PUBLIC CLOUD: ELDORADO FÜR COMPLIANCE & IT-SICHERHEIT?

Die Nutzung der Public Cloud gewinnt immer stärker an Akzeptanz. Dies bedeutet Herausforderungen, aber auch Chancen in den Bereichen Compliance und IT-Sicherheit.

→ **VON DOMINIK LANGER**

Die Public Cloud ist inzwischen auch für Unternehmen in der Schweiz ein real nutzbarer Baustein für die Wertschöpfungskette. Internationale Hyperscaler eröffnen Regionen in unserem Land und kommen so Unternehmen entgegen, die ihre Daten nicht in Rechenzentren im Ausland verarbeiten wollen oder dürfen. Gleichzeitig werden wichtige Rahmenbedingungen für die Nutzung geschaffen. Im Frühjahr dieses Jahres veröffentlichte beispielsweise die Schweizer Bankiersvereinigung die Empfehlung, dass bei Verwendung angemessener Kontrollmechanismen Kundendaten auch in den Rechenzentren im Ausland verarbeitet können, ohne dadurch das Bankkundengeheimnis zu verletzen. Dies unterstützt den Trend in Richtung Public Cloud sogar für den Finanzsektor.

In vielen etablierten Unternehmen standen oder stehen Verantwortliche in Kontrollfunktionen wie Compliance und IT-Sicherheit dem Gang in die Public Cloud jedoch skeptisch gegenüber. Tatsächlich gibt es Herausforderungen, doch sind nicht alle davon fundamental neu: viele klassische IT-Risiken lassen sich in der Public Cloud sogar besser beherrschen.

NEED FOR SPEED

Die Cloud trägt wesentlich zur Unternehmensagilität bei. Trends wie agile Entwicklungsmethoden und DevOps zielen ebenfalls darauf ab, die Durchlaufzeit für neue Anforderungen zu senken und so neue Funktionalität rascher an den Markt zu bringen.

Allerdings stehen die Zuständigen für Compliance und Informationssicherheit in einer Welt, in der der Abstand zwischen neuen Releases nicht mehr Monate, sondern nur noch Stunden, Minuten oder gar Sekunden beträgt, plötzlich ganz neuen Herausforderungen gegenüber. In klassischen Organisationen sind diese Kontrollfunktionen oft zentral organisiert und werden in wasserfallorientierten Projekten in der Regel vor allem in der Designphase und später wieder bei der Abnahme beigezogen. In neuen, agilen Ansätzen entwickelt sich die Situation so rasch weiter, dass dieser klassische Ansatz nicht mehr zielführend ist. Dies führt zu Spannungen: die Kontrollfunktionen werden als Bremsklotz wahrgenommen. Zudem ist das Risiko gross, dass die von den Kontrollfunktionen abgenommenen Systembeschreibungen reine Fiktion sind, die dem tatsächlichen Zustand des Systems stetig mehr hinterherhinken.

Zum Autor

Dr. Dominik Langer (CRISC, CISM, CGEIT) ist Chief Digital & Innovation Officer bei der adesso Schweiz AG und verantwortet dort den Aufbau neuer Dienstleistungen zu aktuellen Technologiethemen. Er hat mehrere Versicherungsunternehmen auf dem Weg in die Public Cloud begleitet.

Zum Unternehmen:
adesso unterstützt Kunden auf ihrer Reise in die Cloud und in der Cloud: von der Ausarbeitung einer Cloud-Strategie über die Auswahl der bestgeeigneten Anbieter und Onboarding bis zur Umsetzung von Cloud-Migrationen oder Entwicklung cloudnativer Applikationen. Durch unsere Branchennähe verstehen wir die spezifischen Herausforderungen in Ihrem Geschäftsumfeld.

Mehr Informationen: www.adesso.ch

Zwei Aspekte sind wichtig, damit dieses Zusammenspiel auch in einer agilen Welt funktioniert: Erstens muss Konformität weniger durch Prozesse als durch aktive Abbildung der Compliance-Regeln in den Softwaresystemen erreicht und fortlaufend überprüft werden. Zweitens müssen Experten für Compliance und IT-Sicherheit in die Entwicklungsteams integriert werden und dort kontinuierlich aktiv mitgestalten, damit sichere und konforme Lösungen gefunden und umgesetzt werden. Die Public Cloud bietet wichtige Instrumente, um diese beiden Punkte zu unterstützen.

