Inhalt

Cloud here, cloud there, cloud everywhere!

Welche Cloud ist die richtige?

So genanntes Cloud Computing dringt in immer mehr Bereiche unseres digitalen Alltags ein. Daten werden dabei nicht mehr auf dem jeweiligen PC, Tablet oder Smartphone gespeichert oder bearbeitet, sondern an einen oder mehrere Server gesendet. Dort findet dann zentral die Verarbeitung und Ablage der Daten statt. Das Verfahren des Cloud Computing ist in keiner Weise auch nur annähernd neu. Die Möglichkeit, Daten auf einem entfernten Server abzulegen, gab es schon zu Urzeiten des Internet. Jeder von Ihnen nutzt diese Möglichkeit. Wahrscheinlich ohne es zu wissen.

Stichwort „E-Mail“

Wo denken Sie, sind E-Mails gespeichert, bevor Sie sie abrufen?

Natürlich auf einem Server im Internet. Wenn Sie WEB-basierte E-Mail Dienste wie z.B. web.de verwenden, dann sind die Daten dort sogar dauerhaft gespeichert und organisiert. Das „Neue“ an Cloud Diensten ist der Umstand, dass man sich nicht nur um E-Mails, sondern um Ihre Anwendungsdaten kümmert. Also um Office Dokumente, Bilder, Videos, Musiken usw. Ohne den PC mitschleppen zu müssen, können Sie von nahezu jedem Ort der Welt auf die Daten zugreifen. Das hört sich nicht nur toll an, das ist auch toll. Auch die erweiterten Möglichkeiten, die sich aus dieser zentralen Verwaltung ergeben sind durchaus positiv. Die Auslagerung der Daten spart durchaus Investition in teure Hardware und Personal, enthebt einen scheinbar von der lästigen Pflicht, Daten regelmäßig zu sichern und rettet einen vor dem totalen Datenverlust, wenn das eigene Büro abbrennt.

Licht ohne Schatten? Mitnichten!

Welche Anwendertypen respektive –strategien gibt es? *

Wer nutzt wie die Cloud? Aus meiner persönlichen Erfahrung heraus gibt es im Zusammenhang mit Cloud Computing vier verschiedene Nutzertypen.

- Typ 1 – **Der Unkritische** – Er ist Technikfreak und von den Möglichkeiten der Cloud derart begeistert, dass er potentielle Gefahren nicht sieht oder ausblendet. Er stellt alle Informationen in die Cloud, ohne sich über mögliche Folgen im Klaren zu sein. Die technische Umsetzung interessiert ihn nicht.
- Typ 2 – **Der Gutgläubige** – Er nutzt die Cloud gerne und ohne Einschränkung was sensible Daten angeht. Er verlässt sich darauf, dass der Cloud Anbieter für die Sicherheit der Daten sorgt. Er nutzt die gleichen Möglichkeiten wie Typ 1, verspürt unterbewusst jedoch immer eine gewisse Restunsicherheit.
- Typ 3 – **Der Gefahrenbewusste** – Er ist sich der Gefahren durchaus bewusst und nutzt Cloud Lösungen ausschließlich punktuell und nur im Zusammenhang mit, aus seiner Sicht, unsensiblen Daten.
- Typ 4 – **Der Ablehner** – Er verzichtet aus Prinzip auf jede bewusste Nutzung der Cloud.

Cloud Anbieter *

Immer mehr Anbieter drängen auf den Markt. Jeder der etwas auf sich hält, verwendet in mindestens einem seiner Produkte die Bezeichnung Cloud. Sei es der Virenscanner, der verdächtige Dateien in die Cloud lädt, analysiert und kategorisiert oder die Bild-App, die Fotos sofort in die Cloud lädt, damit Freunde in Echtzeit in den Genuss der photographischen Meisterwerke kommen. Auf dem Smartphone gibt es kaum mehr eine **App**, die nicht die Nutzung der Cloud anbietet und das Feature besitzt, jede nur erdenkliche Information an Facebook zu senden oder aufbereitet auf eigenen Servern zu präsentieren.

