der Bundeswehr
Universität München
FAKULTÄT FÜR INFORMATIK

Seminar IT-Sicherheit - Sicherheit und Vertrauen in Cloud Computing

Prof. Dr. Udo Helmbrecht
Michael Kretzschmar
Volker Eiseler
(Hrsg.)

Institut für Technische Informatik

Bericht 2011-01
April 2011

Werner-Heisenberg-Weg 39 • 85577 Neubiberg • Germany

Vorwort

Cloud Computing beschreibt ein neues Computing-Paradigma, nach dem Ressourcen der Informationstechnik (IT) wie Rechenleistung, Speicher, Applikationen und Daten dynamisch über das Internet bereitgestellt, verwaltet und abgerechnet werden. Der Wechsel zu diesem Paradigma einer effizienteren Ressourcen-Nutzung und Kommerzialisierung ermöglicht eine stärkere Industrialisierung der IT. Die Entwicklung geht weg von einschränkenden IT-Infrastrukturen der Unternehmen und Konsumenten hin zur dynamischen Nutzung von IT-Ressourcen „aus der Wolke“. IT-Leistungen werden in Echtzeit als Dienst über das Internet bereitgestellt. Dieser dynamische Ansatz hilft dabei, erhebliche Effektivitätsvorteile und Qualitätsverbesserungen zu erzielen und Lösungen für neue Herausforderungen zu finden. Unternehmen können vor allem deutlich flexibler reagieren, wenn es darum geht, welche IT-Leistungen sie wann und wo benötigen.

Ein Schwerpunkt im Seminar liegt auf der Sicherheit und dem Vertrauen im Cloud Computing. Vor allem kleinere Anwenderunternehmen, die nicht selbst aus dem IT-Bereich kommen, haben noch Hemmschwellen, Software oder Hardware in der „Wolke“ des Internets zu nutzen. Sie fragen sich, welchen Angeboten sie vertrauen und wohin sie Daten oder deren Verarbeitung sicher auslagern können. Ein kaum überschaubares Angebot, ständige Neuerungen, ungenügende Standardisierung und komplizierte Geschäftsmodelle erschweren oftmals die Entscheidungsfindung. Weiterhin gibt es zahlreiche rechtliche Herausforderungen. Hierzu zählen Haftungsfragen und vertragsrechtliche Aspekte genauso wie die rechtliche Gewährleistung des Datenschutzes.

Wir wünschen eine interessante und aufschlußreiche Lektüre

Udo Helmbrecht und Michael Kretzschmar

Inhaltsverzeichnis

Kapitel 1

Entwicklung und Abgrenzung des Cloud Computing

Arthur Deobald

Das Thema Cloud Computing ist zurzeit weit verbreitet und zählt zu den Top-Themen in der IT-Branche. Doch was verbirgt sich hinter dem Begriff Cloud Computing? Und wo kommt dieser neue Trend eigentlich her? In Abhängigkeit davon, wem die Fragen gestellt werden, gehen die Antworten in die eine oder andere Richtung. In dieser Arbeit wird zum einen die Frage geklärt, aus welchen historischen Etappen sich Cloud Computing letztendlich entwickelt hat und was an Cloud Computing eigenlich neu sei. Zum anderen werden die wesentlichen Begriffe und Konzepte, die das Cloud Computing mit sich bringt, erläutert und anschaulich dargestellt.