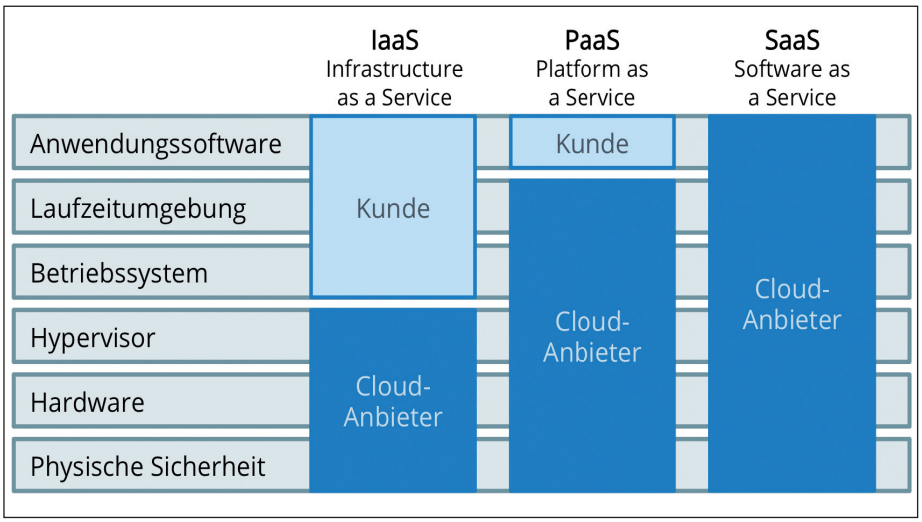
EINE SICHERE GRUNDLAGE

In der Public Cloud teilen sich der Cloud Service Provider und dessen Kunde die Zuständigkeit für die Sicherheit (siehe Abbildung). Dadurch gibt das Unternehmen einen je nach Cloud-Servicemodell unterschiedlich grossen Teil der Zuständigkeit für die Sicherheit an den Cloud Service Provider ab und kann die freigewordenen Ressourcen anderweitig nutzen. Wenn das Unternehmen auf einen erfahrenen Cloud Service Provider setzt, kümmern sich nun bestqualifizierte Spezialisten um die Sicherheit für den ausgelagerten Teil, wodurch sich diese in der Regel verbessert.

Der Cloud-Nutzer kann sich über entsprechende Compliance-Programme davon überzeugen, welche Sicherheitskontrollen der Cloud Service Provider implementiert hat und ob diese effektiv sind. Diese Programme beruhen auf Audits durch unabhängige Drittparteien. Die führenden Cloud Service Provider bieten diverse Compliance-Programme basierend auf globalen, länder- oder industriespezifischen Standards, um die Bedürfnisse verschiedener Kunden zu adressieren.

Wofür der Cloud-Nutzer nach wie vor selber zuständig bleibt, ist die sichere Konfiguration der Cloud und die Sicherheit seiner darin enthaltenen Applikationen. Zwar bedeutet dies je nach Service-Modell viel Flexibilität, aber auch eine grosse Herausforderung: die öffentlich bekannt gewordenen Datenlecks in der Cloud zei-

Bild: adesso Schweiz AG



Cloud Service Provider und dessen Kunden teilen die Zuständigkeit für IT-Sicherheit.

gen, dass man als Cloud-Nutzer viel falsch machen kann. In den folgenden Abschnitten werden Massnahmen aufgezeigt, die dies verhindern können.

GEPRÜFTE VORGABEN

On-Demand Self-Service ist eine der definierenden Eigenschaften der Cloud. Es macht allerdings einen grossen Unterschied, ob jeder im Unternehmen nach Belieben Cloud-Ressourcen starten kann oder eben nur solche Ressourcen, die mit definierten Vorgaben konform sind. Tatsächlich ist es je nach Cloud Service Provider möglich, vorkonfigurierte Services zu implementieren, die unternehmensinterne Compliance-Vorgaben erfüllen. Diese können den Mitarbeitern über einen Service-Katalog zur Verfügung gestellt werden. Berechtigungen sollten dann so definiert werden, dass nur diese im Voraus genehmigten Services und konformen Konfigurationsmöglichkeiten genutzt werden können. So schränkt man die Möglichkeiten zur nichtkonformen Nutzung der Cloud stark ein und fördert konforme Agilität.

HOHE TRANSPARENZ

Ein grosser Vorteil der Cloud gegenüber On-Premise-Infrastruktur ist die hohe Transparenz: Ressourcen sind durch Software definiert und lassen sich durch diese auch auslesen und überwachen. Dies gilt sowohl für den aktuellen Zustand als auch für die vergangene Historie. Wenn man die Cloud-Plattform entsprechend konfiguriert, können alle Aktivitäten nachvollzogen und auf Konformität überwacht werden.

