Datenschutz und Datensicherheit beim Cloud Computing

Felix Malek

Seminararbeit im Interdisziplinären Lehrangebot
des Instituts für Informatik

Leitung: Prof. Hans-Gert Gräbe, Ken Pierre Kleemann

`http://bis.informatik.uni-leipzig.de/de/Lehre/Graebe/Inter`

Leipzig, 31.10.2017

Inhalt

1. Einleitung

Im Jahr 2016 standen ca. 47% aller Unternehmen dem Trend des „Cloud Computing“ aufgeschlossen gegenüber, wohingegen im Jahr 2011 es noch 28%. Die Tendenz ist weiterhin stark steigend. Vor allem größere Unternehmen setzen auf die Lösung in der Datenwolke. Flexibles und effektiveres Arbeiten, zeitlich und räumliche Ungebundenheit sind die klaren Stärken der Cloud und nebenher sollte der Kostenfaktor den Unternehmern sehr gut gefallen. Prognosen sagen dem Cloud Computing einen Umsatz von ca. 31,5 Milliarden € allein in Deutschland im Jahre 2020 voraus.

Doch warum stehen immer noch so viele Unternehmen dem Cloud Computing negativ gegenüber?

Die beiden meist genannten Faktoren sind Datenschutz und Datensicherheit.
In der folgenden Arbeit möchte ich grundlegend die Begriffe „Cloud Computing“, „Datenschutz“ und „Datensicherheit“ erklären, Probleme aufzeigen und eventuelle Lösungsmöglichkeiten anbieten. Ob die 53% der Unternehmer im Recht liegen, oder ob die Zweifel unbegründet sind, sollte am Ende dieser Arbeit geklärt sein.

2. Definitionen

2.1. Cloud Computing

Cloud Computing ist ein mehrschichtiger Begriff. Grundlegend beschreibt er die Auslagerung von Soft- und Hardwareressourcen an externe Serviceanbieter. Durch diese Auslagerung und die Möglichkeit, jeder Zeit von einem kompatiblen Endgerät auf die ausgelagerten Daten und Services zu zugreifen, entstand das Bild der über einem schwebenden „Datenwolke“. Um diese Services nutzen zu können ist in den meisten Fällen ein Webbrowser von Nöten. Ein „Service“, oder auch „Dienst“, beschreibt eine Gruppe von Operationen die eine Schicht (OSI-Schichtenmodell), der höheren Schicht über einen Dienstzugangspunkt (=SAP=Service Access Point) verfügbar macht. (vgl. http://www.itwissen.info/Dienst-service.html (Abgerufen am 29.10.2017))

Je nach Bedarfsbereich, kann man verschiedene Servicemodelle des Cloud Computing nutzen. Benötigt der Nutzer nur Speicherplatz oder virtuelle Maschinen (~Infrastruktur), so sollte er auf Infrastructure-as-a-Service (kurz: IaaS) zurückgreifen. Bei einer Entwicklungs-/ Ausführungsumgebung sollte man Platform-as-a-Sevice (kurz: PaaS). Und für komplette Softwarelösungen (meist direkt über den Webbrowser verfügbar), kann der Nutzer auf Software-as-a-Service zurückgreifen.

Als weiteres Unterscheidungsmerkmal neben den Services, sind die Anwendungsbereiche zu nennen. Dem normalen Verbraucher werden vor allem die Public Clouds ein Begriff sein. Das sind Dienste, die durch einen frei zugänglichen Provider zu erreichen sind. Ein bekanntes Beispiel ist Google Docs.

Im Gegensatz dazu steht die Private Cloud. Viele Unternehmen ziehen es vor, ihre IT-Dienste auch weiterhin allein zu betreiben und ausschließlich ihren Mitarbeitern zugänglich zu machen. Werden diese Dienste so angeboten, dass der Nutzer die cloud-typischen Vorteile nutzen kann, so spricht man von einer Private Cloud.