Inhaltsverzeichnis

1.1 Einleitung

Der Begriff Cloud Computing ist zurzeit eines der Top-Themen im IT-Bereich. Dieses neue Konzept ermöglicht es, IT-Ressourcen nach Bedarf von einem Provider zu beziehen und somit Kosten im Bereich der IT deutlich zu reduzieren. Die Idee, IT-Ressourcen von einem Anbieter zu beziehen statt diese zu kaufen, ist nicht neu. Wie diese Arbeit unter anderem zeigen wird, gab es bereits vor Cloud Computing ähnliche Ideen und Konzepte, um dies zu verwirklichen.
Es steht jedoch fest, dass Cloud Computing auch eigene Techniken und Architekturen mit sich bringt, die ein breites Angebot von IT-Diensten ermöglichen. So können die Bedürfnisse von fast allen Zielgruppen, im Bereich der IT, nach Bedarf und relativ kostengünstig befriedigt werden. Dabei geht es nicht nur um Rechenleistung oder Speicher, wie es in der Vergangenheit oft der Fall war, sondern auch um andere IT-Ressourcen, die ständig benötigt wurden und so eine Menge von Kosten verursachten.
Um Cloud Computing für seine IT-Bedürfnisse einzusetzen, müssen sich die potenziellen Nutzer erstmal mit dem Thema genau auseinander setzten. Es müssen vor allem Hintergründe, Vorgehensweisen und Sicherheitsaspekte für die jeweilige Zielgruppe geklärt und erläutert werden.
In dieser Arbeit wird das Cloud Computing zum einen aus historischen Etappen hergeleitet, zum anderen zu den wesentlichen Begriffen abgegrenzt und schließlich aus technischer und organisatorischer Sicht dargestellt[7].

1.2 Historische Herleitung aus den Etappen

Die Technologie beziehungsweise die Organisation, die hinter Cloud Computing steht, ist nicht von Heute auf Morgen entstanden, sondern unterlag einem langen Entwicklungsprozess. Dabei kann man die Entwicklung aus zwei verschiedenen Strängen historisch herleiten (siehe Abbildung 1.1). Erstens aus der Sicht der technologischen Entwicklung, angefangen bei Supercomputern, über zu Cluster, bis hin zu Grids. Und zweitens aus der Sicht der Serviceorientierung, deren Anfänge man in Utility Computing, später Service Bureaus und schließlich Application Service Providers sehen kann. Anschließend wird geklärt, welche Neuerungen Cloud Computing mit sich bringt.

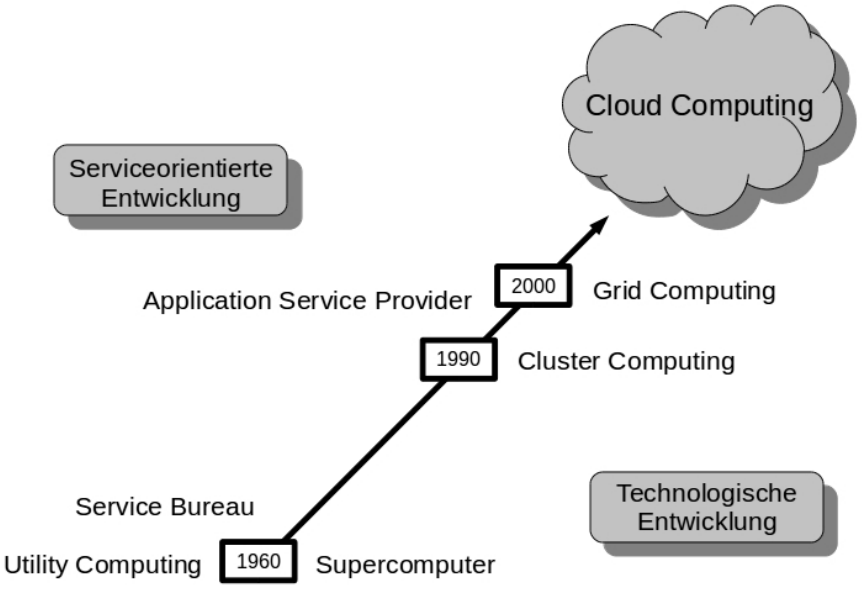

Abbildung 1.1: Historische Entwicklung von Cloud Computing

1.2.1 Technologische Sicht

Die historische Entwicklung des Cloud Computing könnte man selbstverständlich mit den Anfängen des Rechnens beginnen, da wahrscheinlich dort alle mathematischen oder computerwissenschaftlichen Themen ihre Wurzeln haben. Doch das würde den Rahmen dieser Arbeit sprengen. Bei der historischen Herleitung aus der technologischen Sicht werden Etappen aufgezeigt, die für das Cloud Computing eine wichtige Rolle spielen und somit das Fundament der technologischen Seite des Cloud Computing bilden.