Diese Cloud Lösungen sind Anwendungs- oder Datentypen-spezifisch, greifen also nur, wenn es sich um eine konkrete Anwendung oder einen bestimmten Datentyp handelt. De gegenüber stehen die s.g. generischen Lösungen die meist durch die ganz großen angeboten werden. Amazon, Microsoft, Google, Apple etc. gehören dazu. Hier geht es nicht um eine bestimmte Anwendung oder um einen bestimmten Dateityp, hier kann man jede Art von Datei/Information ablegen. Es handelt sich quasi um eine Infrastruktur zum Ablegen beliebiger Informationen respektive beliebiger Daten.

Wo sind die Daten? *

Die Frage ist unglaublich schnell dahin geschrieben und ebenso unglaublich schwer zu beantworten. Im Zweifelsfall kann Ihnen diese Frage nur der jeweilige Betreiber beantworten. Immerhin, werden Sie jetzt denken, dann kann man ja nachfragen. Jetzt werden Sie schnell sehr verwundert sein, wenn ich Ihnen sage, dass Anbieter von Cloud Lösungen oft selbst nicht wissen, wo die Daten liegen. Die Ursache ist rasch erklärt, leuchtet ein, hat durchaus folgenreiche Konsequenzen und verunsichert.

Die wenigsten kleinen Firmen können sich den Luxus leisten, eigene Server zu betreiben und eine technisch so anspruchsvolle Aufgabe einer Cloud Entwicklung meistern. Also baut man auf Vorhandenem auf. Dabei handelt es sich um die Infrastruktur der bereits erwähnten großen **Global Player**. Amazon Cloud, Windows Azur, Apple iCloud etc. stellen solche Infrastrukturen dar. Diese können Softwarefirmen relativ einfach in eigene Lösungen integrieren und so mit geringem Aufwand dem Anwender eine „eigene“ Cloud Lösung bieten. In Wahrheit stammt nur das s.g. Frontend (*Bedienpanel – Anwendung/App auf Ihrem Gerät*) von der Softwarefirma. Die Cloud selbst ist in der Hand eines ganz anderen Anbieters, der

vollkommen autark über alles entscheiden kann, was im Zusammenhang mit der Cloud steht. Also auch den Serverstandort, die Art der Speicherung, die Datenvolumina, die Kosten, den Umgang mit den Daten etc.

Wo liegt jetzt die Gefahr? *

Der Begriff **Global Player** deutet es an. Die Großen haben eigene Lizenz- und Nutzungsbedingungen, die die Anbieter der Anwendungen akzeptieren müssen. Sie hängen gnadenlos am Tropf dieser großen Firmen. Entschließt sich z.B. Amazon, den Cloud Dienst künftig exklusiv anzubieten, ihn also keinem Drittanbietern mehr zur Verfügung zu stellen, stehen alle im Regen, die auf die Amazon Cloud aufgebaut haben. Geht ein Großanbieter in die Insolvenz, gilt gleiches. Ändert Windows seine AGB für Azure, dann gilt das für alle Endanwender, deren Lösung auf diesem Dienst aufbaut. Und zwar unabhängig davon, was der Softwareanbieter selbst in seinen AGB stehen hat.

Der Begriff **Global** birgt noch eine andere große Gefahr. Die Server stehen in den seltensten Fällen in Deutschland, sondern meist irgendwo in Übersee. Dort werden die Daten dann nicht mehr durch deutsches Recht vor dem Zugriff durch Dritte geschützt. Vielmehr sind sie dem Zugriff durch staatliche Institutionen vollkommen schutzlos ausgeliefert. Zu diesem Schluss kommt auch eine Studie, die im Auftrag des EU-Parlaments die Sicherheit des Cloud Computing untersuchte. Hier gelangt man zur Erkenntnis, dass die Zunahme des Cloud Computing nicht zwingend mit einem Anstieg der Cyber Kriminalität einhergeht. ABER: Das Centre D'Etudes Sur Les Conflits (CetC)und das Centre for European Policy Studies (CEPS) warnen eindringlich davor, dass Cloud Anbieter wie Amazon, Google und Facebook US-Behörden heimlich Zugriff auf die Daten europäischer Nutzer verschaffen können.

