Cloud – ein Sicherheitsrisiko?

Die Nutzung von Cloud ist allgegenwärtig. Praktisch kein Dienst kommt mehr ohne Nutzung einer Cloud aus. Doch was passiert dabei mit den Daten? Wie sicher sind diese?

Vor einiger Zeit beschäftigten sich viele Firmen mit dem Gedanken, die Cloud zu nutzen. Die Vor- und Nachteile wurden sorgfältig gegeneinander abgewogen. Heute stellt sich die Frage „Cloud – Ja oder Nein“ nicht mehr, sondern nur noch, welche Art von Cloud nutzen wir. Am 3. Cloud Day der Fachhochschule Nordwestschweiz hiess es sogar, die Cloud ist ein Must-have, die grossen Firmen drängen richtiggehend in die Cloud. Dabei Geld zu sparen steht nicht mehr im Fokus, sondern das schnelle und flexible Abbilden der eigenen Business-Prozesse. Wichtig ist es aber, die verschiedenen Anforderungen nicht aus den Augen zu lassen.

Service-Arten

Die Vielzahl an Cloud-Möglichkeiten ist unüberschaubar gross geworden. An dieser Stelle sind nur die drei Hauptarten erwähnt:

- IaaS – Infrastructure as a Service
  Bei dieser Art wird eine komplette Umgebung gemietet. Dies können Ressourcen wie Rechner, Netzwerk und Speicher sein. Der Nutzer ist dabei frei, was und in welcher Ausprägung er nutzt. Der Benutzer ist selber für die Installation, den Betrieb und die Funktion der Software verantwortlich. Dies gilt selbstverständlich auch für die regelmässige Wartung und Aktualisierung der eingesetzten Produkte.

- PaaS – Platform as a Service
  Hier wird die Plattform des Anbieters genutzt, z.B. ein Windows oder Linux-Server. Die Anwendung oben drauf wird durch den Benutzer installiert, betrieben und unterhalten.

- SaaS – Software as a Service
  Dies ist vermutlich die weitverbreitetste Art der Cloud-Nutzung. Der Anbieter stellt sowohl die Plattform, das Betriebssystem sowie die Applikation zur Verfügung. Der Anwender muss sich um nichts Zusätzliches kümmern und nutzt nur die Applikation selber. Dies ist können die Daten eines Fitnessbandes, einer Waage, aber auch Daten bei Dropbox, OneDrive oder ähnlichen Diensten sein. Der Benutzer muss sich um nichts kümmern.

