consol
Wir unternehmen IT

Cloud Security: Mit klaren Standards sind Ihre Daten sicher

ConSol Leitfaden

INHALT

Einführung

Datenschutz ist Top-Anforderung an Cloud Provider

Cloud Computing ist einer der wichtigsten Grundpfeiler der digitalen Transformation. Je mehr die Welt miteinander vernetzt wird und Dinge miteinander vernetzt sind (Internet of Things), desto mehr Datenmengen entstehen. All diese Daten wollen – natürlich gewinnbringend – verarbeitet werden. Hierbei ist die Cloud nicht mehr wegzudenken, verspricht sie uns doch ununterbrochen verfügbare und skalierbare Rechenleistung.

Nutzung von Cloud Computing in Deutschland

Mit den unterschiedlichen Cloud-Modellen und vielfältigen Services holen die Provider die Nutzer bzw. Unternehmen mit ihren Bedürfnissen ab. Public, Private oder Hybrid – laut Cloud Monitor 2019 von KPMG stellten sich 2014 nur 44 Prozent der deutschen Unternehmen ab 20 Beschäftigten diese Frage. 2018 liegen wir bei 73 Prozent, die Cloud Computing entweder schon nutzen oder den Einsatz planen bzw. diskutieren.

Große Unternehmen, die Cloud-Dienste schon länger in Anspruch nehmen, haben mittlerweile verstanden, dass die Entscheidung für ein Cloud-Modell nicht für alle Zeit in Stein gemeißelt sein muss: Kunden diversifizieren ihre Cloud-Strategie zunehmend in Richtung Hybrid, wobei die Public Cloud im Vergleich den größten Zuwachs verzeichnet. 2014 sagten noch 76 Prozent der Unternehmen, dass für sie die Public Cloud kein Thema sei, laut Cloud Monitor 2019 sank dieser Wert auf 37 Prozent. Umgekehrt nutzten 2014 nur 16 Prozent die **Public Cloud**, Ende 2018 waren es 35 Prozent und immerhin 28 Prozent diskutierten die Einführung.

Skepsis gegenüber der Public Cloud

Während der Trend auf der einen Seite zu mixed Modellen geht, gibt es immer noch überzeugte Nicht-Nutzer der Cloud. „Solange die Public-Cloud-Anbieter die Nicht-Nutzer nicht von der Sicherheit der Public Cloud überzeugen können, wird der Public-Cloud-Markt nur langsam wachsen.“ [1] Datendiebstahl oder gar Datenverlust sind hierbei die größten Ängste, die nach wie vor dafür sorgen, dass die Public Cloud für Skeptiker keine Option ist.

Es überrascht also nicht, dass wie schon 2018 das Top-Auswahlkriterium für einen Cloud Provider immer noch die Konformität mit der DSGVO ist. Darüber hinaus setzen viele die Public Cloud mit einem Sicherheitsrisiko gleich. Doch wie berechtigt sind diese Bedenken wirklich?

Der folgende Leitfaden räumt mit verbreiteten Vorurteilen auf und klärt gleichzeitig, welche Verantwortung der Nutzer beim Thema Cloud Security übernehmen muss.

[1] KPMG Cloud Monitor 2019, Kapitel 2.3, Seite 15.

Sorgenfrei und sicher in der Public Cloud

Sicherheit im Cloud-Umfeld

Das Thema Sicherheit ist weiterhin auf Platz eins, wenn es um Kritikpunkte an der Public Cloud geht. Dabei werden gerne Beispiele angeführt, bei denen Fotos von Prominenten, Passwörter oder sogar Kontodaten gestohlen wurden.

