielsweise mit Equinix zusammen. Das global aufgestellte Unternehmen verfügt über weltweite Rechenzentren und betreibt auch in Deutschland Colocation-Center mit schnellen Public Cloud-Anbindungen. Insgesamt bietet diese Lösung also eine vollständige Kontrolle über die eigenen Unternehmensdaten: CIOs erfüllen damit die Anforderungen an die Daten-Compliance, da jederzeit transparent ist, wo sich die Daten befinden und gleichzeitig bleibt die Datenkontrolle beim Unternehmen.

Quellen

Whitepaper: „NetApp Private Storage for Cloud – eine Stellungnahme unter Anlegung europäischer Datenschutzstandards“, Autor: Dr. Jens Bücking, Rechtsanwalt und Fachanwalt für IT-Recht. Internet: www.netapp.de

Pressekontakt

NetApp Deutschland GmbH
Ursula-Barbara Schmidt
Sonnenallee 1
85551 Kirchheim bei München
Tel.: 089 900 594-192
ursula-barbara.schmidt@netapp.com

Hill+Knowlton Strategies

Sabine Roth
Darmstädter Landstraße 112
60598 Frankfurt
Tel.: 069 97362-41
sabine.roth@hkstrategies.com