Wenn sich mehrere Private Clouds, beispielsweise von verschiedenen Unternehmen, für ein Projekt o.ä. zusammenschließen, so dass die Nutzer Zugriff auf alle Teile der zusammengefügten Cloud haben, spricht man von einer Community Cloud.

Die letzte Art der Cloud ist die Hybrid Cloud. Diese ist eine Mischform bestehend aus den Vorteilen der Public Cloud, aber der Absicherung sensibler Daten durch die Nutzung von Diensten in einer Art „Private Cloud“. Wenn das Unternehmen Datenschutzkritische und –unkritische Workflows trennen und auf die jeweiligen

Public- und Private-Anteile der Hybrid Cloud auszulagern, stellt diese Form der Cloud eine Nachdenkens Werte Alternative dar.

2.2. Datenschutz

Grundlage des Datenschutzes ist der Schutz der Privatsphäre des Menschen. Auch durch verschiedene Gesetze wird der Bürger vor der missbräuchlichen Nutzung seiner Daten geschützt.
„Jeder soll selbst bestimmen können, wem und wann er welche Daten zu welchem Zweck zugänglich macht.“ (Zu finden auf https://www.bdsg-externer-datenschutzbeauftragter.de/datenschutz/was-ist-datenschutz/ (Abruf 31.10.2017))
Der Datenschutz soll, vor allem in der heutigen Gesellschaft der Tendenz zum „Gläsernen Menschen“, sowie dem Entstehen von Datenmonopolen als auch dem Ausufern Staatlicher Überwachungsmaßnahmen entgegen wirken.

Datenschutzregeln bestehen in Deutschland seit den 70er Jahren, als Reaktion zur Einführung der elektronischen Datenverarbeitung. Diese Regelungen gelten jedoch nur für Deutschland und sind teilweise durch den Austausch von Daten mit Ländern, welche diese Regelungen nicht eingeführt haben, schwer bis kaum durchsetzbar.

Datenschutz beinhaltet nicht den Schutz von Daten vor Diebstahl oder Verlust im Allgemeinen (siehe 2.3. Datensicherheit)

2.3. Datensicherheit

Datensicherheit beinhaltet den Schutz von Daten vor Manipulation, Diebstahl oder Verlust ebendieser. Wie dieser Schutz aussieht kann vielfältige Formen annehmen. Ob es nun die physische Sicherheit, Verschlüsselung der Kommunikation, Schutz vor Fremdzugriffen oder Datensicherungen (uvm.), alle diese Aspekte sind ein Teil der Datensicherheit.

Dem Datenschutz liegen drei Grundsätze zu Grunde: Der Grundsatz der Vertraulichkeit (nur autorisierte Benutzer können Daten lesen od. bearbeiten), der Grundsatz der Integrität (sollten Veränderungen an den Daten vorgenommen

werden, so müssen diese lückenlos nachzuvollziehen sein) und der Grundsatz der Verfügbarkeit (Daten müssen innerhalb eines vereinbarten Zeitraumes stets verfügbar sein.)

Trotz alledem, kann man Datenschutz und Datensicherheit nicht zu 100% voneinander getrennt definieren. Beide Begriffe können maximal abgegrenzt und damit zu Orientierung verwendet werden.

3. Gefahren für Datenschutz/Datensicherheit durch Cloud Computing

Cloud Computing wird oftmals eher skeptisch betrachtet, vor allem hinsichtlich der Aspekte der Datensicherheit und des Datenschutzes. Viele entscheiden sich daher gegen die Nutzung einer Cloud.
Welche Risiken bestehen wirklich bei der Nutzung von Cloud-Diensten?

Eines der Grundprobleme vom Cloud Computing ist der Betrieb der Infrastruktur durch Dritte. Die Nutzer haben ihre Daten nicht auf ihrem eigenen Rechner gespeichert, sondern auf einem Server, welcher irgendwo anders in der Welt steht und auf diesen greift der Nutzer nur über IP-Netze zu.
Man vertraut also einem Server Daten an, welchen man selber nicht betreibt und daher von einer fremden Person betrieben wird.

