Fachhochschule Wedel

Seminararbeit

in der Fachrichtung

Wirtschaftsinformatik (Bachelor)

Seminar IT-Sicherheit

Thema:

(In-)Secure Cloud Computing

Wintersemester 2012/2013

Eingereicht von: Jan Nill

Matr.Nr.: Winf9102

E-mail: winf9102@fh-wedel.de

Seminarleiter: Prof. Dr. Gerd Beuster

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

1.1 Motivation

Die Cloud (zu deutsch: Wolke) ist *das* Schlagwort der heutigen Zeit. Der Begriff Cloud Computing beschreibt das externe Bereitstellen einer Menge von Diensten über das Internet, die u.a. Serverstrukturen, Datenspeicher oder auch Software darstellen können. Diese Dienste können individuell an Nutzer angepasst werden und bieten so eine optimale Ressourcennutzung für Unternehmen, die keine eigenes Rechenzentrum betreiben.
Durch die Globalisierung werden Unternehmen immer internationaler und benötigen ein gemeinsames Netzwerk um überall auf der Welt den gleichen Standard bieten zu können. Auch Privatpersonen nutzen heutzutage häufig die Cloud, um ihre Fotos, Musik oder Dokumente in ihr zu speichern. Das Cloud Computing bietet dafür die notwendige Flexibiltät an jedem Ort auf der Welt mit beliebigen Medien auf gespeicherte Daten zugreifen zu können.
Auch wenn Cloud Computing viele Vorteile/Potentiale ermöglicht, so sollten jedoch die Gefahren nicht außer Acht gelassen werden. Bei der Nutzung der Cloud ergeben sich zwangläufig Fragen über die Sicherheit der Daten und die Gefahr des unerlaubten Fremdzugriffs.
Somit ist es sowohl für Unternehmen als auch für Privatpersonen wichtig herauszustellen, ob die Cloud ein geeigneter Weg in die Zukunft ist und wo sie Gefahren und Chancen bietet.

1.2 Themenstellung und Gliederung

Die vorliegende Seminararbeit beschäftigt sich mit dem Thema (In-)Secure Cloud Computing. Dabei gilt es herauszustellen, welche neuen Anforderungen und Risiken sich ergeben, wenn Daten und Rechenschritte ausgelagert werden. Zudem werden Möglichkeiten zur Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit bei der Arbeit mit und in der Cloud geklärt.
Die Seminararbeit befasst sich im ersten Kapitel zunächst mit der Motivation und Notwendigkeit für die Auseinandersetzung mit dem Thema (In-)Secure Cloud-Computing.
Dazu gilt es in Kapitel zwei auf die wesentlichen Begriffe in diesem Zusammenhang einzugehen. Neben der Definition von Cloud Computing und den verschiedenen Servicemodellen werden unterschiedliche Cloud-Infrastrukturen erläutert, die die

Möglichkeiten der Cloud-Nutzung veranschlaulichen. Zudem werden datenschutzrechliche Anforderungen bei der Speicherung von Daten im Ausland und die vertragliche Bindung zwischen Cloud-Nutzer und -Anbieter dargestellt.
Im darauf folgendenden Kapitel werden zunächst die in der Einleitung bereits angesprochenen Potentiale des Cloud Computings für Unternehmen, Wirtschaft und Privatpersonen näher erläutert. In diesem Zusammenhang werden Sicherheiten des Cloud Computings wie Zertifizierungen für Cloud-Anbieter als Entscheidungskriterium für Cloud-Nutzer dargestellt.
Daraufhin werden in Kapitel vier die Unsicherheiten von Cloud Computing dargestellt und Lösungsansätze diskutiert. Dabei spielen Verfügbarkeit und Datensicherheit bei einem Ausfall und Angriff auf die Cloud-Umgebung die zentralen Aspekte und müssen durch effektive Sicherheitsmechanismen gewahrt werden.
Schließlich werden in einer finalen Schlussbetrachtung die wichtigsten Erkenntnisse aus der vorliegenden Arbeit zusammengefasst und ein persönliches Fazit gezogen.

2 Grundlagen zu Cloud Computing

Dieses Kapitel definiert den Begriff, die Eigenschaften und die zentrale Technologie von Cloud Computing und beschreibt die verschiedenen Arten des Cloud Computing. Dazu werden auch datenschutzrechtliche Anforderungen veranschaulicht, wenn beispielsweise Daten im Ausland gespeichert werden. Zudem werden einzuhaltende Richtlinien im Vertrag zwischen Cloud-Nutzer und -Anbieter dargestellt.

2.1 Begriffsbestimmung Cloud Computing

2.1.1 Definition

Für das Cloud Computing gibt es keine allgemeingültige Definition, jedoch verwenden viele Publikationen die Definition des National Institut of Standards and Technology (NIST). Demnach ist „Cloud Computing ein Modell, das es Nutzern ermöglicht bei Bedarf jederzeit und überall bequem über ein Netzwerk auf einen gemeinsamen Pool von konfigurierbaren Rechnerressourcen (z.B. Netzwerke, Server, Datenspeicher, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringfügiger Service Provider Interaktion zur Verfügung gestellt werden können.“[1]
Cloud Computing benutzt die Virtualisierung und das moderne Web, um Ressourcen verschiedenster Art miteinander zu kombinieren und als verfügbare Dienste dem

[1] Mell, P., Grance, T.: Definition of Cloud Computing, 2011, S. 2 (eigene Übersetzung)

Nutzer bereitzustellen. Diese Dienste können für jeden Nutzer individuell eingerichtet werden. Durch virtuelle Rechen- und Speicherressourcen und das moderne Web stellt Cloud Computing individuell anpassbare, netzwerkzentrierte IT-Infrastrukturen, Plattformen oder Anwendungen als on-demand Dienste (Dienste auf Anforderung) zur Verfügung. Diese werden entsprechend der genutzten Ressourcenumfänge individuell für jeden Nutzer abgerechnet.[2] Im weiteren Verlauf dieser Arbeit wird im Bezug auf Cloud Computing immer von dieser Definition ausgegangenen.