1.2.1.1 Supercomputer

Die erste Historische Etappe, die für die Entwicklung von Cloud Computing einen Grundbaustein darstellt, ist das parallele Rechnen, das durch die Entwicklung von Supercomputern realisiert wurde. Die ersten Rechner mit der Fähigkeit parallel zu Arbeiten wurden in

den 1960er Jahren entwickelt. In dieser Zeit entstand auch der Begriff Supercomputer und bezeichnete die schnellsten und leistungsfähigsten Rechnersysteme ihrer Zeit. Der erste erfolgreiche Supercomputer, der 1964 bei der Firma Control Data Corporation (CDC) von Seymore Cray entwickelt wurde, war der CDC 6600. Mit solch einer Technologie war es nun möglich, die Entwicklung der Supercomputer immer schneller voranzutreiben. Seit den 1960er Jahren ist die Höchstleistung der Supercomputer ständig angestiegen und bewegt sich heute im Bereich von 2-3 Peta-Flops. Dabei entspricht 1 Flop einer Gleitkommaoperation pro Sekunde[1, 15].
Aus der heutigen Sicht sind Supercomputer spezielle Rechner, die auf extrem hohe Verarbeitungsleistung ausgerichtet sind. Um möglichst hohe Verarbeitungsleistung zu erreichen, werden sie, im Hinblick auf ihre Architektur, für bestimmte Anwendungen optimiert. Bei Supercomputern handelt es sich um parallelverarbeitende Systeme, Multiprozessorsysteme, Vektorrechner oder MIMD- und SIMD-Architekturen. Die Prozessoren solcher Systeme bilden eine Art Array, auf dem die Aufgaben verteilt und abgearbeitet werden. Diese Arrays können aus mehreren tausend Prozessoren bestehen. Die Leistung solcher Supercomputer wird in Tera-Flops oder zur heutiger Zeit, wie schon oben vorgegriffen, in Peta-Flops angegeben. Dabei entspricht 1 Peta-Flop 10^{15} Gleitkommaoperationen pro Sekunde. Zum heutigen Zeitpunkt (Februar 2011) ist der weltweit schnellste Supercomputer der Tianhe-1A von Nation Supercomputing Center in Tianjin (China). Er erzielt eine Rechenleistung von 2,566 Peta-Flops[16]. Im Vergleich dazu erzielte der CDC 6600, und somit auch der erste Supercomputer, eine Rechenleistung von gerade mal 3 MegaFlops[17]. Da Supercomputer für umfangreiche Probleme eingesetzt werden, die in kürzester Zeit gelöst werden müssen, ist die Geschwindigkeit von solchen Rechnern von großer Bedeutung. Ein Beispiel dafür ist der Einsatz eines Supercomputers für die Wettervorhersage. Es wäre durchaus möglich die Wettervorhersage mit der großen Menge an vorhandenen Daten auch auf einen weniger leistungsstarken Rechner zu berechnen. Doch das würde eine lange Zeit dauern und somit der Wettervorhersage ihren Sinn nehmen. Übertrieben gesehen würde es niemandem nützen, die Wettervorhersage für Morgen erst in einem Monat ausgewertet zu haben. Weitere Beispiele für den Einsatz von Supercomputern sind Berechnungen für die Weltraumforschung, die Klimaforschung oder die Festkörperphysik[18].