Die Gefahren für die Daten beginnen aber nicht mal auf dem Cloud-Server an sich, sondern bereits beim Datentransport. Daten werden nicht nur vom Anwender zum Dienstleister transportiert, sondern noch zwischen verschiedener Rechenzentren und ebenfalls innerhalb der Rechenzentren als solche. Durch die Vielzahl an Transportwegen besteht die Gefahr, dass Daten verloren gehen, Daten abhört oder verfälscht werden.

Sobald die Daten auf dem Zielserver angekommen sind, sind die Sicherheitsbedenken immer noch nicht von der Hand zu weisen. Die Cloud-Anwendung als solche ist ebenfalls eine Gefahr. Unsichere Schnittstellen und APIs machen es verhältnismäßig leicht eine Cloud (vorallem die Public Cloud)

anzugreifen. Auch über Schwachstellen im Interface und/oder bei Schnittstellen zur Konfiguration des Cloud-Services bestehen Möglichkeiten für Angriffe.
Da eine Cloud-Anwendung für viele Nutzer dieselben Ressourcen verwendet (Pooling) kann es zu Problemen bei der Trennung von Nutzerdaten kommen.

Ein weiteres Risiko stellt die Anwendung als solche beim Endnutzer dar. Der Nutzer greift über seine Clientseitige-Anwendung auf den Server zu, da eine Internetverbindung von Nöten ist und kann damit ebenfalls als Ziel für Angriffe als Möglichkeit dienen. Hervorzuheben wäre hier das Phishing.

(Spear-Fishing (=Phishing innerhalb bestimmter Personengruppen) oder Whaling (=Phishing bei einer Person mit einer hohen Anzahl an Rechten (z.b. Administratoren) um Zugriff auf die Cloud-Anwendung zu erhalten)).

Dieser Gedanke kann beispielsweise auch weitergesponnen werden. Der Angriff kann beispielsweise auch durch Insider geschehen. Wie bereits erwähnt lagern die Daten auf Servern bei Firmen/Personen, welche den Server stellen, man als Nutzer aber nur in den aller seltensten Fällen wirklich kennt.
Die Gefahr, dass also Mitarbeiter des Dienstleisters sich Zugriffe auf Kundendaten beschaffen und/oder der allgemeine Diebstahl von Benutzerkonten stellt sich hierbei als besonders problematisch dar.

Ein weiteres, eher banal klingendes Problem, ist die ständige Abhängigkeit von einer stabilen Internetverbindung. Ohne kann die Cloud nicht verwendet werden vom Nutzer. Dadurch eröffnet sich ein weiteres Problem. Wenn eine Internetverbindung von Nöten ist, was ist dann mit eventuellen Ausfällen beim Anbieter als solches. Zu nennen, wäre hierbei eine (D)DoS-Attacke ((Distributed) Denial-of-Service) auf den Server des Anbieter, was passiert, wenn der Anbieter eventuell (auch versehentlich) fehlerhafte Software auf dem Server installiert? Und währenddessen eine Übertragung von Daten zwischen Anwendung und Cloud stattfindet? Gehen die Daten dann verloren?
Ein ähnlicher Fall wäre der sogenannte „Vendor-Lock-In“. Dieser besagt, dass eine Abhängigkeit vom Nutzer zum Anbieter besteht. Sei es vertraglich oder aus anderen Gründen, ist es dem Nutzer nicht möglich den Anbieter zu wechseln. Sollte das der Fall sein und der Anbieter fährt seinen Cloud-Dienst herunter, was passiert mit den Daten des Nutzers?

Diese Fragen sind es, welche die Nutzer beschäftigen und welche von den Cloud-Anbietern gelöst werden müssen.