2.1.2 Eigenschaften

Das National Institute of Standards and Technology bestimmt für das Cloud Computing fünf wesentliche Eigenschaften:

1. *on-demand Diensterbringung*: Die Dienste einer Cloud sind für Konsumenten automatisch ohne zusätzliches Handeln des Internet Service Providers nutzbar.
2. *Netzwerkbasierter Zugang:* Dienste können über das Netzwerk durch Standard-technologien abgerufen werden.
3. *Ressource Pooling:* Die Ressourcen einer Cloud sind in einem sogenannten Ressourcen-Pool konzentriert und erlauben so den zeitgleichen Zugriff von mehreren Nutzern mit individueller Ressourcen-Anpassung. Dabei ist dem Nutzer der genaue Standort der Ressourcen nicht bekannt. In dem Vertrag mit dem Cloud-Anbieter hat der Cloud-Nutzer die Möglichkeit abstrakt den gewünschten Standort zur Speicherung seiner Daten anzugeben (z.B. Land).
4. *Schnelle Elastizität:* Dadurch, dass die Ressourcen schnell und flexibel zur Verfügung gestellt werden können, in manchen Fällen sogar automatisch, entsteht für den Nutzer der Eindruck einer unerschöpflichen Ressourcen-Menge.
5. *Messbare Dienstqualität:* Die Ressourcennutzung kann überwacht und dokumentiert werden, sodass dem Nutzer nur seine verbrauchten Ressourcen in Rechnung gestellt werden.[3]

2.1.3 Virtualisierung

Die zentrale Technologie unterschiedlicher Cloud-Architekturen ist die Virtualisierung von Ressourcen. Dabei werden physische Ressourcen wie Netzwerke, Server, Anwendungen oder Datenspeicher virtuell dargestellt. Dies ermöglicht verschiedene Ressourcen zu einem gemeinsamen Ressourcen-Pool zu konsolidieren. Dabei können nicht nur Server- und Speicherstrukturen zusammengefasst werden, sondern

[2] Vgl.: Baun C., et al.: Cloud Computing, 2011, S. 4
[3] Vgl.: Mell, P., Grance, T.: Definition of Cloud Computing, 2011, S. 2 und Baun C., et al.: Cloud Computing, 2011, S. 5f.

auch ganze Systemlandschaften und Datenbanken. Im Kontext Cloud Computing ist der wichtigste Leitgedanke: „Konsolidierung führt zur Effizienzsteigerung und damit zur Kostensenkung.“ [4] Bei Anforderungen von Nutzern können durch die Virtualisierung dynamisch und schnell angepasste Plattformen erzeugt werden.[5] Weiterhin ist ein großer Vorteil der Virtualisierung, dass die physischen Ressourcen flexibel erweitert werden können, ohne die virtuellen Maschinen zu beeinflussen.

2.1.4 Servicemodelle

Im Cloud Computing werden drei unterschiedliche Servicemodelle unterschieden. Je nach Art der Dienstleistung, welche die Kunden verwenden möchten, können sie das passende Modell wählen.

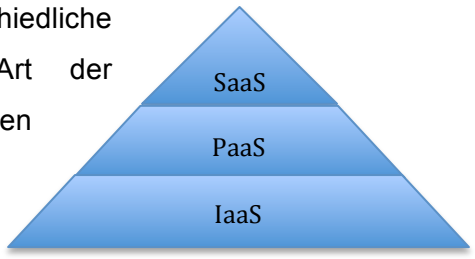

Abbildung 1: SaaS-, PaaS-, IaaS Modell

Unterschieden werden die Servicemodelle *Infrastructure as a Service (IaaS), Platform as a Service (PaaS)* und *Software as a Service (SaaS)*, die wie folgt definiert werden:

Das Modell *Infrastructure as a Service* beschreibt das Bereitstellen von Server- und Datenspeicherressourcen, das heißt der Nutzer kann seine eigenen Ressourcen auf eine effiziente Weise erweitern. So können auf der gemieteten Infrastruktur beliebige Betriebssysteme und Anwendungen installiert werden. Beispiele für das IaaS-Modell sind *Amazon Elastic Compute Cloud (Amazon EC2)*[6] und *Windows Azure*[7].

Dem gegenüber stellt das Modell *Platform as a Service* dem Nutzer Programmierschnittstellen und Entwicklertools auf den Ressourcen des Anbieters bereit. Der Nutzer hat in diesem Servicemodell – anders als beim IaaS-Modell – nicht die Möglichkeit das Betriebssystem oder die Hardware zu verändern, vielmehr liegt hier der Fokus auf der Programmierung von Software. So kann der Nutzer beispielsweise Programme auf der Plattform schreiben, sie dort bereitstellen und austesten. Beispiele für das PaaS-Modell sind *Google App Engine*[8] und *Windows Azure.* Auf der Windows Azure Plattform werden zugleich IaaS und PaaS Dienste angeboten[9].

Beim dritten Modell *Software as a Service* werden Anwendungen als Dienste bereitgestellt. Dabei muss der Anbieter für den reibungslosen Betrieb und die

[4] Baun C., et al.: Cloud Computing, 2011, S. 9f.
[5] Vgl. ebenda
[6] Vgl.: o.V.: Amazon EC2, 2012
[7] Vgl.: o.V.: Windows Azure, o.J.
[8] Vgl.: o.V.: Google App Engine], o.J.
[9] Vgl.: o.V.: Windows Azure, o.J.