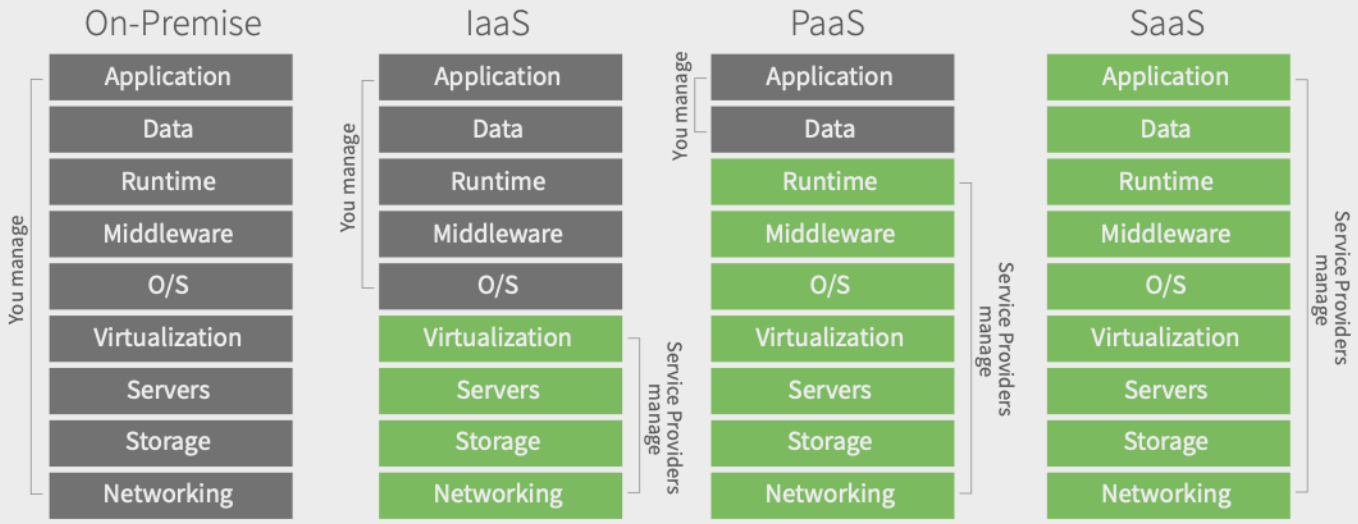
Von einem technischen Standpunkt her scheint es auch gefährlich zu sein, mehrere virtuelle Server auf einem realen Server laufen zu lassen. Schließlich teilen sich Cloud-Nutzer hier Ressourcen mit anderen Unternehmen, die theoretisch aus ihrer virtualisierten Isolation ausbrechen und so Dienste unterbrechen oder Daten stehlen könnten.

Und dann bleibt noch die Frage, was mit den Daten überhaupt passiert, beispielsweise wenn eine ausländische Regierungsbehörde diese von dem dort ansässigen Cloud Provider einfordert. Und wem gehören die Daten eigentlich, wenn sie in der Cloud sind, dem Unternehmen oder doch dem Cloud Provider?

Gemeinsame Verantwortung in Cloud-Projekten

Aus diesen kritischen Beispielen und Fragestellungen ergeben sich drei Themenbereiche. Sicherheit bei der Nutzung, Sicherheit der Cloud-Infrastruktur und Compliance. Um Sicherheit in Public Cloud-Projekten zu gewährleisten, ist es notwendig zu verstehen, welchen Teil die User selbst dazu beitragen müssen. Im Cloud-Bereich sprechen wir von einem Shared Responsibility Model, also einem Modell der gemeinsamen Verantwortung.

Hierbei berufen wir uns wieder auf das Schichtenmodell – Infrastructure as a Service, Platform as a Service und Software as a Service. Dabei sieht die Verantwortungsverteilung aus wie in nachstehender Abbildung. Je weiter oben sich Cloud User in den Schichten befinden, desto weniger obliegt der Punkt Sicherheit den Nutzern und desto mehr dem Cloud Provider. Wir unterscheiden also die Sicherheit der bereitgestellten Cloud **(Security of the Cloud)** und die Sicherheit in der Cloud, also dem, was der Nutzer selbst konfigurieren kann und muss **(Security in the Cloud).**



Sicherheit der Cloud

Cloud Provider sind die wohl am meisten von Cyber-Attacken betroffenen Unternehmen. Allein schon durch ihre Größe stellen sie für Angreifer ein interessantes Ziel dar. Umgekehrt sind dadurch aber die Sicherheitsmaßnahmen der großen Cloud Provider besonders gefestigt. Zudem werden sie durch die Vielzahl der weltweiten Kunden gewissermaßen zu höchsten Standards gezwungen. Das beginnt bei der Sicherheit der Rechenzentren, die mit modernsten Methoden bewacht werden und sogar mit Panzersperren ausgestattet sind. Die Möglichkeit, dass ein Einbrecher hier das Backup der Daten stiehlt, oder auch nur zu Gesicht bekommt, ist ausgeschlossen.