4. Lösungsansätze für die sichere Nutzung von Clouds

Vorallem für Unternehmen stellt sich die Frage: „Benötigen wir eine Cloud? Wenn ja, welche?“
Diese Frage lässt sich niemals pauschal beantworten und bedarf auch einige Zeit bis man als Unternehmer die optimale Lösung gefunden hat. Diese sollte möglichst sichersein und den eigenen Ansprüchen entgegenkommen.
Um möglichst Fehler zu vermeiden, wie z.B: fälschlicherweise einen mangelhaften Vertrag mit dem Anbieter abzuschließen, sollte vorher ein oder mehrere Personen eine Analyse des eigenen Unternehmens erstellen um herauszufinden: „Welche Dienstleistungen benötigt die Firma? Was für Daten werden im Zuge des Projektes (o.ä.) verwendet? Sind diese Daten schützenswert? Wie viele Mitarbeiter sollen Zugriff auf die Cloud haben? Wie groß ist das Budget für das Cloudsystem? Ist die Bandbreite in der Firma groß genug?“ Dies ist nur eine Auswahl der Fragen, welche für die Analyse von Relevanz sind. Für die Datensicherheit und den Datenschutz sind vor allem die Fragen zum Thema Daten und Kosten relevant. Viele Anbieter von Clouds bieten ideale Lösungen an, wobei es dann am finanziellen Aspekt scheitert.

Anschließend sollte eine Risikoanalyse durchgeführt werden. Eventuelle Risiken bei der Nutzung von Clouds werden ausgiebig unter Punkt 3 ausgeführt.
Alle bisherigen Analysen sind Grundgerüste, welche immer weiter verfeinert werden. Der potentielle Kunde formuliert dann weiterhin noch eine Service- (Was soll die Cloud können), Schnittstellen- (Schnittstellen des Anwenders/Authentisierungsmittel) und Verandwortungsbereichs-Definition (Definieren, wofür Anbieter und Kunde verantwortlich sind).

Das Sicherheitskonzept ist dann einer der letzten Schritte bevor es zu Auswahl des Cloud-Anbieters geht. Jeweils Anbieter und Anwender sollten ein solches besitzen. Auf Anfrage, sollte der Cloud-Anbieter dem Anwender Einsicht gewähren.

Nun kann der Cloud-Anbieter aufgrund der angegebenen Kriterien gesucht werden. Der Vertrag mit dem Cloud-Anbieter sollte folgende Bestandteile enthalten:

„» Subunternehmer

» Einhaltung von Sicherheitsanforderungen, möglichst mindestens nach dem BSI Anforderungskatalog Cloud Computing C5

» Infrastruktur des Cloud-Diensteanbieters und Personal

» Kommunikationswege und Ansprechpartner

» Regelungen zu Prozessen, Arbeitsabläufen und Zuständigkeiten

» Ggf. besondere Regelung bei Sicherheitsvorfällen oder Betriebsunterbrechungen beim Cloud-Anbieter (z. B. Zugriff auf Log-Dateien)

» Beendigung und Datenlöschung

» Notfallvorsorge

» Regelungen zu rechtlichen Rahmenbedingungen

» Änderungsmanagement

» Kontrollen

» Vertragsstrafen bei Nichterfüllung

» Haftungsfragen“

(Zu finden unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Sichere_Nutzung_Cloud_Dienste.pdf?__blob=publicationFile Abgerufen am 29.10.2017)

Wichtig ist es hierbei, dass die eigenen gesetzten Sicherheitsrichtlinien- und Ziele eingehalten werden.
Hält man sich als Unternehmen an diesen Plan (Detailliert unter der ebengenannten Website (Broschüre) des BSI zu finden) minimiert man einige Sicherheitsrisiken.