> **Werden Daten auf ausländischen Servern abgelegt, verliert man jede Kontrolle.**

Der 11. September 2001 machte in den USA den Weg frei für die Sicherheitsgesetzte zur Terrorabwehr. Mit dem s.g. Patriot Act und dem Foreign Intelligence Surveillance Amendment Act (FISAA) steht ein umfassendes Recht zum Abhören bereit. Neben diesem Recht zur umfänglichen Überwachung steht man einer anderen Bedrohung gegenüber. Die National Security Agency (NSA) verfügt über gigantische

Rechenkapazitäten. Wer also denkt, sich in der unüberschaubaren Menge an Daten verstecken zu können, wird böse enttäuscht. Mit einer derart schlagkräftigen **Rechenarmada** im Hintergrund kann man unglaubliche Datenmengen in überschaubarer Zeit auf jede nur erdenkliche Weise nach Inhalten und Zusammenhängen durchforsten. Das betrifft nicht nur Privatpersonen, sondern kann besonders Firmen treffen, die, um ein paar Euro zu sparen, die Speicherung von Daten outsourcen. Industriespionage wird damit zum Kinderspiel.

Während man von diesen heimlichen Zugriffen wortgemäß nicht direkt etwas erfährt, gibt es inzwischen Beispiele für Zugriffe und Manipulationen durch die Cloud Anbieter, die zunächst lustig oder wenig beunruhigend erscheinen.

Apple bietet mit iTunes Match einen Dienst an, bei dem man seine komplette Musiksammlung in die Cloud verlagern kann. Vorteil: Man kann von überall auf die Daten in der Musiksammlung über die Cloud zugreifen. Soweit, so gut! Jetzt gibt es aber durchaus Musikstücke, in denen Wörter und Formulierungen vorkommen, die nicht zwingend „jugendfrei“ sind. [*Anm.: Es geht hier nicht um indizierte Titel*] Was liegt da für den guten Cloud Anbieter näher, als die Verpiepung entsprechender Passagen.

Google ist moralisch gesehen mit Sicherheit auf Augenhöhe mit Apple. Wen wundert es also, wenn man sehr ähnliche Verfahren findet. Vorerst dürfen sich jedoch nur amerikanische Nutzer des Scan und Match Dienstes über diesen kostenlosen Verpiepungsdienst freuen. Europäer müssen leider noch warten.

Wie angedeutet kann man hier schmunzeln. Denkt man darüber nach, was hier geschieht, friert das Lachen rasch ein. Es handelt sich um nichts anderes, als um **Zensur**. Und zwar um eine Zensur durch ein privates Unternehmen! Das Beispiel zeigt auch ganz wunderbar, wie unser obiger Typ 3 – Der Gefahrenbewusste – Cloud Nutzer in die Falle tappen kann. Musik ist sicher nichts, was der Durchschnittsbürger in die Kategorie sensible Daten stecken würde. Es kommt der Tag, an dem Computerprogramme unsere Musik und unsere eBooks durchsuchen und anhand der Inhalte Rückschlüsse über unsere Charaktermerkmale ziehen werden. Minority Report lässt grüßen.

Kehren wir noch einmal zu den Anwendertypen zurück

Wie reagieren unsere Nutzertypen auf beunruhigende Nachrichten oder auf Konsequenzen aus den obigen Gefahren?