1.2.1.2 Cluster

Mit Supercomputer war es nun möglich rechenintensive Aufgaben auszuführen, jedoch muss immer noch so ein Supercomputer dem Unternehmen oder der Institution zur Verfügung stehen. Hat man ihn nicht, kann man die Aufgaben nicht durchführen. Der logisch nächste Entwicklungsschritt in Richtung Cloud Computing müsste nun sein, nicht mehr die Berechnung mit Hilfe eines Supercomputers auszuführen, sondern eine Alternative zu finden, mit der es ebenfalls möglich wäre rechenintisive Aufgaben auszuführen. Das 1990 entstandene Konzept, das sogenannte Cluster Computing, war so ein Entwicklungsschritt. Die Idee dabei war es, mehrere Rechner irgendwie zu bündeln, um mehr Rechenleistung zu erhalten. Damit könnte man rechenintensive Aufgaben ausführen, ohne dabei unbedingt einen Supercomputer benutzen zu müssen. Ein Cluster ist eine Gruppe von miteinander vernetzten eigenständigen Computern, die die Knoten des Clusters bilden und sich wie ein einheitlicher Uniprozessor verhalten. Diese eigenständigen Computer sind in der Regel entweder einfache handelsübliche PCs oder Workstations. Es können aber auch Ser-

ver oder Supercomputer als Knoten eines Clusters eigesetzt werden. Da bei Ausfall von Komponenten diese schnell und in der Regel günstig ersetzt werden können, weil es sich meistens um Standardkomponenten handelt, sind solche Cluster Systeme günstiger als Großrechner und können nach Bedarf vergrößert oder verkleinert werden. Jedoch wird beim Vergrößern solcher Systeme auch der Administrationsaufwand deutlich größer und demnach steigen die dabei entstandenen Kosten.
Für die technische Realisierung eines Cluster Systems spielt die Anzahl der Knoten eine bedeutende Rolle, da die Knoten über ein Netzwerk miteinander verbunden werden. Besteht so ein Cluster System aus nur wenigen Knoten, kann Fast- oder Giga-Ethernet verwendet werden. Bei größeren Clustern, die aus mehreren hundert Knoten bestehen, muss ein Hochgeschwindigkeitsnetzwerk verwendet werden. Die Aufstellung der Cluster erfolgt entweder nach dem Konzept Glass-House oder nach dem Konzept Campus-Wide. Bei Glass-House wird der Cluster in einem extra für ihn vorgesehenen Raum oder Server-Schrank aufgestellt. Beim Konzept Campus-Wide dagegen, befinden sich die einzelnen Knoten des Clusters in mehreren Räumen oder sogar Gebäuden eines Unternehmens oder Instituts. Wegen der Entfernung zu den einzelnen Knoten, kann bei Campus-Wide kein Hochgeschwindigkeitsnetzwerk verwendet werden. Deshalb ist die Leistung bei Glass-House deutlich höher.
Cluster können in homogene und heterogene Cluster unterteilt werden. Sind die Hard- und Softwarekomponenten aller Knoten eines Cluster Systems gleich, so spricht man vom homogenen Cluster. Unterscheiden sie sich, spricht man vom heterogenen Cluster. Weiterhin können Cluster nach ihren Einsatzgebieten und Anforderungen unterteilt werden. Dabei unterscheidet man zwischen vier Arten von Clustern: Hochverfügbarkeits-Cluster, High Performance-Cluster, High Throughput-Cluster und Skalierbare-Cluster[2].

- **Hochverfügbarkeits-Cluster**
  Hochverfügbarkeits-Cluster oder High Availability Cluster bieten eine große Ausfallsicherheit und somit auch eine hohe Verfügbarkeit. Um dies zu erreichen, müssen die Knoten und die Hardware redundant ausgelegt werden und eine unterbrechungsfreie Stromversorgung gewährleistet sein. Das bedeutet, dass das System Komponenten enthält, die zum Betrieb nicht notwendig sind, und im Fehlerfall die Arbeit von baugleichen Komponenten übernimmt. Es gibt zwei Arten von Hochverfügbarkeits-Clustern: Active/Passive-Cluster und Active/Active-Cluster. Bei Active/Passive-Cluster ist mindestens ein Knoten des Clusters nicht in Verwendung und übernimmt keine Dienste. Fällt ein Knoten aus, übernimmt dieser Passiv-Knoten dessen Dienste. Bei Active/Active-Cluster hingegen sind alle Knoten in Verwendung. Fällt ein oder mehrere Knoten aus, so übernehmen die noch aktiven Knoten die Anfragen an den ausgefallenen Knoten[2].