Auch was Brandabschnitte und redundante Infrastruktur angeht, kann eine Private Cloud bei weitem nicht mithalten. Es ist also nicht verwunderlich, dass die führenden Public Cloud-Anbieter weitaus mehr Zertifikate haben, als viele der regionalen Dienstleister. Besonders interessant ist dabei gerade in Deutschland natürlich die General Data Protection Regulation (GDPR, die europäische Grundlage für die deutsche DSGVO), die mitunter über das C5-Zertifikat abgedeckt wird. Hier wird beispielsweise sichergestellt, dass die Daten sicher und nur bei durch den Kunden festgelegten Rechenzentren innerhalb Deutschlands oder der EU gespeichert werden.

Übersicht über die Zertifizierungen der führenden Cloud Anbieter:

https://www.microsoft.com/en-us/trustcenter/Compliance/C5,
https://aws.amazon.com/de/compliance/services-in-scope/,
https://cloud.google.com/security/compliance/#/

Die eingangs beschriebenen Angriffe über die Virtualisierungsschicht werden gerne als Argument vorgehalten, nicht in die Public Cloud zu migrieren. 2018 wurden zwei Methoden bekannt, wie aus geteilten Prozessoren fremde Daten abgegriffen werden können. Hierbei können komplexe Algorithmen im Prozessor ausgenutzt werden, um theoretisch auf fremde virtuelle Server auf dem gleichen physischen Server zuzugreifen. Auf diese enorme, potenzielle Bedrohung wurde relativ schnell reagiert und die Sicherheitslücken wurden bestmöglich geschlossen. Inzwischen sind weitere, sehr ähnliche Methoden bekannt.

Obwohl dieser Angriff nicht nur in der Public Cloud, sondern in jeder virtualisierten Umgebung auftreten kann, sind keine Fälle bekannt geworden, in denen diese Lücke tatsächlich ausgenutzt werden konnte. Das liegt daran, dass dieser Angriff äußerst komplex ist und anders als das Erraten von Passwörtern höchstes Expertenwissen voraussetzt. Wer sich trotzdem zusätzlich absichern möchte, dem bleibt die Möglichkeit, sich dedizierte Hosts anzumieten, auch in der Public Cloud. Hierbei ist vom Cloud Provider garantiert, dass nur Server eines einzigen Kunden auf den physischen Servern laufen. Angriffe über die Virtualisierungsschicht werden somit also ausgeschlossen.

Wem gehören die Daten in der Public Cloud?

Auch wem die Daten in der Cloud gehören ist eindeutig, wenn auch nicht jedem bewusst. Daten, die man als Nutzer oder Unternehmen in angemieteten Cloud Services ablegt, gehören immer dem Kunden. Trotzdem hält sich das Gerücht, dass beispielsweise AGB-Klauseln existieren, mit denen man seine Datenkontrolle an Google oder andere überschreibt. Fakt ist, dass solche AGBs existieren, sie aber keinesfalls versteckte Klauseln in Verträgen darstellen. Sie gelten klar für eine Auswahl von öffentlichen Diensten. So zum Beispiel für Anfragen, die über die Google Suchmaschine gestellt werden, welche zur internen Verbesserung des Dienstes genutzt werden. Dies betrifft aber keineswegs angemietete Cloud-Ressourcen oder Services.

Wichtig ist auch, dass Regierungsbehörden nicht auf die Daten von Nutzern und Unternehmen aus der Public Cloud zugreifen können und dürfen. Das garantiert zumindest für amerikanische Unternehmen der sogenannte CLOUD Act. Hier ist ganz klar festgelegt, dass nur im kriminellen Verdacht und auch nur gerichtlich abgesichert Daten von Cloud Providern an die Regierung übergeben werden müssen. Das auch nur dann, wenn es nicht den regional gültigen Gesetzen widerspricht, also zum Beispiel den deutschen (1).

