DAS PRINZIP DER GETEILTEN VERANTWORTUNG

Die großen Bedenken gegenüber der Public Cloud sind bei den meisten deutschen Unternehmen mittlerweile verschwunden. Spätestens mit Corona hat die Nutzung von Cloud-Diensten einen gewaltigen Schub erfahren, auch in kleinen und mittelständischen Unternehmen. Ein wesentlicher Punkt wird dabei aber oft übersehen: Die Absicherung der Cloud obliegt nicht nur dem entsprechenden Cloud-Anbieter, sondern ebenso dem Nutzer der Cloud. Es gilt das Prinzip der Shared Responsibility.

Autor: Lukas Höfer ***Redaktion: Diana Künstler***

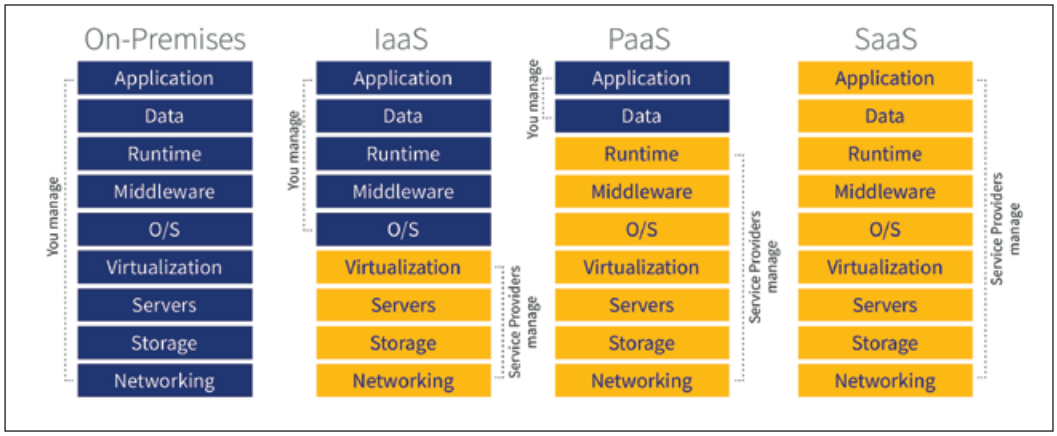

Bild: Consol

Je nach Cloud-Modell tragen Unternehmen eine unterschiedlich große Verantwortung für die Sicherheit ihrer Anwendungen und Daten in der Cloud.

➤ Auf die Cloud können und möchten die meisten Unternehmen nicht mehr verzichten, doch Sorgen bereitet ihnen oft das Thema Sicherheit. Es rückt vor allem immer dann in den Fokus, wenn sich Angreifer Zugriff auf Fotos von Prominenten verschaffen oder im großen Stil Passwörter oder Kontodaten stehlen, worüber dann auch die Massenmedien berichten. Dabei gibt es bei der Absicherung der Cloud durchaus verschiedene Perspektiven zu berücksichtigen. Denn es geht nicht nur um den Schutz der bereitgestellten Infrastruktur, für die der Cloud-Anbieter verantwortlich zeichnet, sondern auch um die Konfiguration und Nutzung der Dienste, die der Kunde kontrolliert. Man spricht daher von einem Shared-Responsibility-Modell, also einem Prinzip der geteilten Verantwortung von Cloud-Anbieter und -Anwender.

Sicherheit der Cloud selbst...

Kaum eine andere Branche steht so sehr im Fokus von Cyberkriminellen wie die der Public-Cloud-Provider. Allein durch ihre Größe stellen sie für Angreifer ein lukratives Ziel dar, bei dem sich viele Daten erbeuten lassen. Daher sind die Sicherheitsmaßnahmen der großen Provider besonders strikt – etwas, das auch von den global agierenden Unternehmen, die zu ihren Kunden zählen, eingefordert wird.

Cloud-Anbieter erfüllen die höchsten Sicherheitsstandards. Das beginnt bei der physischen Sicherheit der Rechenzentren, die mit modernsten Verfahren und oft sogar mit Panzersperren ausgestattet sind. Die Möglichkeit, dass ein Einbrecher hier das Back-up der Daten stiehlt, ist nahezu ausgeschlossen. Auch gegen kleine und große Katastrophen wie Stromausfälle, Brände oder Unwetter sind die Rechenzentren in der Regel perfekt gewappnet. Ebenso haben die Public-Cloud-Anbieter weitreichende Maßnahmen gegen Cyber-Angriffe getroffen. Zumindest theoretisch stellt auch die gemeinsame Nutzung der zugrundeliegenden Hardware-Ressourcen ein Risiko dar, sollte es gelingen, über die Virtualisierungsschicht auf fremde Anwendungen und Daten zuzugreifen. 2018 wurden in diesem Zusammenhang zwei Methoden entdeckt, über die auf andere virtuelle Server auf demselben physischen Server zugegriffen werden konnte. Tatsächlich sind bislang aber keine Fälle bekannt, in denen diese Lücken tatsächlich ausgenutzt wurden. Wer trotzdem eine zusätzliche Absicherung anstrebt, kann aber auch in der Public Cloud dedizierte Hosts anmieten.