Instandhaltung der Hard- und Software sorgen. Bedient wird diese Software meist über eine Web-Plattform.[10] Anwendungsbezogene Beispiele für das SaaS-Modell sind *Google Docs*[11] und *Dropbox*. Dropbox nutzt dabei die Speicherkapazitäten von Amazon S3 (Amazon's Simple Storage Service) welches wiederum ein IaaS-Modell ist.[12]

2.2 Cloud-Infrastrukturen

2.2.1 Public Cloud

Die *Public Cloud* (bzw. External Cloud) bezeichnet eine Cloud-Infrastruktur die für die offene Nutzung der Allgemeinheit ausgelegt ist. Die Anbieter bieten ihre Cloud öffentlich zugänglich an und Nutzer können über ein Webportal ihre Ressourcenumfänge spezifizieren. Im Zuge der dadurch entstandenen vertraglichen Bindung werden dem Nutzer nur die Leistungen für genutzte Ressourcen in Rechnung gestellt. Die Ressourcen befinden sich dabei im Verfügungsbereich des Cloud-Anbieters. [13] Ein Beispiel für eine Public Cloud sind die von Amazon angebotenen *Amazon Web Services*.[14]

2.2.2 Private Cloud

Bei der *Private Cloud* (bzw. Internal Cloud) gehören die Nutzer und Anbieter derselben organisatorischen Einheit an und die Cloud wird mehreren Nutzern der Organisation zur Verfügung gestellt. Im Gegensatz zur Public Cloud bleiben die Daten unter der Kontrolle der Organisation. Die Private Cloud stellt ein virtualisiertes Rechenzentrum in einem Unternehmen dar, welches aufgrund dieser Virtualisierung einfacher separiert werden kann. So können die Ressourcen auf die unterschiedlichen Abteilungen oder Tochtergesellschaften effizient aufgeteilt werden. Dementsprechend kann für unterschiedliche Standorte unternehmensweit immer der gleiche Standard gewährleistet werden. Durch die Sicherheit, dass die Daten im Unternehmen bleiben, sind besonders sensible Daten gut geschützt.[15] Ein Beispiel für eine Private Cloud sind die HP Data Centers.[16]

[10] Vgl.: Mell, P., Grance, T.: Definition of Cloud Computing, 2011, S. 2f.
[11] Vgl.: o.V.: Google Docs, o.J.
[12] Vgl.: o.V.: Dropbox, o.J. und o.V.: Amazon S3, 2012
[13] Vgl.: Baun C., et al.: Cloud Computing, 2011, S. 27f. und Mell, P., Grance, T.: Definition of Cloud Computing, 2011, S. 3
[14] Vgl.: o.V.: Amazon Web Services, 2012
[15] Vgl.: Baun C., et al.: Cloud Computing, 2011, S. 28f. und Mell, P., Grance, T.: Definition of Cloud Computing, 2011, S. 3
[16] Vgl.: o.V.: Data Center and Virtualization und Private Cloud, 2011

2.2.3 Community Cloud

Die *Community Cloud* ist eine gemeinschaftlich genutzte Public Cloud, bei der sich eine Gemeinschaft von Nutzern unterschiedlicher Organisationen die Ressourcen und Kosten der Cloud teilt.[17] Ein Beispiel für eine Community Cloud ist die *Media Community Cloud* von Siemens.[18]

2.2.4 Hybrid Cloud

Die *Hybrid Cloud* vereint die Dienste der Public-, Community- und Private Cloud. Die Dienste der Private Cloud werden auf organisationsinternen Ressourcen betrieben und zudem wird versucht die gleichen technischen Schnittstellen wie in der Public Cloud zu realisieren. Bei Belastungsspitzen eines Unternehmens können so zu den internen Ressourcen beliebig externe Ressourcen hinzugezogen werden.[19] Ein Beispiel für eine Hybrid Cloud ist eine Virtual Private Cloud, die im Kapitel 4.2.3.2 näher erläutert wird.

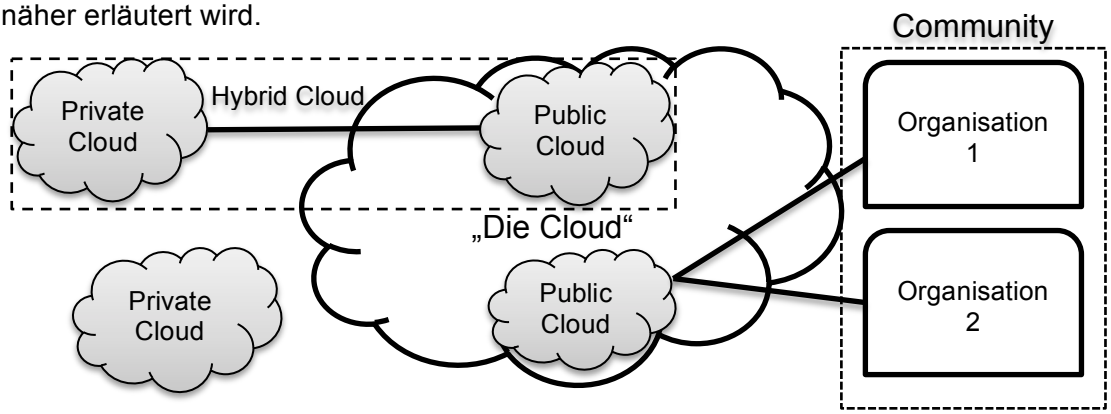

Abbildung 2: Public, Private, Hybrid und Community Cloud[20]

2.3 Datenschutz

Für Cloud-Nutzer ist nicht immer transparent, an welchem Ort oder in welchem Land ihre Daten auf einem Server gespeichert werden. Die unterschiedlichen Rechenzentren eines Cloud-Anbieters werden vernetzt und ermöglichen so die Ressourcen optimal einzusetzen und den Umständen entsprechend anzupassen. Dabei müssen die Rechenzentren nicht zwangsläufig nur in einem Land liegen. Aber das Auslagern von personenbezogenen Cloud-Daten auf einen technisch hochwertigeren Server im Ausland birgt auch seine Risiken. Dazu muss ein deutscher Anbieter bestimmte Auflagen des Bundesdatenschutzgesetzes erfüllen.

[17] Vgl.: Mell, P., Grance, T.: Definition of Cloud Computing, 2011, S. 3
[18] Vgl.: Henneberger, M., Luhn, A.: Community Clouds, 2010, S. 2
[19] Vgl.: Baun C., et al.: Cloud Computing, 2011, S. 28f. und Mell, P., Grance, T.: Definition of Cloud Computing, 2011, S. 3
[20] Eigene Darstellung in Anlehnung an Baun C., et al.: Cloud Computing, 2011, S. 28

Gemäß §4b BDSG ist es entscheidend, ob personenbezogene Daten eines deutschen Anbieters in der EU oder einem Drittland gespeichert werden.[21] Drittländer müssen ein angemessenes Datenschutzniveau vorweisen, erst dann werden sie durch die Europäische Kommission für den Datenaustausch zugelassen. Zusätzlich gibt es zwischen der EU und den Vereinigten Staaten das sogenannte Safe-Harbour-Abkommen, in dem Richtlinien für die Übermittlung von personenbezogenen Daten geregelt werden.[22] Durch die genannten rechtlichen Rahmenbedingungen soll die Datensicherheit im Rahmen des Cloud Computings gewährleistet werden.