Bisher ist zudem kein Fall bekannt, an dem ein Cloud Provider Daten an die Regierung übergeben musste. China ausgenommen, doch hier gilt auch der CLOUD Act nicht. Wer trotzdem sicher gehen möchte, dass seine Daten nicht preisgegeben werden, dem bleiben mannigfaltige Möglichkeiten die Daten zu verschlüsseln. So sind die Daten selbst nach einer Herausgabe oder einem Diebstahl durch falsche Konfiguration oder spezialisierte Hacker für Dritte unbrauchbar. Hierbei handelt es sich dann um die Security in der Cloud (Security in the Cloud).

(1) IDC bietet in Zusammenarbeit mit AWS eine vierseitige Stellungnahme zum Thema CLOUD Act, die als sehr guter Einstieg in die Thematik dient.

Sicherheit in der Cloud: Der User als Schwachstelle

In dem ersten Beispiel zu gestohlenen Bildern, Passwörtern und Kontodaten handelt es sich stets um leicht durchzuführende Hacking-Angriffe. Leicht deshalb, weil die einfachste Schwachstelle im System genutzt werden kann, die Sorglosigkeit des Nutzers. In allen bisher bekannten Fällen konnten ganz einfach Passwörter erraten oder anderweitig gestohlen werden. Dasselbe Problem besteht bei jedem System, das über das Internet erreichbar ist. Der Fehler liegt hier klar bei den Nutzern selbst und nicht beim Cloud Provider. Allerdings ist die Angriffsfläche über die Homogenität und die Skalierung in der Cloud deutlich gewachsen, weshalb solche Attacken inzwischen enorme Nutzerzahlen betreffen können. „Schreckensnachrichten“ gelangen somit schneller und häufiger an die Öffentlichkeit, was die gefühlte Bedrohung erhöht.

Es liegt in der Verantwortung der Nutzer, solche Gefahren abzuwenden, indem sie die Sicherheit in der Cloud sorgfältig gestalten.

Bei Software as a Service geht es hauptsächlich darum, sich an Best Practices für Passwörter zu halten. Gleichzeitig ist es notwendig zu verstehen, welche Daten mit der Lösung verarbeitet werden dürfen. Denn unter Umständen kann es hier zu Ausnahmen kommen. Bewegt man sich im Schichtenmodell (siehe S. 5) weiter nach unten, fällt auch die Identitäts- und Zugriffsverwaltung in den Zuständigkeitsbereich des Nutzers. Ebenso zählen die korrekte Verwaltung der Plattform und die Sicherheit der selbst entwickelten Applikationen zu den Aufgaben des Users, genauso wie die Verschlüsselung der Daten in Bewegung oder am Speicherort.

Bei Infrastructure as a Service erweitert sich der Zuständigkeitsbereich um die Verwaltung von Betriebssystemen, der Firewall und des Netzwerks. Wichtig ist, dass auch die Zertifizierungen der Cloud Provider nur bis zur Grenze der eigenen Verantwortung reichen. Möchte man beispielsweise PaaS nutzen und GDPR-compliant sein, muss man sich selbstständig um die Speicherorte und Speicherdauer der Daten kümmern. Gewährleistet ist nur, dass die genutzten Funktionen des Cloud Providers dies unterstützen.

Allerdings bieten die führenden Provider exzellente Tools sowie Informationsmaterialien und Beratung an, um dem Nutzer die Konfiguration und kontinuierliche Gewährleistung der Sicherheit und Compliance so einfach wie möglich zu machen.

Cloud Security Tipps

Um Sicherheit in der Cloud zu gewährleisten, benötigt man in komplexen Projekten selbstverständlich Experten. Doch wer klein anfängt und iterativ vorgeht, kann die wichtigsten Kniffe auch schnell selbst erlernen. Vor allem, da man in der Cloud sehr vieles von dem wiederfindet, was man aus dem klassischen IT-Betrieb gewohnt ist: Netzwerke, Firewalls, Speicher. Was man sich aber vor Augen halten sollte ist, dass eine Public Cloud zunächst global verfügbar ist und die Angriffsfläche somit gewachsen ist. Nachdem man nicht mehr so einfach wie früher das Netzwerk nach außen dicht machen kann, muss man den Sicherheitsfokus nun auf Nutzer und deren Berechtigungen legen. Dabei ist es stets sinnvoll, Multi Factor Authentication (MFA) einzusetzen.