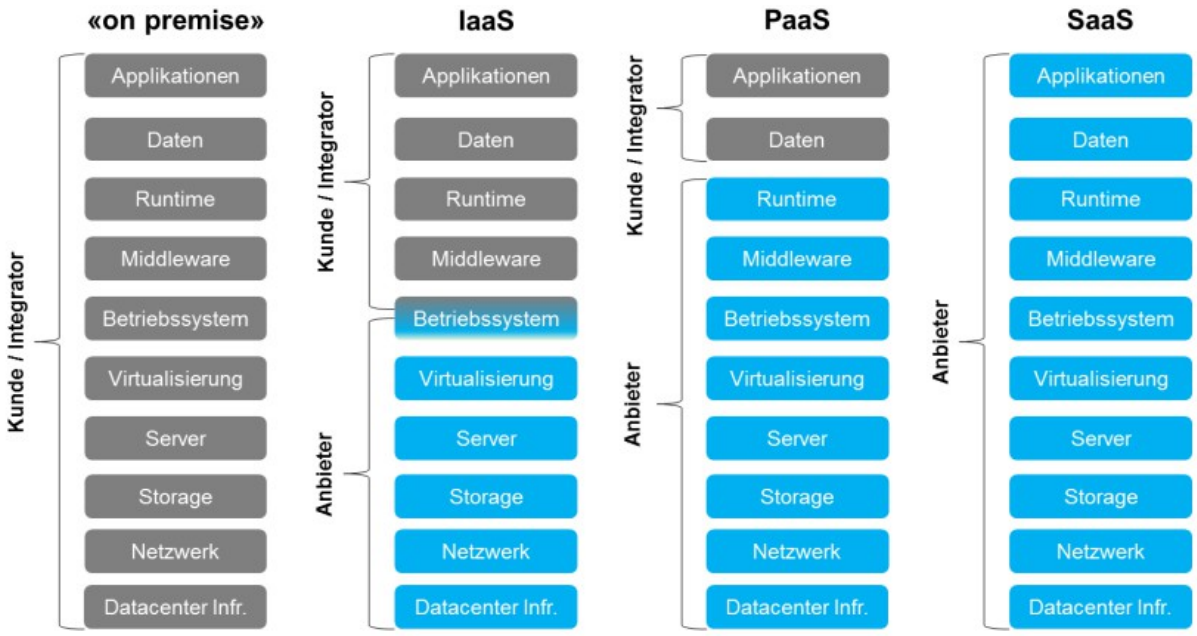


Abbildung: Abgrenzung der Cloud-Dienste

Herausforderungen

Wichtig bei Cloud-Lösungen ist die Überlegung der Datenhoheit. Das schweizerische Datenschutzgesetz erlaubt das Auslagern von schützenswerten Daten nur in Länder mit einem ebenbürtigen Datenschutz. Dies ist z.B. in Amerika nicht gegeben. Aus diesem Grund wurde das Safe-Harbor-Abkommen mit der USA erstellt. Das Pendant für die Schweiz ist das Swiss Safe Harbor Abkommen (http://www.edoeb.admin.ch/datenschutz/00626/00753/00970/index.html?lang=de oder http://export.gov/safeharbor/swiss/). Dabei verpflichten sich Amerikanische Firmen das Datenschutzgesetz der EU bzw. der Schweiz zu respektieren. Im Oktober 2015 stellte der Europäische Gerichtshof fest, dass dieses nicht eingehalten werde und kündigte die EU-Vereinbarung. Somit war es EU-Firmen nicht mehr erlaubt, Daten in die USA zu transferieren. Seit dem 2. Februar 2016 gibt es den Nachfolger EU-US Privacy Shield. Inwieweit sich die Probleme mit dem Datenschutz damit erledigt haben, gilt es noch abzuwarten, erste Stimmen meinen, dies sei auch hier nicht der Fall.

Weiter gilt es zu beachten, dass Cloud-Lösungen oft mit weiteren Kunden geteilt werden. Sollten Schwachstellen in der Infrastruktur des Cloud-Anbieters gefunden werden, ist es allenfalls möglich, dass eigene Daten „verschwinden“ oder unerlaubt kopiert werden. Zudem muss im Hinterkopf daran gedacht werden, dass unter anderem der Administrator des Cloud-Anbieters Zugriff auf die Daten hat.

Ein wichtiger Aspekt ist auch das Backup. Zwar versprechen alle grossen Cloud-Anbieter, dass Sie ein Backup der Daten anfertigen. Doch ist dies genügend? Die Vergangenheit beweist leider das Gegenteil. So kam es bei mehreren grossen Anbietern zu Ausfällen und damit verbunden zu einem Datenverlust. Es war nicht immer möglich, die Daten komplett wiederherzustellen. Je nach Vertrag erhält man als Geschädigter eine finanzielle Entschuldigung, doch das bringt die Daten nicht wieder zurück. Daher gilt es, nicht blind auf die Cloud zu vertrauen und selber für die Datensicherung zu sorgen. Es ist blauäugig sich hier alleine auf den Anbieter zu verlassen.

Neben dem Backup ist natürlich auch die Verfügbarkeit wichtig. Obwohl die grossen Anbieter die Daten redundant auf mehrere Standorte verteilen, kann es geschehen, dass der Zugriff nicht möglich ist. Sei dies durch eine technische Störung oder einen DoS-Angriff (Denial of Service, der Service ist so

stark beschäftigt, dass er keine weiteren Anfragen mehr entgegen nehmen kann). Die eigenen Business-Prozesse stehen dann eventuell still und es muss gewartet werden.

Wird der Vertrag mit einem Cloud-Anbieter beendet, müssen die Daten restlos gelöscht werden. Kann dies der Anbieter auch tatsächlich umsetzen? Die Daten sind oft noch in Backups vorhanden und können nicht so einfach restlos gelöscht werden. Das Unternehmen muss sich in der Regel damit abfinden, dass die Daten noch über mehrere Jahre (oder gar für immer) beim ehemaligen Partner in irgendeiner Art und Weise vorhanden sind.

Auch Hacker haben grosses Interesse an der Cloud. Zum einten kann die Leistung der Cloud für Angriffe missbraucht werden, zum anderen sind die dort gespeicherten Daten sehr interessant. So untersuchen Hacker die Protokolle und Zugangsmöglichkeiten zu den Diensten. Vielleicht ist es auch möglich, einen Verbindungsaufbau abzufangen bzw. umzuleiten (z.B. mittels eines Man-in-the-middle-Angriffs) und so an die Logindaten zu kommen. Danach ist es sehr einfach, die Daten anzuschauen und interessante herunterzuladen. Die Folge kann in Missbrauch der Daten oder ein Erpressungsversuch sein.