...und bei der Nutzung

Bei den bekannten Sicherheitsvorfällen, bei denen Fotos, Passwörter oder Kontodaten aus der Cloud gestohlen wurden, handelte es sich nicht um komplexe Hacking-Angriffe. Sie waren vergleichsweise leicht durchzuführen, weil die größte Schwachstelle im System genutzt wurde: die Sorglosigkeit der Nutzer. In allen bisher aufgetretenen Fällen

konnten Passwörter leicht erraten oder entwendet werden. Die Verantwortung dafür liegt bei den Nutzern selbst und nicht beim Cloud-Provider, dementsprechend ist die Gefahrenabwehr an dieser Stelle ihre Aufgabe. Ihr Verantwortungsbereich umfasst unter anderem die Einhaltung von Passwort-Best-Practices, die Identitäts- und Zugriffsverwaltung, die korrekte Verwaltung der Plattform und selbstverständlich die Sicherheit der selbst entwickelten Applikationen. Auch die Verschlüsselung der Daten während der Übertragung und am Speicherort muss vom Anwender durchgeführt werden. Letzteres ist vor allem deshalb wichtig, da nach wie vor große Rechtsunsicherheit besteht, was die Vereinbarkeit europäischer und amerikanischer Datenschutzbestimmungen angeht und den Zugriff von US-Behörden auf in Europa gespeicherte Daten.

Eine helfende Hand für die Anwender

Bei der Einhaltung der DSGVO stehen Unternehmen, die die Cloud nutzen, gegenüber ihren Kunden in der Verantwortung. Sie müssen sich darum kümmern, dass Speicherorte und Speicherdauer den Vorgaben entsprechen. Allerdings bieten die führenden Provider Consulting-Dienste, verschiedene Tools und Informationsmaterialien an, um dem Nutzer die Konfiguration und kontinuierliche Gewährleistung der Sicherheit und Compliance zu erleichtern. Auch viele Systemhäuser und IT-Dienstleister können interessierten Unternehmen hier mit Beratung und eigenen Services zur Seite stehen.

Beispielhaft zeigt sich die Aufgabenteilung zwischen Cloud-Anbieter und Cloud-Nutzer beim Anwendungsfall Infrastructure-as-a-Service (IaaS): Dem Provider obliegt die Sicherung von Server, Storage, Netzwerk und Virtualisierung. In den Verantwortungsbereich des Anwenders fallen die über der Infrastruktur liegenden Schichten wie Betriebssystem, Middleware, Runtime, Applikationen und Daten.

Schutzmaßnahmen

Um die Cloud sicher zu nutzen, benötigen insbesondere kleine und mittlere Unternehmen in der Regel eine Unterstützung durch Experten. Doch die Basics lassen sich oft auch mit etwas Einarbeitung selbst umsetzen, da viele IT-Komponenten und Sicherheitskonzepte aus dem klassischen IT-Betrieb auch in der Cloud anzutreffen sind. Allerdings stehen dort viel mehr Berechtigungen und die Kontrolle von Zugriffen im Fokus, da die Public Cloud global verfügbar ist und somit auch eine andere Angriffsfläche bietet.

Zwischen Cloud Security und „normaler“ IT-Security gibt es im Prinzip keine grundlegenden Unterschiede, mit einer Ausnahme: Es gilt das Shared-Responsibility-Prinzip.

Als Basis-Schutzmaßnahme sollten Unternehmen für alle Cloud-Modelle unbedingt eine Mehr-Faktor-Authentifizierung verwenden, die zum Beispiel aus einem starken Passwort und einem mobilen Gerät besteht. Darüber hinaus sollte ein Unternehmen ein Least-Privilege-Konzept umsetzen, das heißt, es sollte Mitarbeitern nur Zugriffsrechte erteilen, die sie für ihre Tätigkeit tatsächlich benötigen. Wird ein Account trotz aller Vorsichtsmaßnahmen kompromittiert, erhält ein Cyberkrimineller nur Zugriff auf einen kleinen, klar umgrenzten Bereich der Unternehmens-IT.

Insgesamt gibt es zwischen Cloud Security und „normaler“ IT-Security keine grundlegenden Unterschiede, mit einer Ausnahme: Es gilt das Shared-Responsibility-Prinzip. Der Cloud Provider ist zwar für die Sicherheit verantwortlich, aber nur für die Serviceschichten, die er seinen Kunden anbietet. Für die restlichen Schichten trägt der Kunde die Verantwortung. Erkennen Unternehmen die Notwendigkeiten, die aus dem Prinzip der Shared Responsibility resultieren, ist ein entscheidender Schritt zu einer hohen Public-Cloud-Sicherheit getan.

Lukas Höfer ist Cloud Solutions Architect bei Consol Software in München