Um Vereinbarungen für die Benutzung einer Cloud festzuhalten, wird ein Vertrag in Form eines Service-Level-Agreements zwischen Cloud-Anbieter und -Nutzer abgeschlossen. Der Cloud-Anbieter definiert u.a. den Leistungsumfang, Dienstzeit und Datenschutzaspekte, um bei einem Ausfall eine angemessene Entschädigung für den Nutzer zu garantieren. Der Cloud-Nutzer bekommt somit gleichermaßen einen gewissen Handlungsrahmen vorgegeben.[23]

3 Potentiale und Sicherheiten

3.1 Vorteile von Cloud Computing

Bei der Betrachtung der vorangegangenen Kapitel wird deutlich, dass das Cloud Computing viele Potentiale für deren Nutzer bereithält. Besonders bei einer Public Cloud können sich Unternehmen durch das Nutzen externer Ressourcen auf ihr Kerngeschäft konzentrieren und benötigen keine eigenen kosten- und zeitintensiven Rechenzentren mehr. Auch Privatanwender nutzen häufig eine Public Cloud zur Speicherung ihrer Daten auf die sie so jederzeit von jedem Ort Zugriff haben.
Aber auch die Private Cloud stellt eine effiziente Lösung für ein Unternehmen dar. Sie bietet die Möglichkeit die Ressourcen durch Virtualisierung effizient aufzuteilen und dynamisch zu erweitern.
Nicht zu vergessen ist die Hybrid Cloud. Sie bietet den Unternehmen eine effiziente Lösung zur flexiblen Anpassung an Belastungsspitzen falls Unternehmen kurzfristig zusätzliche Ressourcen benötigen.

[21] Vgl.: Bundesministerium der Justiz: Bundesdatenschutzgesetz, o.J.
[22] Vgl.: o.V.: Amtsblatt, 2000: L 215/7
[23] Vgl.: Jansen, W., Grance, T.: Guidelines, 2011, S. 7f.

Somit lässt sich zusammenfassend sagen, dass die wesentlichen Vorteile der Cloud die große Flexibilität, die Anpassungsfähigkeit, die Kosteneinsparungen und die globale Verfügbarkeit sind.

3.2 Zertifizierungen

Um den potentiellen Cloud-Nutzern eine vertrauenswürdige Basis bei der Auswahl von Cloud-Anbietern zu bieten, können sich diese beispielsweise durch die ISO 27001 zertifizieren lassen und garantieren dadurch ein hohes Maß an Datensicherheit und Datensicherheit. Durch diese Zertifizierung können Cloud-Anbieter auch nachweisen, dass sie hohe Sicherheiten bezüglich Vertraulichkeit und Verfügbarkeit gewährleisten können.[24] Zertifizieren lassen können sich Cloud-Anbieter in Deutschland unter anderem durch den TÜV-Süd.[25] Ein Beispiel für ein solches Zertifikat ist in Abbildung 2 dargestellt.


ZERTIFIKAT

Mustermann GmbH

ISO/IEC 27001:2005

Abbildung 3: Beispiel Zertifikat ISO 27001 TÜV Süd[26]

Neben der ISO 27001 existieren weitere Zertifikate, wie beispielsweise das Gütesiegel für SaaS-Anbieter, welches von der EuroCloud Deutschland_eco e.V. zur Förderung und Akzeptanz von Cloud Computing vergeben wird (EuroCloud Star Audit SaaS Zertifizierung).[27] Hierbei werden speziell SaaS-Modelle in einem Audit auf Datensicherheit und Datenschutz überprüft und zertifiziert.

4 Gefahren und Lösungen

Trotz aller Vorzüge des Cloud Computing soll in dieser Seminararbeit auch auf die Gefahren hingewiesen und mögliche Lösungsansätze aufgezeigt werden. Denn bei der Speicherung der Daten im Internet besteht immer die Gefahr, dass die Daten von Unbefugten mitgelesen oder kopiert werden können. Dadurch ergibt sich die Notwendigkeiten nach Möglichkeiten Ausschau zu halten, die die Cloud bietet, um die Daten sicher zu übertragen und zu speichern.

[24] Vgl.: BSI: Eckpunktepapier, 2012, S. 25
[25] Vgl.: TÜV Süd: ISO 27001, o.J.
[26] Vgl.: TÜV Süd: ISO/IEC 27001, o.J., S. 7
[27] Vgl.: o.V.: EuroCloud, 2012

4.1 Verfügbarkeit

4.1.1 Verfügbarkeit gewährleisten

Beim Cloud Computing ist die Verfügbarkeit des Cloud-Anbieters äußerst wichtig, da die Daten in der Cloud nicht mehr zugänglich wären, sobald zu den Ressourcen des Cloud-Anbieters keine Verbindung mehr aufgebaut werden kann.

Unter Verfügbarkeit (engl.: availability) versteht man den unterbrechungsfreien Zugriff von Nutzern auf ihre Daten und Dienste in IT-Netzwerken, IT-Systemen und IT-Anwendungen.[28]

Der Cloud-Nutzer ist abhängig von einer dauerhaften Verbindung zum Anbieter. Diese Abhängigkeit ist ein großes Risiko, denn im Falle eines Ausfalls ist auch der Cloud-Nutzer ggf. nicht mehr in der Lage seinen Kunden gegenüber die vertraglich geregelten Dienstleistungen anzubieten. Eine Lösung dafür wäre das redundante Speichern der Daten auf verschiedenen Cloud-Plattformen unterschiedlicher Cloud-Anbieter. So würden die Daten mit einer höheren Wahrscheinlichkeit verfügbar bleiben. Dieses Vorgehen erhöht natürlich die Kosten, wobei man in diesem Zusammenhang die Sicherheit gegenüber den Kosten abwägen sollte.