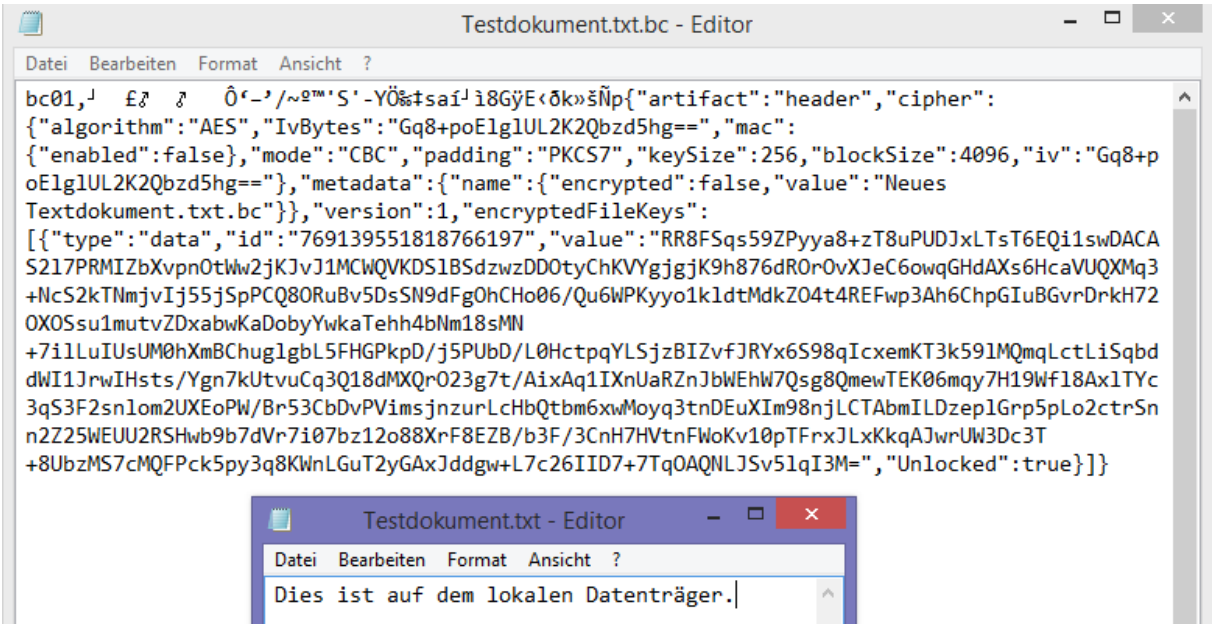
Für ein Unternehmen ist es aber auch wichtig zu wissen, wo die Daten überall sind. Dies betrifft nicht nur, in welchem Land die Daten gespeichert sind (siehe den vorherigen Datenschutz-Aspekt), sondern auch, wer und wie die Daten nutzt. Gerade Cloud-Dienste ermöglichen die einfache Nutzung auf beliebigen Geräten. So sind die Daten auf Handys, Tablets, Laptops und vielen weiteren Geräten gespeichert. Wie wird der Schutz auf diesen Endgeräten sichergestellt? Was, wenn die Mitarbeiter von einem beliebigen Ort auf dieser Welt via App oder Browser auf die Daten zugreifen? Die Verantwortung für die Daten bleibt beim Unternehmen bzw. der Geschäftsleitung. Somit müssen klare Anweisungen erstellt werden, wie die Daten auf eigenen und fremden Geräten geschützt werden.

Überprüfen der Sicherheit

Ideal ist es, wenn bereits in der Vertragsphase ein Auditrecht gewährleistet wird. Der Anbieter wird es zwar kaum erlauben, dass ein Auditor im Rechenzentrum alles anschauen und überprüfen darf (da würden viel zu viele Auditoren vorbei kommen und das Sicherheitsniveau könnte sogar abnehmen, wenn Fremde Personen Zutritt erhalten), deshalb ist es sinnvoll, Auditrechte für Dokumente, Protokolle, Prozessbeschreibungen zu erhalten. Auch ist es sinnvoll, Zertifizierungen zu verlangen, die einen Mindeststandard für Informationssicherheit gewährleisten. Hier bietet sich beispielsweise die internationale Norm ISO 27001 bzw. davon abgeleitet die Norm ISO 27017 für Cloud Security an.

Verschlüsseln der Daten

Um die Daten effektiv gegen die erwähnten Gefährdungen zu schützen, sollten die Daten in verschlüsselter Form abgespeichert werden. Lösungen dazu gibt es eine Vielzahl. An dieser Stelle wird nur eine Lösung vorgestellt: Boxcryptor. Für bis zu zwei Geräte ist diese Lösung sogar kostenlos. Nach dem Installieren klinkt sich die Software zwischen der eigenen Festplatte und einer Vielzahl von Cloud-Diensten (Dropbox, OneDrive, Google Drive und über 20 weiteren Anbieter). Wird eine Datei auf das virtuelle Laufwerk X: (Standard-Laufwerk, kann aber geändert werden) kopiert oder verschoben, wird die Daten auf dem eigenen Rechner mit AES-256 und RSA-4096 verschlüsselt. Beides Verfahren, die als sehr sicher gelten. In der Cloud ist die Datei nur als „Daten-Schrott“ lesbar. Somit kann niemand auf den Inhalt der Daten zugreifen, ohne den passenden Schlüssel zu haben.



Bei der Cloud-Nutzung ist nicht mehr eine Frage, ob sondern wie diese optimal und sicher genutzt werden kann. Verschiedene Anforderungen zwingen, die Daten geschützt aufzubewahren. Die Verschlüsselung ist dabei eine effektive Möglichkeit, viele der (Business-) Anforderungen zu erfüllen und die Cloud sicher zu nutzen.