Typ 1 – Der Unkritische – lässt sich durch nahezu nichts abschrecken. Er schreibt höchstens eine geharnischte E-Mail an den Support, wenn er sich durch Piepen in seiner Musik gestört fühlt. Eine Standard-Antwort des Supports beruhigt ihn. Typ 1 wird kaum dazu zu bewegen sein, den unkritischen Umgang mit der Cloud aufzugeben. Erst dann, wenn er selbst erhebliche Nachteile aus der Cloud-Nutzung erfahren muss, wird er nachdenklich.

Typ 2 – Der Gutgläubige – wird sich von einzelnen Cloud Lösungen verabschieden, wenn er sein Vertrauen getäuscht sieht. Dazu genügt es bereits, dass er von Missbräuchen und Manipulationen erfährt. Typ 2 wird am ehesten auf „sichere“ Cloud Lösungen umsteigen.

Typ 3 – Der Gefahrenbewusste – verzichtet künftig vermutlich komplett auf Cloud Lösungen, weil er trotz vermeintlich umsichtigen Umgangs erfahren musste, dass er einer Fehleinschätzung unterlag.

Typ 4 – Der Ablehner – sieht sich in seinem Verhalten bestätigt und setzt weiterhin auf den Totalverzicht.

Welcher Anwendungstyp fährt am sichersten?

Ganz klar der ablehnende Typ 4. Nur er ist durch den Verzicht gegen jede Art von Missbrauch gewappnet. Wer diese Strategie fahren kann, ohne wesentliche Nachteile zu erleiden, ist hier gut aufgehoben. Die Frage ist, ob die normative Kraft des Faktischen nicht irgendwann einmal die Nichtnutzung der Cloud unmöglich macht. In diesem Fall ist Typ 3, der nur punktuell auf die Cloud zurückgreift und dann zur Absicherung seiner Daten zusätzliche Mittel wie Verschlüsselung einsetzt, derjenige, der mit der größten Sicherheit unterwegs ist.

Was ist bei den verschiedenen Cloud Lösungen zu beachten? *

Als Leser hat man schnell bemerkt, dass es zwischen den zwei Arten von Clouds (*Anwendungs- Datentypen- spezifische Cloud und generische Cloud*) erhebliche Unterschiede gibt. Bei Anwendungs- oder Datentyp-bezogenen Clouds hat man im besten Falle die Wahl zwischen verschiedenen Großanbietern. Einfluss über die Art der Ablage der Daten hat man nicht. So ist es z.B. nicht möglich, Daten bei iTunes

Match oder Google Scan and Match mit einem unabhängigen Werkzeug abzusichern. Verschlüsselung ist nicht möglich, folglich kann der Anbieter mit den Daten machen, was er möchte.

> Man kann sich nur für oder gegen den Dienst entscheiden.

Ein „gutes“ Beispiel ist What’s App“. Die Anwendung speichert das Adressbuch des Anwenders mit allen Kontakten auf dem eigenen Server. Stimmt man dem nicht zu, kann man die Anwendung nicht verwenden. Obwohl man What’s App selbstverständlich auch nutzen könnte, indem man die Anwendung selbst mit entsprechenden Daten füttert. Hier geht es also von Seiten des Anbieters nicht um etwas, was technisch nicht anders zu realisieren wäre. Es geht, wie so oft, um das Sammeln und Auswerten von Daten.

Insgesamt schadet es nicht, wenn man sich vor der Benutzung der entsprechenden Cloud gedanklich klar macht, welchen Vorteil die Nutzung eines Dienstes wirklich bringt. Hier geht es um eine Güterabwägung.

Beantworten Sie sich bei dieser Art der Cloud die folgenden Fragen:

- Möchte ich im Zweifelsfall, dass andere diese Daten einsehen können?
- Was können andere mit diesen Daten für „Unfug“ anstellen?
- Sind persönliche Informationen anderer Betroffen?