Multi Factor Authentication und Least Privilege müssen Standard sein

Hierbei hat der Nutzer nicht nur ein Passwort, das im schlimmsten Fall erraten oder gestohlen werden kann, sondern er hat zusätzlich ein physisches Gerät: zum Beispiel sein Smartphone, das für die Authentifizierung eingesetzt wird. Die Wahrscheinlichkeit eines erfolgreichen Angriffs nimmt somit drastisch ab. Außerdem sollten nur die Berechtigungen vergeben werden, die auch tatsächlich benötigt werden, um bei einem erfolgreichen Angriff den Schaden möglichst gering zu halten. Man spricht hier von Least Privilege. Darüber hinaus ist es in den meisten Fällen ratsam, Daten nur verschlüsselt aufzubewahren und zu transportieren.

Diese Punkte gab es zwar alle in der klassischen IT genauso, sie wurden allerdings oft nur in sehr sicheren Systemen eingesetzt. Im Zeitalter der Cloud sollten sie aber als Standard wahrgenommen werden.

Es muss nicht alles Public sein – VPN und private Zugangsleitungen

Standardmäßig ist der Zugriff auf die Cloud nur über öffentliche Netzwerke möglich. Dies schürt Bedenken, inwiefern Datenschutz in dieser Umgebung gewährleistet werden kann. Neben den oben genannten Authentifizierungsmethoden gibt es noch weitere Sicherheitsmaßnahmen, die User ergreifen können und die dem erhöhten Sicherheitsbedürfnis entsprechen.

Ein verschlüsseltes VPN, Virtual Private Network, ermöglicht den exklusiven Zugriff auf die Cloud. Die Verschlüsselung erfolgt über das Internet. Den VPN-Zugang kennen viele aus der Arbeitswelt, da man sich über ihn aus dem Home Office ins Firmennetzwerk einloggen kann. VPN ermöglicht eine geschlossene Kommunikation der teilnehmenden Partner, die die Sicherheit der ausgetauschten Daten garantiert.

Gegen Aufpreis stellen die Cloud Provider, auf Basis der verfügbaren Infrastruktur beim Kunden, auch private Leitungen zur Verfügung, über die der Zugriff auf die Cloud exklusiv möglich ist. AWS zum Beispiel nennt diesen Service „Direct Connect“.

Fazit

Einige gängige Gerüchte konnten wir mit unseren Ausführungen hoffentlich aus der Welt räumen. Zusammenfassend lässt sich sagen, dass Cloud-Sicherheit und „normale“ IT-Sicherheit sich nicht grundsätzlich voneinander unterscheiden. Auch bei traditionellen IT-Systemen müssen Zugriffe geregelt und Rollen festgeschrieben sein. Kreieren Sie starke Passwörter und legen Sie diese zugangsbeschränkt ab.

Wenn dieses Prinzip verstanden worden ist, haben Cloud User schon viel gewonnen! Der wesentliche Unterschied zwischen IT- und Cloud-Security liegt im Shared Responsibility-Modell, das wir ausführlich erklärt haben. Auch dieses zielt darauf ab, den Usern ihre Verantwortung bewusst zu machen und sorgfältig mit den eigenen Daten umzugehen.

ConSol
Consulting & Solutions Software GmbH

St.-Cajetan-Straße 43
D-81669 München
Tel.: +49-89-45841-100
vertrieb@consol.de
www.consol.de
Folgen Sie uns auf Twitter: @consol_de

ConSol
Austria Software GmbH

Maysedergasse 2/25
A-1010 Wien, Österreich
Tel.: +43-1-9971392
info-austria@consol.com
consol-software.at
Folgen Sie uns auf Twitter: @consol_at