Ein Cloud-Anbieter kann die Verfügbarkeit dadurch erhöhen, dass die Nutzerdaten auf mehreren Servern redundant gespeichert werden. Dadurch wird der Ausfall eines Servers durch einen anderen kompensiert. Gleichermaßen besitzt ein Cloud-Rechenzentrum meist mehrere Datenleitungen und eine Notstromversorgung, welche eine unterbrechungsfreie Stromversorgung darstellt.[29]

In einem Bericht der *International Working Group on Cloud Computing Resiliency* über Cloud Computing Verfügbarkeit wird von einer durchschnittlichen Nichtverfügbarkeit der Cloud Anbietern von 7,5 Stunden im Jahr gesprochen. Dies entspricht in einer Umrechnung: 1-(7,5/(24*365)) = 99,91% Verfügbarkeit. Laut diesem Bericht wir von geschäftskritischen Systemen jedoch eine Verfügbarkeit von 99,999% erwartet. Dabei wird bei Unternehmen wie Google, Microsoft oder Amazon schätzungsweise ein Verlust von ca. 200.000€ pro Stunde eingefahren.[30]

Amazon gibt an, dass ihr Amazon Simple Storage Service (Amazon S3) eine Verfügbarkeit von 99,99% besitzt.[31] In einem Rechenbeispiel mit 24 Stunden * 365 Tage ergeben sich: (24*365)*(1-0,9999) = 0,876 Std/Jahr Ausfallzeit.

[28] Vgl.: BSI: Glossar und Begriffsdefinitionen, 2009, Verfügbarkeit
[29] Vgl.: BSI: Eckpunktepapier, 2012, S. 28 und Müller, M.: Cloud Computing, 2008, S.2
[30] Vgl.: Gagnaire, M. et al.: Downtime statistics, 2012
[31] Vgl.: o.V.: Amazon S3, 2012

Hingegen gibt Windows Azure eine Verfügbarkeit von 99,95%[32] an:
(24*365)*(1-0,9995) = 4,38 Std/Jahr Ausfallzeit. Letztlich liegen beide Werte über der angegebenen Branchen-Durchschnitts-Verfügbarkeit und stellen damit für den Nutzer sichere Systeme dar.

4.1.2 Angriff auf die Verfügbarkeit

Ein Beispiel für ein Vorgehen von Angreifern die Verfügbarkeit eines Rechenzentrums außer Kraft zu setzen ist das Bündeln von mehreren Rechnern zu einem sogenannten Botnetz. Ein Botnetz ist ein Verbund von Computern, die durch eine Schadsoftware infiziert wurden und über einen zentralen Server kontrolliert und ferngesteuert werden können. Durch den Verbund von mehreren tausend Computern kann der zentrale Server gleichzeitig mehrere Anfragen lossenden lassen, um beispielsweise einen Service Anbieter zu attackieren. Bei einer so großen Menge von Anfragen werden die meisten Anbieter überlastet und es kommt zu einem sogenannten Denial of Service.[33]
Ein Denial of Service ist das Überlasten einer IT-Infrastruktur, welches dazu führt, dass viele oder alle Dienste eines Anbieters für einen bestimmten Zeitraum nicht mehr verfügbar sind. Dabei bieten Cloud Plattformen ideale Voraussetzungen für einen solchen verteilten Denial of Service Angriff.[34]
In einem Bericht über einen gelungenen Denial of Service Angriff durch eine Cloud-Infrastruktur wird aufgezeigt, wie einfach es ist einen solchen Angriff auszuführen, wenn nur schlechte Sicherheitsmechanismen verwendet werden.
Kurz zusammengefasst: Zwei Sicherheitsexperten haben für einen Test einen Angriff mit Hilfe einer angemieteten Cloud-Infrastruktur auf einen ihrer Kunden durchgeführt. Dabei wurde eine Software in der Cloud installiert, die einen Denial of Service Angriff auf ihren Kunden durchgeführt hat. Dieser Angriff war erfolgreich, weil keine Bandbreitenbeschränkung und Erkennungsmaßnahmen installiert waren. Der ausführliche Bericht ist im Quellenverweis zu finden.[35]
Solche Angriffe können aber auch auf den Cloud-Anbieter selbst, auf einzelne Nutzer oder zwischen Nutzern durchgeführt werden.

[32] Vgl.: o.V.: Windows Azure, o.J.
[33] Vgl.: Eckert, C.: IT-Sicherheit, 2012, S. 72f.
[34] Vgl.: Jansen, W., Grance, T.: Guidelines, 2011, S. 33
[35] Vgl.: Rei: Donnerschlag aus der Cloud, 2012

4.2 Datensicherheit

Wenn Cloud-Nutzer ihre Daten in die Cloud auslagern, liegt ihr größtes Augenmerk auf der Unversehrtheit ihrer Daten (Integrität). Besonders Unternehmen, die sensible Unternehmensdaten auslagern, möchten einen zuverlässigen Schutz ihrer Daten vor dem Zugriff Unbefugter gewährleistet haben (Vertraulichkeit). Im Folgenden werden Risiken und entsprechende Lösungsmöglichkeiten bei der Übertragung von Daten, der Trennung von Mandanten und der Speicherung der Daten in der Cloud erläutert.

4.2.1 Übertragung

4.2.1.1 VPN und verschlüsselte Übertragungsprotokolle

Die Übertragung der Daten vom Cloud-Nutzer zum Cloud-Anbieter sollte immer gesichert durch eine verschlüsselte Datenübertragung erfolgen. Dabei empfiehlt sich der Einsatz von Übertragungsprotokollen wie SSL/TLS, SSH und/oder IPSec. Darauf aufbauend ist zur Tunnelübertragung ein Virtual Private Network (VPN) einzusetzen. Durch eine solche VPN-Verbindung und die verschlüsselten Übertragungsprotokolle wird die Integrität der Daten bei der sicheren Übertragung gewährleistet und ist vor dem Mitlesen oder der Manipulation Unbefugter geschützt.[36]

4.2.1.2 Integrität

Die Integrität (engl.: integrity) ist die Korrektheit (Unversehrtheit) der Daten. Das bedeutet im Fall der Übertragung, dass die Daten bidirektional vom Cloud-Nutzer zum Cloud-Anbieter vollständig und unverändert übertragen worden sein müssen. Neben dem Inhalt werden auch die Attribute der Daten auf Manipulation überprüft. Beispielsweise ist zu untersuchen, ob die Angaben über den Verfasser oder der Titel der Datei beim Transport verändert wurden.[37] Sichergestellt werden kann die Integrität beispielsweise durch eine Prüfsumme an jedem Datensatz, die mit der Originalprüfsumme verglichen wird. Die Originalprüfsumme sollte dabei verschlüsselt an einem sicheren Ort gespeichert werden.