- **High Performance-Cluster**
  High Performance-Cluster besteht, wie die meisten Cluster, aus handelsüblichen PCs und hat das Ziel möglichst hohe Rechenleistung zu erreichen. Im Gegensatz zu Großrechnern sind High Performance-Cluster in der Anschaffung wesentlich günstiger und sind bezüglich des Herstellers unabhängig. Die Hardware-Komponenten können bei Ausfall schnell und günstig beschafft werden. Um seine Leistungsfähigkeit zu vergrößern, kann ein High Performance-Cluster schnell erweitert werden. Jedoch ist der Administations- und Wartungsaufwand deutlich größer als bei einem

Großrechner. Meistens werden solche Cluster in Forschungseinrichtungen und in Unternehmen, wie Finanzdienstleistung oder Automobilbau, eingesetzt.
Man kann High Performance-Cluster in zwei Arten unterteilen: Beowulf und Wolfpack. Bei Beowulf kommen immer OpenSource-Betriebssysteme, wie Linux, BSD- oder andere UNIX-Derivate, zum Einsatz. Wolfpack hingegen verwendet kein Open-Source, sondern Betriebssysteme wie Windows[2].

- **High Throughput-Cluster**
  Beim High Throughput-Cluster wird versucht den Datendurchsatz zu maximieren. Wo beim High Performance-Cluster versucht wird ein umfangreiches Problem schnell zu berechnen, ist beim High Throughput das Ziel möglichst viele Jobs auf einem Cluster in einer bestimmten Zeit zu bewältigen. Bei den Jobs handelt es sich um Aufträge, die normalerweise auf einem gewöhnlichen PC bewältigt werden können. Ein Beispiel für High Throughput-Cluster wären Web- oder Mail-Server[2].

- **Skalierbare-Cluster**
  Skalierbare-Cluster sind eine Art Kompromiss zwischen High Performance und Hochverfügbarkeit. Das heißt, dass einige oder alle Knoten eines solchen skalierbaren Clusters redundant ausgelegt sind und dass alle Knoten Aufträge von einem Lastverteiler zugewiesen bekommen. Dabei überwachen die Knoten des Clusters sich gegenseitig, damit, im Falle eines Ausfalls, ein aktiver Knoten die Dienste des ausgefallenen Knotens übernehmen könnte[2].

1.2.1.3 Grid Computing

Das Konzept von Cluster Computing erlaubt rechenintensive Aufgaben mit Hilfe von handelsüblichen Computern, die miteinander vernetzt sind, auszuführen. Doch wenn man so eine Menge von Rechnern nicht hat, ist auch die Berechnung nicht möglich. Die nächste Etappe, die es möglich macht und uns somit einen Schritt weiter in Richtung Cloud Computing bringt, ist das im Jahr 2000 aufgestellte Konzept des Grid Computing. Die Idee von Grid Computing wird schon mit dessen Bezeichnung verdeutlicht. Der Begriff Grid Computing leitet sich aus dem Englischen *grid* (deutsch: Stromnetz) und *to compute* (deutsch: rechnen) ab. Das bedeutet, dass Grid Computing es uns ermöglichen soll, Rechenleistung wie Strom aus der Steckdose, oder in unserem Fall Netzwerkdose, zu beziehen. Dabei sollen die Nutzer die benötigten Ressourcen genau so einfach wie Strom beziehen können. Zum einen heißt das, dass die Ressourcen über eine standardisierte Verbindung bezogen werden und zum anderen soll der Nutzer nicht genau wissen wo diese Ressourcen herkommen.
Bei der praktischen Umsetzung dieses Konzepts handelt es sich bei Grid Computing um eine Infrastruktur zur gemeinschaftlichen Nutzung von Ressourcen. Diese Ressourcen sind meist geographisch auseinander liegend und können unterschiedlichen administrativen Domänen angehören. Institutionen und Individuen, die sich zur Nutzung ihrer Ressourcen zusammenschließen, bilden eine sogenannte *Virtuelle Organisation* (VO). Im Gegensatz zu Cluster Computing können bei einem Grid neben der Rechenleistung auch andere Ressourcen, wie Daten, Applikationen und sogar wissenschaftliche Geräte, die sich an anderen Orten befinden, gemeinsam genutzt werden[4].