> Gerade die letzte Frage hat es in sich. Kontaktdaten und Bilder, auf denen andere zu sehen sind, dürfen nur weiter gegeben werden, wenn der Rechteinhaber dieser Weitergabe ausdrücklich zustimmt! Wenn Sie What’s App die Genehmigung erteilen, Ihre Kontaktdaten auf den Server zu laden, verstoßen Sie mit Sicherheit gegen diesen Grundsatz!

Bei den **generischen Cloud Lösungen** hat man weitergehende Möglichkeiten, Einfluss auf die Art der Dateiablage zu nehmen. Dabei sollten Sie folgende Hinweise berücksichtigen.

- Legen Sie in der Cloud nur die Daten ab, die Sie in der Cloud benötigen. Dazu

müssen Sie sich klar machen, was Sie mit der Cloud erreichen wollen. Die Cloud macht Sinn, wenn man dort zum Beispiel Sicherungen lokaler Daten abgelegt. Möchte man unterwegs auf bestimmte Daten zugreifen, sollte man diese Daten als Kopie in der Cloud ablegen. Verzichten Sie unbedingt darauf, die kompletten Daten ausschließlich in der Cloud zu halten (*siehe nächster Punkt*).
- Sofern möglich, belassen Sie die Datenhoheit in ihrem Haus und verzichten Sie auf Outsourcing in diesem Bereich. Im Zweifelsfall ist man dem Betreiber der Cloud auf Gedeih und Verderb ausgeliefert und steht ohne eigene Daten da. Serverausfall, Netzwerkstörungen und im schlimmsten Fall Insolvenz können fatale Folgen haben.
- Wenn eine Auslagerung in die Cloud stattfindet, dann ausschließlich verschlüsselt. Vertrauen Sie nicht darauf, dass die Daten auf dem Server ver- und entschlüsselt werden. Suchen Sie nach einer Lösung, die die Daten lokal auf Ihrem System ver- und entschlüsselt. Das Passwort, mit dem Sie den Zugriff auf die Daten steuern, sollte dabei niemals Ihren Rechner verlassen. So verhindern Sie, dass zum Beispiel Administratoren der entsprechenden Server auf die Daten zugreifen können. Verschaffen sich Angreifer Zugriff auf die Server, schützt Sie immer noch die eigene Verschlüsselung.
- Suchen Sie eine Lösung, bei der die Server in Deutschland stehen.
- Achten Sie darauf, dass Sie die Daten aus der Cloud regelmäßig laden und lokal sichern können. Unabhängig von den Sicherungsmaßnahmen des Cloudanbieters.
- Wenn Sie auf einen der populären Dienste (*Google Drive, Dropbox etc.*) zurückgreifen möchten oder **müssen**, laden Sie **niemals** sensible Daten ungeschützt in die Cloud. Nutzen Sie Programme wie zum Beispiel das kostenlose ArchiCrypt Easy Encryption um Unbefugten den Zugriff zu verweigern.

Fazit: Wir haben gelernt, das Cloud Computing im Prinzip nichts Neues ist. Auch der E-Mail Dienst ist eine Art Cloud-Computing. Es gibt zwei Arten von Cloud Lösungen. Eine Anwendungs- und Datentyp-spezifische Cloud, die sich nur auf eine bestimmte Anwendung oder einen bestimmten Datentyp bezieht (*zum Beispiel iTunes Match – Musikdateien*) und eine generische Cloud (*z.B. Google Drive*), die grundsätzlich jede Art von Daten aufnehmen kann. Während man bei der Anwendungs- und Datentyp-spezifischen Cloud oft nur entscheiden kann, ob man die Lösung nutzt, oder nicht, hat man bei den generischen Lösungen weitergehende Möglichkeiten. Dabei gilt, dass man ausschließlich Daten in die Cloud laden soll, die dort zwingend sein müssen. Dabei ist unbedingt darauf zu achten, dass die Daten in verschlüsselter Form abgelegt

werden.

