Regulierte Branchen und die Unsicherheit bei der Auslagerung in die Cloud

Organisationen in streng regulierten Branchen, die ihre IT in die Cloud auslagern, lösen damit die Daten- und Informationssicherheitsprobleme nicht per se. Sicherheitskonzepte müssen angepasst und Lieferanten auf die Einhaltung von Branchenstandards, Regulatorien und Gesetzen hin geprüft werden.

DER AUTOR

Marc Zimmermann
Head of Cloud Services und Member des Leadership-Teams, UMB

Den Beitrag finden Sie auch online
www.netzwoche.ch

In den regulierten Branchen gelten strenge Vorschriften und Gesetze hinsichtlich Sicherheit, Informations- und Datenschutz. Diese gehen über die allgemeingültigen Datenschutzgesetze hinaus. Banken und Versicherungen etwa unterliegen den Auflagen der schweizerischen Finanzmarktaufsicht Finma. Lagern sie ihre IT in die Cloud aus, übergeben sie damit in der Regel zumindest Teile der Security-Aufgaben, etwa die physische Sicherheit, an ihren Lieferanten. Dennoch gilt es, diese auf die korrekte Einhaltung entsprechender Massnahmen hin zu prüfen. Cloud-Anbieter können sich aber nicht von einer Regulierungsbehörde zertifizieren lassen. Lediglich externe Auditoren können prüfen, ob nach den geltenden Regeln gearbeitet wird. Aber auch die Betriebsorganisation des Anbieters und die Cloud-Umgebung, welche die Kunden konfigurieren, müssen den Kontrollen standhalten. Für die Cloud-Umgebung ist nicht der Cloud-Anbieter verantwortlich, sondern der Kunde selbst. Hyperscaler stellen dafür besondere Compliance-Dashboards zur Verfügung, die den Konfigurationen gegenübergestellt werden können.

Integrierte Sicherheitstechnologien auch bei Hyperscalern

Finanz- oder Handelsunternehmen wiederum, die mit Kreditkarten als Zahlungsmittel operieren, müssen den PCI-DSS-Nachweis (Payment Card Industry Data Security Standard) erbringen. Im Falle einer Cloud-Auslagerung müssen sie deshalb den Lieferanten regelmässig hinsichtlich Firewalls, Passwörter und Datenschutz bei den Kreditkarteninhabern, Pflege der Sicherheitssysteme, Zugriffskontrolle etc. prüfen oder prüfen lassen.

Auch in anderen, streng regulierten Branchen haben sich Sicherheitsstandards etabliert – etwa bei den Wirtschaftsprüfern der internationale ISAE-Standard 3402, in dem die Prüfung eines internen Kontrollsystems bei Dienstleistungsunternehmen geregelt ist. Auch hier gilt: Mit der Auslagerung der IT in die Cloud sind Unternehmen nicht aus der Verantwortung. In regulierten Branchen werden aus dieser Unsicherheit heraus Public Clouds oft (noch) nicht vollständig genutzt. Dabei bieten Hyperscaler mittlerweile Sicherheitsmechanismen, die mit On-Prem-Lösungen viel schwieriger und aufwendiger anzuwenden und zu implementieren wären.

Bestehende Sicherheitskonzepte greifen in der Cloud nicht

Organisationen in regulierten Branchen sollten ein besonderes Augenmerk auf die Einhaltung entsprechender Zertifizierungen haben. Gerade aber kleine Organisationen, wie etwa Städte und Gemeinden mit wenig oder keinen IT-Ressourcen, müssen sich bewusst machen, welche Rolle der Cloud-Anbieter und sie selbst einnehmen und wie die Schnittstellen dazwischen funktionieren. Denn in einer Cloud- oder hybriden Umgebung sind Sicherheitsarchitekturen anders aufgebaut als bei klassischen Betriebsmodellen.

Für Unternehmen in hochregulierten Branchen ist aber auch eine (Public-)Cloud-Lösung mindestens so sicher, wenn nicht sogar noch sicherer als eine On-Prem-Installation. Voraussetzung dafür sind entsprechende technische und organisatorische Massnahmen, Weisungen und Kontrollen sowie die richtigen Tools und Features. Dass aber zum Beispiel eine Public-Cloud-Lösung sicherer ist als eine On-Prem-Lösung, heisst noch nicht, dass sie den gesetzlichen Vorgaben standhält. Für Schweizer Anbieter wiederum sprechen die grössere Flexibilität und vor allem die Gewissheit, dass bei ihnen gespeicherten Daten dem Schweizer Recht unterstehen.

Bild: Jakub Jirsák / AdobeStock.com