Grids werden in der Regel in fünf Grid-Arten unterteilt: Compute Grid, Data Grid, Application Grid, Resource Grid und Service Grid. Dabei erfolgt die Unterteilung nach der Art, wie der jeweilige Grid genutzt wird. Oder anders ausgedrückt, für welchen Zweck dieser gebraucht wird.

- **Compute Grid**
  Ein Compute Grid wird genutzt, wenn ein Anwender Rechenleistung oder Rechenkapazität benötigt, diese ihm jedoch in seiner eigenen Umgebung nicht zur Verfügung steht. Diese Rechenleistung wird ihm verteilt bereitgestellt. Dabei kann es sich um die Nutzung von nicht verwendeten Ressourcen, wie Arbeitsplatzrechner außerhalb der üblichen Arbeitszeiten, handeln oder das Lösen von Extremproblemen auf zusammengeschalteten Rechenanlagen[5].

- **Data Grid**
  Beim Data Grid wird eine große Datenmenge gemeinsam genutzt und verarbeitet. Die Nutzung des Data Grids ist insbesondere für die Nutzer von Vorteil, die die gleichen Daten benötigen, sich jedoch an verschiedenen Orten befinden. Dabei wird eine Data-Federation gebildet, die eine gemeinsame, organisations- und ortsübergreifende Sicht auf die entsprechenden Daten ermöglicht. So können zum Beispiel Daten die zu einem Projekt gehören, gemeinsam und vor allem ortsunabhängig eingesehen werden. Beim Data Grid behält derjenige, der die Daten zur Verfügung stellt, auch die volle Kontrolle über diese[5].

- **Application Grid**
  Der Application Grid kann als der erste Schritt oder der erste Ansatz der virtuellen Organisation betrachtet werden, da man nicht mehr einer einzigen Organisation oder Sicherheitsdomäne angehören muss, um einen Grid gemeinsam nutzen zu können. Das Ziel des Application Grids ist Ressourcen gemeinsam und vor allem organisationsübergreifend zu nutzen. Damit wird erreicht, dass der Anbieter eine bessere Auslastung und der Nutzer ein breiteres Angebot haben[5].

- **Resource Grid**
  Beim Resource Grid wird zwischen einem Grid-Nutzer, Grid-Provider und Resource-Provider unterschieden. Der Grid-Nutzer greift bei diesem Modell auf die Infrastruktur des Grid-Providers zu und nutzt Ressourcen, die vom Resource-Provider dort angeboten werden. Im Gegensatz zum Application Grid, bei dem alle Komponenten individuell integriert werden können, muss beim Resource Grid der Resource-Provider dafür sorgen, dass sein Angebot die erforderlichen Spezifikationen für die Grid-Umgebung des Grid-Providers erfüllt[5].

- **Service Grid**
  Ein Service Grid ist eine Kombination aus der Technik des Resource Grids und dem Konzept des nutzerorientierten Services. Dabei besteht ein Service aus mehreren Komponenten, die von mehreren Resource-Providern bereit gestellt werden. Jede Komponente eines Services kann von jeweils einem anderen Resource-Provider in Form eines Utility bereit gestellt werden. Beim Service Grid stehen Grid-Nutzer und Resource-Provider nicht mehr direkt gegenüber, sondern überlassen die Verantwortung für den gesamten Nutzerservice einem Grid-Service-Provider. Im Einzelnen be-

deutet das, dass der Grid-Service-Provider den Resource-Provider auswählt und die Abrechnung ihm gegenüber, genauso wie dem Grid-Nutzer gegenüber, durchführt[5].

