Cloud-Lösungen

Vollständige Kontrolle ist eine Illusion

[09.07.2025] Für Behörden und regulierte Branchen gewinnen souveräne Cloud-Lösungen an Bedeutung. Doch was genau bedeutet Souveränität in der Cloud? Jochen Malinowski von Accenture gab auf einer Presseveranstaltung einen Überblick über verschiedene Ansätze – von der Public Cloud mit Einschränkungen bis hin zu vollständig isolierten Rechenzentren.

Cloud-Lösungen sind aus der digitalen Infrastruktur nicht mehr wegzudenken, auch nicht im öffentlichen Sektor. Bei der Nutzung von Angeboten großer internationaler Anbieter wie Amazon Web Services (AWS), Microsoft Azure oder Google Cloud stellen sich jedoch Fragen nach Datenschutz und Kontrolle. Auf einer Online-Veranstaltung des Beratungsunternehmens Accenture für die Presse am 8. Juli 2025 stellte Jochen Malinowski, Geschäftsführer Cloud, Software und Infrastruktur, aktuelle Entwicklungen rund um souveräne Cloud-Angebote vor und erläuterte die Anforderungen an eine solche Infrastruktur.

Unterschiedliche Definitionen

Gleich zu Beginn machte Malinowski deutlich, dass der Begriff souveräne Cloud unterschiedlich ausgelegt wird. „Jede und jeder versteht etwas anderes darunter“, sagte er. In einem von Accenture gegründeten Kompetenzzentrum für souveräne Clouds wird deshalb zunächst geklärt, warum Kundinnen und Kunden eine solche Lösung überhaupt benötigen und für welche Daten sie relevant ist (wir berichteten). Dabei zeigt sich regelmäßig, dass es nicht um eine allgemeine, sondern um eine abgestufte Lösung für unterschiedliche Datenarten geht. Grundsätzlich umfasse Souveränität laut Malinowski drei Aspekte: die Kontrolle darüber, wo die Daten gespeichert werden, wer auf sie zugreifen darf und wer die Cloud-Infrastruktur betreibt.

Technische Abstufungen

Der Vortrag bot einen Überblick über die verschiedenen Ausprägungen souveräner Cloud-Angebote. Am einen Ende des Spektrums stehen vollständig abgeschottete Rechenzentren mit lokaler Hardware und ohne Verbindung zu US-Anbietern. Am anderen Ende des Spektrums befindet sich die klassische Public Cloud, bei der die Daten auf Servern internationaler Konzerne, oft in den USA, liegen und der Betreiber vollen Zugriff hat.

Dazwischen gibt es zahlreiche Zwischenstufen. Viele Anbieter versuchen, ihre Public-Cloud-Dienste mithilfe technischer Maßnahmen anzupassen. So bietet Microsoft beispielsweise eine Sovereign Cloud, bei der bestimmte Zugriffe von außen nur mit Zustimmung der Kundin oder des Kunden erfolgen dürfen. Auch können Schlüssel zur Datenverschlüsselung lokal verwaltet werden. Laut Malinowski richten sich diese Lösungen vor allem an Organisationen, die gewisse Kontrolle benötigen, aber dennoch nicht auf die umfangreichen Dienste großer Anbieter verzichten wollen.

AWS geht einen anderen Weg. Der Amazon-Konzern plant, Ende 2025 eine AWS Sovereign Cloud in Brandenburg zu eröffnen. Diese soll von einem rechtlich unabhängigen Unternehmen betrieben werden. Auch hier ist das Ziel, den Zugriff aus den USA auszuschließen.

Deutsche Alternativen

Zunehmend treten auch europäische Anbieter auf den Markt. Dazu zählen Unternehmen wie Ionos, die Deutsche Telekom oder Schwarz Digits, eine Tochter des Handelsunternehmens Schwarz, mit dem Cloudprovider Stackit. Diese Unternehmen betreiben ihre Rechenzentren in Deutschland oder Europa und versprechen volle Kontrolle über Daten und Betrieb. Allerdings können diese Anbieter laut Malinowski derzeit noch nicht den gesamten Funktionsumfang internationaler Cloud-Dienste bieten, insbesondere nicht bei KI-Anwendungen oder spezialisierten Softwarediensten. Einige Organisationen stünden daher vor der Frage, ob sie auf bestimmte Funktionen verzichten oder Sicherheitsbedenken in Kauf nehmen wollten.

Besondere Konstruktionen

Malinowski stellte ein spezielles Modell am Beispiel der Delos Cloud vor. Dabei handelt es sich um eine Microsoft-Cloud-Lösung, die von der SAP-Tochter Delos und dem Dienstleister Arvato in Deutschland betrieben wird (wir berichteten). Die Daten liegen in Deutschland und der Zugriff erfolgt ausschließlich durch deutsches Personal. Updates aus den USA werden zunächst geprüft und erst nach Freigabe installiert. Das Ziel besteht darin, den US-Einfluss technisch und organisatorisch zu minimieren.

Multi-Cloud-Strategie für den Public Sector

Laut Malinowski werde sich in der Praxis der öffentlichen Verwaltung ein Multi-Cloud-Ansatz als Mischmodell durchsetzen. Hochsensible Daten, etwa Verschlusssachen, könnten in der vom ITZBund betriebenen Bundescloud gespeichert werden. Weniger kritische Informationen, wie die Inhalte öffentlicher Webseiten, lassen sich dagegen problemlos in der Public Cloud ablegen.

Eine vollständige digitale Souveränität sei technisch kaum möglich. „Man kann sich ihr jedoch annähern“, sagte Malinowski. Doch auch in einer souveränen Cloud könnten Komponenten aus den USA stecken, beispielsweise in Chips oder Netzwerkkomponenten. Zudem bleibt der Softwarecode oft im Besitz amerikanischer Firmen. „Die vollständige Kontrolle über jede Ebene ist illusorisch“, so seine Einschätzung.

()

Stichwörter: Digitale Souveränität, Accenture, Cloud, Cloud-Infrastruktur, Delos Cloud, Google Cloud, Microsoft