4.2.1.3 Sicherheit durch Firewalls

Ein weiterer Aspekt zur Sicherheit bei der Übertragung von Daten ist auf Seiten des Nutzers und des Anbieters Firewalls einzurichten, um den Datenverkehr zu filtern. Diese bieten die grundlegende Sicherheit, dass nur bekannte Protokolle und Ports benutzt werden dürfen. Der Anbieter sichert seine Cloud-Umgebung mit Firewalls ab,

[36] Vgl.: Weber, M.: Cloud Computing, 2010, S. 76
[37] Vgl.: BSI: Glossar und Begriffsdefinitionen, 2009, Integrität

aber für die Einrichtung einer Firewall auf Seiten des Nutzers ist dieser selbst zuständig.

4.2.1.4 Homomorphe Verschlüsselung

Neben allen Sicherheitsmechanismen, die eine Cloud zu bieten hat, ist der sicherste Weg in die Cloud die Daten vom Nutzer durch einen sicheren Verschlüsselungsalgorithmus zu kodieren und erst anschließend in die Cloud zu senden. Neben vielen Verschlüsselungsalgorithmen stellt beispielsweise die homomorphe Verschlüsselung einen Algorithmus zum Rechnen auf den Daten in der Cloud dar. Der Nutzer kann verschlüsselte Daten in die Cloud schicken, dort rechnet der Cloud-Anbieter auf den Daten mit Hilfe von Addieren oder Multiplizieren und beim Zurücksenden der Daten aus der Cloud, kann nur der Nutzer die Daten wieder entschlüsseln. Bei diesem Verfahren hat der Anbieter zu keinem Zeitpunkt Kenntnis vom verwendeten Schlüssel, kann aber trotzdem auf den verschlüsselten Daten arbeiten.

Ein simples Beispiel: Der Verkäufer Jan hat den Schlüssel $\mathrm{k} = 2$ gewählt. Die Verschlüsselung seiner Daten erfolgt durch die Funktion: $\mathrm{E(m)} = \mathrm{m} \cdot \mathrm{k}$ mit m als die zu verschlüsselnden Daten. Die Entschlüsselung erfolgt über die Funktion: $\mathrm{D(c)} = \frac{c}{k}$ mit c als die zu entschlüsselnden Daten. Wenn Jan nun täglich die Anzahl seiner verkauften Brötchen: m = 1 über die Verschlüsselung $\mathrm{E}(1) = 1 \cdot 2 = 2$ in die Cloud schickt, dann entsteht nach 5 Tagen in der Cloud die Summe:
$2 + 2 + 2 + 2 + 2 = 10$. Möchte Jan nun wissen, wie viel er verkauft hat, bekommt er aus der Cloud die Summe 10 und berechnet daraus durch
$\mathrm{D}(10) = \frac{10}{2} = 5$ Brötchen. Der Algorithmus ist im Beispiel stark vereinfacht und es sind auch keine weiteren Operationen neben Addition und Multiplikation über die homomorphe Verschlüsselung möglich, jedoch bietet sie eine gute Basis für mehr Sicherheit von persönlichen Daten in der Cloud.[38] Wenn in der Cloud nicht auf den Daten gerechnet werden muss, kann der Nutzer auch einen anderen gängigen Verschlüsselungsalgorithmus verwenden, um so seine Daten vor Unbefugten zu schützen.

[38] Vgl.: Tom S. et al.: Datenwolke, 2011

4.2.2 Mandantentrennung - Vertraulichkeit

Sobald die Daten in der Cloud sind, ist es auf Seiten des Cloud-Anbieters sehr wichtig die Daten der einzelnen Nutzer bei der Speicherung strickt voneinander zu trennen. Dazu muss auf den Cloud-Plattformen eine Mandantentrennung (Multi-tenant) vorgenommen werden, um die Vertraulichkeit der Daten zu gewährleisten.
Die Vertraulichkeit (engl.: confidentiality) ist der Schutz der Daten vor dem Zugriff Unbefugter.[39] Die Mandantentrennung kann dadurch realisiert werden, dass jedem Cloud-Nutzer eine eigene virtuelle Maschine zugeteilt wird. So werden die Daten jedes Mandanten vor der unbefugten Nutzung eines anderen Mandanten geschützt.

4.2.3 Virtualisierung

4.2.3.1 Hypervisor

Die Server-Virtualisierung wird durch einen sogenannten Hypervisor bzw. Virtual Maschine Monitor (VMM) realisiert. Der Hypervisor ist eine Virtualisierungssoftware, die zwischen dem Betriebssystem und der Hardware-Plattform integriert wird. Durch ihn können mehrere virtuelle Maschinen parallel betrieben werden und er steuert den Zugriff auf die gemeinsam genutzten Ressourcen. Verglichen mit einer nicht-virtualisierten Implementation bildet der Hypervisor eine zusätzliche Angriffsfläche für Angreifer.[40] Durch Manipulation von CPU-Registern, die für die Virtualisierung zuständig sind, kann ein Angriff auf den Hypervisor durchgeführt werden.[41] Um ein Beispiel zu nennen, wie ein Hypervisor geschützt werden kann, ist von IBM ein Kontrollmechanismus entwickelt worden, der sHype genannt wird. Er kontrolliert jeden Informationsfluss zwischen und jeden Zugriff auf virtuelle Maschinen, um mögliche Schadsoftware erkennen zu können.[42]