Ob nun als Unternehmen oder doch als Privatperson, trotz sorgfältiger Auswahl des Cloud Anbieters, besteht immer noch ein gewisses Sicherheitsrisiko. Welche Möglichkeiten bestehen dahingehend noch?
Man kann seine Daten, bevor man sie in die Cloud legt verschlüsseln mittels einer Ende-zu-Ende-Verschlüsselung (kurz E2EE="end-to(=2)-end-encryption") verschlüsseln. Dafür gibt es mittlerweile zahlreiche Programme, welche dies ermöglichen (Bsp.: tresorit, SecureSafe).
Wer den Betreibern solcher Cloud-Dienste immer noch skeptisch gegenüber ist, kann auch noch, mit dem gewissen IT-KnowHow sich eine ownCloud anlegen. Diese Cloud läuft auf dem eigenen Server, funktioniert ähnlich wie z.B.: Dropbox und ermöglicht es dem Nutzer zu wissen, wo genau seine Daten sich befinden und wer genau wirklich Zugriff auf seine Daten hat.

5. Fazit

Cloud-Dienste sind die Zukunft. Diesen Satz hat wohl jede Person, welche sich mit IT beschäftigt schon einmal gehört. Aber die Zahlen belegen es. Die Nutzung von Cloud-Anwendungen steigt unaufhaltsam. Bereits kleinere Unternehmen setzen mehr und mehr auf Cloud Computing.
Auch verschwinden mehr und mehr die Sicherheitsbedenken der Nutzer. 2012 gab es einen großen Hackerangriff auf Dropbox, den wohl bekanntesten Anbieter von Cloud-Diensten, bei dem ca. 68 Millionen Nutzerdaten gestohlen wurden. Genau solche Vorkommnisse sind immer noch das Problem, welches viele Nutzer noch davon abhält ihre Daten in der Cloud zu sichern. Trotzdem fällt mein persönliches Plädoyer für die Cloud aus. Noch nie war es einfacher mit mehreren Leuten an Projekten zusammen zu arbeiten, noch nie war es leichter Daten zu übertragen. Viele der Sicherheitsrisiken (z.B.: Angriffe während der Datenübertragung) könnten natürlich vermindert werden, aber in Zeiten des WWW 2.0, in welchen fast sowieso jeder Nutzer mit jedem anderen Kontakt aufnehmen kann, besteht immer ein gewisses Risiko. Auch ohne Cloud Computing, besteht also die Möglichkeit für einen Angreifer, gezielt an meine Daten zu kommen, wenn er es wirklich darauf ansetzt. Natürlich stellen Clouds eine besondere Angriffsfläche dar und auch für Firmen, welche sensible Daten innerhalb der Cloud nutzen wollen/müssen, ist das Risiko

wirklich latent spürbar. Und auch hier gibt es eine Lösung. Die Private Clouds und/oder ownClouds. Wie bereits in Punkt 4 erwähnt, stellen diese Lösungen für einige in Punkt 3 aufgezeigte Probleme. Auch die Cloud-Anbieter als solche werden immer sicherer, denn z.B.: seit 2012 wurde kein Fall von einem weiteren Angriff o.ä. auf Dropbox (siehe Beispiel oben) berichtet. Der Fortschritt, vor allem bei der Sicherheit von Clouds, ist rasend schnell.

Der Cloud gehört die Zukunft. Und ich sehe das genauso.

6. Literaturverzeichnis

Internetquellen:

https://www.datenschutzbeauftragter-info.de/datenschutz-und-datensicherheit-beim-cloud-computing/ (Abruf: 26.10.2017)

http://eddi.informatik.uni-bremen.de/SUSE/pdfs/Diplomarbeit_Steffen_Bothe.pdf (Abruf: 26.10.2017)

https://www.tecchannel.de/a/ratgeber-sicheres-cloud-computing,2039977 (Abruf: 28.10.2017)

https://de.statista.com/themen/562/cloud-computing/ (Abruf: 28.10.2017)

http://www.itwissen.info/Dienst-service.html (Abruf: 29.10.2017)

https://www.bdsg-externer-datenschutzbeauftragter.de/datenschutz/was-ist-datenschutz/ (Abruf: 29.10.2017)

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Sichere_Nutzung_Cloud_Dienste.pdf?__blob=publicationFile (Abruf 29.10.2017)