COMPLIANCE-AUTOMATISIERUNG

Der weitaus grösste Teil der Sicherheitspannen in der Cloud, die in den vergangenen Jahren bekannt geworden sind, waren auf Fehlkonfigurationen durch deren Nutzer zurückzuführen. Die führenden Cloud Service Provider investieren daher viel in die Automatisierung von Compliance. Proaktive Dienste weisen automatisch auf mögliche Fehlkonfigurationen hin. Es lassen sich Compliance-Regeln konfigurieren, so dass in entsprechenden Dashboards auf einen Blick erkenntlich ist, ob und wo Abweichungen vorliegen. Da die Regeln in Echtzeit überwacht werden, kann bei auftretenden Regelverletzungen sofort zuständiges Personal benachrichtigt oder sogar automatisch der vorherige, konforme Zustand wieder hergestellt werden.

Maximale Automatisierung sollte jedoch nicht nur in der Überwachung eingesetzt werden, sondern im ganzen IT-Betrieb. Dadurch sinkt die Wahrscheinlichkeit sowohl von absichtlichen als auch von unabsichtlichen Fehlmanipulationen.

BEWEISBARE SICHERHEIT

Der höchste Grad an Sicherheit ist mathematisch beweisbare Sicherheit. AWS beispielsweise betreibt hierfür eine eigene Abteilung, welche mittels mathematischer Beweisführung z.B. die Sicherheit von Programmcode verifiziert. Nach und nach stellt AWS solche Services auch Kunden zur Verfügung, so dass diese Compliance-Regeln einrichten können, welche in Echtzeit automatisierte mathematische Beweisführung auslösen, um Aussagen über konforme und sichere Konfiguration der Cloud zu treffen. Die Resultate können zu Auditzwecken verwendet werden oder wie oben beschrieben automatisiert Benachrichtigungen oder kurative Aktionen auslösen.

MASCHINELLES LERNEN

Nicht alle Compliance-Vorgaben oder sicherheitsrelevanten Ereignisse lassen sich durch einfache Regeln abbilden. Unscharfe und komplexe Szenarien können durch maschinelles Lernen besser erfasst werden.

Beispielsweise erkennt, klassifiziert und schützt der AWS-eigene Dienst Macie vertrauliche Daten automatisch. Dienste wie Amazon GuardDuty oder Azure Advanced Threat Protection wiederum erkennen sicherheitsrelevante Vorfälle automatisiert basierend auf Abweichungen zwischen aktuellen Messdaten vom „normalen“ Verhalten innerhalb der Cloud-Umgebung des Kunden. Ähnliche Tools werden auch von Drittanbietern angeboten und können anstelle von oder in Kombination mit Services, die der Cloud Service Provider selbst anbietet, eingesetzt werden.

CHAOS ENGINEERING

Chaos Engineering ist eine Disziplin, die durch Netflix bekannt gemacht wurde. Der Streaming-Anbieter setzte bereits früh vollständig auf die Public Cloud und entwickelte starke Kompetenzen in deren zuverlässigen Nutzung. Berühmt geworden ist ihre Simian Army, eine Sammlung von Tools, die nicht nur Compliance in der Cloud überwachen und nichtkonforme Cloud-Ressourcen abschalten, sondern auch absichtlich Störungen einführen, wie z.B. den Ausfall einzelner virtueller Maschinen oder ganzer Rechenzentren. Dies zwingt die Entwickler, bereits im Design der Applikationen mögliche Störungen zu berücksichtigen, so dass das System auch gegen echte Ausfälle wesentlich besser gewappnet ist. Weitere Unternehmen haben diesen Ansatz übernommen und üben regelmässig entsprechende Ausfälle oder Störungen, um für den Ernstfall gerüstet zu sein.

FAZIT

Die meisten der Risiken der Public Cloud in den Bereichen Compliance und IT-Sicherheit existieren auch in Unternehmen, die auf eigene Datenzentren setzen. Die Public Cloud bietet jedoch Möglichkeiten, viele dieser Risiken auf einem höheren Maturitätslevel zu beherrschen. Durch das Outsourcing in die Public Cloud kann ein Teil der Anforderungen durch einen hochautomatisierten und spezialisierten Anbieter abgedeckt werden. Durch gezieltes Konfigurieren gemäss spezifischer Geschäftsregeln können Sicherheits- und Compliance-Vorgaben effektiver umgesetzt werden. In Kombination verschafft dies den Compliance- und Security-Verantwortlichen mehr Zeit, zusammen mit dem Business und den Entwicklungsteams neue Ideen auszuloten und deren Umsetzung konform und sicher mitzugestalten.

Bei der Auswahl der richtigen Public-Cloud-Services und deren Konfiguration ist adesso ein verlässlicher Partner. ←

Dieser Beitrag wurde von **adesso** zur Verfügung gestellt und stellt die Sicht des Unternehmens dar. Computerworld übernimmt für dessen Inhalt keine Verantwortung.