4.2.3.2 Virtual Private Cloud (VPC)

Eine interessante Lösung zum Schutz der Daten durch Virtualisierung bietet die Virtual Private Cloud, die eine Private Cloud innerhalb einer Public Cloud darstellt. Dabei werden externe Ressourcen direkt in die IT-Infrastruktur des Cloud-Nutzers mittels einer gesicherten VPN-Verbindung integriert und bilden so eine Hybrid Cloud.[43] Um sicherzustellen, dass die Daten auch privat bleiben, werden diese entweder schon verschlüsselt in die Cloud gesendet oder es wird eine direkte

[39] Vgl.: BSI: Glossar und Begriffsdefinitionen, 2009, Vertraulichkeit
[40] Vgl.: Jansen, W., Grance, T.: Guidelines, 2011, S. 22
[41] Vgl.: BSI: Eckpunktepapier, 2012, S. 30
[42] Vgl.: Sailer, R. et al.: sHype, 2005, S. 5, Kapitel 2.4
[43] Vgl.: Baun C., et al.: Cloud Computing, 2011, S. 45 sowie Kapitel 2.2.4 dieser Arbeit

Hardware-VPN-Verbindung zwischen der VPC und dem Unternehmen angelegt. Somit hat das Unternehmen einen direkten Zugriff auf die ausgelagerten Unternehmensdaten und kann die Infrastruktur genau wie das interne Netzwerk einrichten.[44]

Der traditionelle Weg über VPN ist durch eine Software-VPN realisiert. In der VPC wird jedoch eine Hardware-VPN verwendet.

Eine Hardware-VPN ist ein Virtuelles Privates Netzwerk, das auf einem einzelnen, alleinstehenden Gerät betrieben wird. Zwei Standorte haben dabei jeweils ein solches Hardware-VPN Gerät, um eine Verbindung aufzubauen. Diese Geräte werden VPN-Router genannt, welche optimierte Prozessoren enthalten, Authentifizierung verwalten und eine starke Verschlüsselung ermöglichen. Zudem ist in den VPN-Routern auch eine Hardware-Firewall integriert. Der große Vorteil einer Hardware-VPN gegenüber einer Software-VPN ist die Lastenverteilung, wodurch Engpässe in einem Netzwerk minimiert werden und die Fähigkeit eine große Anzahl von Klienten-Lasten zu bewältigen, sichergestellt ist. Somit ist es im Hinblick auf die Virtualisierung vorteilhaft mit einer Hardware-VPN eine Verbindung zu einer Virtual Private Cloud aufzubauen.[45]

4.2.3.3 VLAN

Eine sichere Maßnahme um ein physisches Netz in einer Cloud zu unterteilen, ist das Virtual-LAN (VLAN). Dabei können bestimmte Benutzer durch ein VLAN logisch voneinander getrennt werden. In einer Public Cloud kann für einen Nutzer ein einzelnes Netz segmentiert werden, um beispielsweise wiederum ein eigenes Unternetz darin aufzuteilen.[46] Durch die Zugriffsrechte, die jeder VLAN-User benötigt, sind seine Daten vor dem unbefugten Zugriff eines anderen Cloud-Nutzers sicher.

4.2.4 Datenvernichtung

Die Daten eines Nutzers müssen nicht nur sicher gespeichert, sondern auch sicher und zuverlässig von allen Medien des Cloud-Anbieters gelöscht werden, sobald diese Funktion vom User gewählt wird, oder der Vertrag aufgelöst und damit beendet wird. Dabei ist es wichtig, dass neben der aktuellen Sicherung auch alle vorherigen Sicherungen gelöscht werden. Der Zeitpunkt, wann die Daten nach dem Auflösen

[44] Vgl.: o.V.: Amazon VPC, 2012
[45] Vgl.: Rouse, M.: hardware VPN, 2007 und Janssen, C.: Hardware VPN, 2012
[46] Vgl.: Schawohl, E.: Networking, 2005, S.279

eines Service-Vertrages gelöscht werden müssen, wird in dem Service-Level-Agreement (SLA) definiert.[47]

5 Schlussbetrachtung

Cloud Computing bekommt durch die flexiblen Möglichkeiten der unterschiedlichen Servicemodelle IaaS, PaaS und SaaS eine immer größere Bedeutung für Unternehmen und Privatpersonen. Die Potentiale, besonders der Public Cloud, bestehen ohne Frage in der Kosteneinsparung, dadurch dass keine eigenen Ressourcen gekauft und Instand gehalten werden müssen. Ein weiterer Vorteil ist die Flexibilität, die es ermöglicht, dass an jedem Ort auf der Welt auf die Daten zugegriffen werden kann. Dabei lässt Cloud Computing durch die Public und die Private Cloud zusätzlich eine individuelle Gestaltung der Unternehmensressourcen zu.
Trotzdem muss der Cloud-Nutzer insbesondere bei einer Public Cloud besondere Aufmerksamkeit auf die sorgfältige Auswahl eines geeigneten Anbieters legen. Dies ist mit Hilfe verschiedener Sicherheitszertifikate möglich, auf die sich Cloud-Anbieter prüfen lassen können.
Abschließend ist aber auch deutlich geworden, dass Cloud Computing neben den vielfältigen Potentialen, trotzdem einige Gefahren, insbesondere im Bezug auf Verfügbarkeit und Datensicherheit, vermuten lässt. Diese Gefahren machen es notwendig, dass die Cloud-Anbieter hohe Sicherheitsanforderungen einhalten müssen, damit die Daten der Cloud Nutzer vor unbefugten Zugriffen absichert sind.

Im Hinblick auf die Beantwortung der Einleitungsfrage, ob die Cloud ein geeigneter Weg in die Zukunft ist, ist unter Berücksichtigung der erarbeiteten Informationen dieser Seminararbeit, meiner Meinung nach mit Ja zu beantworten.
Die offensichtlichen Vorteile der Cloud überwiegen den Nachteilen bzw. Gefahren, für die bereits Lösungsmöglichkeiten in dieser Arbeit erläutert wurden. Somit ist Cloud Computing eine zukunftssichere und flexible Möglichkeit für moderne IT-Kommunikation.

[47] Vgl.: BSI: Eckpunktepapier, 2012, S. 38

Literaturverzeichnis

Literaturquellen

Baun C., et al., 2011: [Cloud Computing]: Web-basierte dynamische IT-Services, 2. Aufl., Informatik im Fokus, Berlin Heidelberg: Springer, 2011

Eckert, C., 2012: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg-Verlag, München, 7. Auflage, 2012

Schawohl, E., 2005: Cisco [Networking] Academy Program 3. und 4. Semester, Cisco Systems, 3. Aufl., München: Markt+Technik Verlag, 2005

Internetquellen

BSI, 2009: Bundesamt für Sicherheit in der Informationstechnik - BSI: 4 [Glossar und Begriffsdefinitionen], Bonn, 2009, Internet https://www.bsi.bund.de/cln_174/DE/Themen/weitereThemen/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html, Stand 2009, Abruf: 20.09.2012

BSI, 2012: Bundesamt für Sicherheit in der Informationstechnik – BSI: [Eckpunktepapier]: Sicherheitsempfehlungen für Cloud Computing Anbieter, Bonn, 2012, Internet https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf?__blob=publicationFile, Abruf 27.09.2012

Bundesministerium der Justiz, o.J.: [Bundesdatenschutzgesetz], o.O., o.J., Internet http://www.gesetze-im-internet.de/bdsg_1990/__4b.html, Abruf 02.10.2012

Gagnaire, M. et al. 2012: [Downtime statistics] of current cloud solutions, o.O., 2012, Internet http://iwgcr.org/wp-content/uploads/2012/06/IWGCR-Paris.Ranking-002-en.pdf, Abruf 09.12.2012

Henneberger, M., Luhn, A., 2010: [Community Clouds] – Unterstützung von geschäftlichen Ökosystemen mit Cloud Computing, o.O, 2010, PDF

Jansen, W., Grance, T., 2011: [Guidelines] on Security and Privacy in Public Cloud Computing, National Institut of Standards and Technology, Gaithersburg, 2011, Internet http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494, Abruf 27.09.2012

Janssen, C., 2012: Hardware Virtual Private Network ([Hardware VPN]), o.O., 2012, Internet http://www.techopedia.com/definition/15237/hardware-virtual-private-network-hardwarevpn, Abruf: 13.12.2012

Mell, P., Grance, T., 2011: The NIST [Definition of Cloud Computing], National Institut of Standards and Technology, Gaithersburg, 2011, Internet http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, Abruf: 24.09.2012

Müller, M., 2008: Risiken beim [Cloud Computing], Wismar, 2008, Internet http://www.wi.hs-wismar.de/~laemmel/Lehre/WA/Artikel1006/mueller_Cloud.pdf, Abruf 01.10.2012

o.V., 2000: [Amtsblatt] der Europäischen Gemeinschaft, Aktenzeichen: K(2000) 2441, o.O., 2000, Internet http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:DE:PDF, Abruf 02.10.2012

o.V., 2011: HP: [Data Center and Virtualization und Private Cloud], o.O., 2011, Internet http://www8.hp.com/de/de/services/services-detail.html?compURI=tcm:144-807123, Abruf: 09.10.2012

o.V., 2012: Amazon Elastic Compute Cloud ([Amazon EC2]), o.O., 2012, Internet http://aws.amazon.com/de/ec2/, Abruf: 08.10.2012

o.V., 2012: Amazon Simple Storage Service ([Amazon S3]), o.O., 2012, Internet http://aws.amazon.com/de/s3/#functionality, Abruf: 08.10.2012

o.V., 2012: [Amazon VPC], o.O., 2012, Internet http://aws.amazon.com/de/vpc/, Abruf 21.11.2012

o.V., 2012: [Amazon Web Services], o.O., 2012, Internet http://aws.amazon.com/de/, Abruf 05.12.2012

o.V., 2012: [EuroCloud] Deutschland_eco, o.O.,2012,Internet http://www.eurocloud.de/ueber-uns/ziele/, Abruf 03.10.2012

o.V., o.J.: [Dropbox], Internet https://www.dropbox.com/help/7/en, Abruf: 09.10.2012

o.V., o.J.: [Google App Engine], o.O., o.J., Internet https://cloud.google.com/products/index, Abruf: 09.10.2012

o.V., o.J.: [Google Docs], o.O., o.J., Internet http://www.google.com/docs, Abruf: 09.10.2012

o.V., o.J.: [Windows Azure], o.O., o.J., Internet http://www.windowsazure.com/de-de/home/features/overview/, Abruf: 09.10.2012

Rei, 2012: [Donnerschlag aus der Cloud], o.O., 2012, Internet http://www.heise.de/security/meldung/Donnerschlag-aus-der-Cloud-1051889.html, Abruf: 21.11.2012

Rouse, M., 2007: [hardware VPN], o.O., 2007, Internet http://searchnetworking.techtarget.com/definition/hardware-VPN, Abruf: 13.12.2012

Sailer, R. et al., 2005: [sHype] – Secure Hypervisor Approach to Trusted Virtualized Systems, Yorktown Heights, 2005, Internet http://domino.watson.ibm.com/library/cyberdig.nsf/papers/265C8E3A6F95CA8D85256FA1005CBF0F/$File/rc23511.pdf, Abruf: 04.10.2012

Tom S. et al., 2011: Mehr Sicherheit für die [Datenwolke], o.O., 2011, Internet http://www.heise.de/tr/artikel/Mehr-Sicherheit-fuer-Datenwolken-1324650.html, Abruf 05.12.2012

TÜV Süd, o.J.: [ISO 27001]:2005, o.O., o.J., Internet http://www.tuev-sued.de/management_systeme/it-dienstleistungen/iso_27001_2005, Abruf: 08.10.2012

TÜV Süd, 2010: [ISO/IEC 27001]: Transparenz und Sicherheit mit System, o.O., 2010, Internet http://www.tuev-sued.de/uploads/images/1283848593494581250607/pi_9_isoiec27001_d0710.pdf, Abruf: 08.10.2012

Weber, M., 2010: BITKOM: [Cloud Computing] – Was Entscheider wissen müssen, Berlin, 2010, Internet http://www.bitkom.org/files/documents/BITKOM_Leitfaden_Cloud_Computing-Was_Entscheider_wissen_muessen.pdf, Abruf: 27.09.20