1.2.2 Serviceorientierte Sicht

Die historische Herleitung, im Bezug auf die Serviceorientierung, erfolgt aufgrund von Ansätzen und Ideen, die für die Entwicklung des Cloud Computing eine wichtige Rolle spielen und somit die zweite Hälfte des Fundaments vom Cloud Computing bilden.

1.2.2.1 Utility Computing

Die Anfänge von Utility Computing liegen in den 1960er Jahren, als John McCarthy seine Vision über das Anbieten beziehungsweise das Beziehen von IT-Services äußerte. Seiner Meinung nach sollte es irgendwann möglich sein, IT-Services in gleicher Weise wie Strom, Wasser oder Gas beziehen beziehungsweise anbieten zu können[19]. Für eine Definition wird dieser Ansatz jedoch nicht genügen, da IT-Services verständlicherweise viel komplexer als Strom, Wasser oder Gas sind. Im Buch von H. Kircher wird Utility Computing ziemlich treffend wie folgt definiert:

Utility Computing beschreibt eine grundlegende Transformation der Bereitstellung und des Managements von IT-Services - von einem technologieorientierten zu einem geschäftsorientierten Ansatz. Diese Umstellung erfordert eine äußerst flexible und effizient verwaltete dynamische IT-Infrastruktur mit vollständiger Kostenkontrolle, flexibler Kostenverrechnung und aktivem SLA-Management[6].

In anderen Worten bedeutet das, dass Utility Computing als ein Geschäftsmodell gesehen werden kann, bei dem ein Service-Provider seine IT-Services anbietet und diese dem Kunden nach Bedarf zur Verfügung stellt. Ein wesentliches Merkmal des Utility Computing ist die verbrauchsabhängige Abrechnung, bei der der Kunde nur das bezahlt, was er auch tatsächlich in Anspruch genommen hat. So können Unternehmen, die als Kunden von Utility Computing IT-Services in Anspruch nehmen, ihre Kosten im Bereich der IT deutlich reduzieren. Dabei kann es sich um Kosten handeln, die aufgrund der blossen Bereitstellung von Rechenressourcen in einem Unternehmen, die nur zu einem bestimmten Zeitpunkt benötigt werden, entstehen. Hat ein Unternehmen beispielsweise zur Weihnachts- oder Urlaubszeit eine deutlich höhere Auslastung der IT-Ressourcen, so müsste dieses, ohne des Konzepts von Utility Computing, diese Ressourcen auch das ganze Jahr über bereitstellen, da diese ja irgendwann benötigt werden. Mit Utility Computing kann das Unternehmen die entsprechenden IT-Ressourcen seinem Bedarf nach zum gegebenen Zeitpunkt anpassen[6].
Utility Computing wird in drei Typen unterteilt: Internal Utility, External Utility und eine Mischung aus Internal und External Utility. Dabei erfolgt die Unterteilung nach der Art, woher die IT-Services bezogen werden.

- **Internal Utility**
  Bei Internal Utility nutzt ein Unternehmen ein Rechenzentrum, das allein IT-Services an die einzelnen Abteilungen dieses Unternehmens anbietet.

- **External Utility**
  Bei External Utility stellt ein externer Service-Provider IT-Services zur Verfügung, die von mehreren verschiedenen Unternehmen aus einem Rechenpool bezogen werden.

- **Mischform**
  Bei der Mischform werden für das Unternehmen IT-Services teilweise vom eigenen Rechenzentrum und teilweise von externen Service-Providern bereitgestellt[2].

1.2.2.2 Service Bureau

Service Bureau ist ein Geschäftsmodell, dass auf dem Konzept des Utility Computing aufbaut. Ein Service Bureau war ein Unternehmen, das gegen eine Gebühr anderen Unternehmen ihre IT-Dienste zur Verfügung stellte. Dabei wurde nicht nur die EDV zur Verfügung gestellt, sondern auch Diensleistungen, die von Mitarbeitern solcher Service Bureaus durchgeführt wurden. Zum Leistungsspektrum der Service Bureaus zählten Dienste wie Datenverarbeitung, Bereitstellung von Speicherplatz und individuelle Programmierung. Dabei wurde die Verbindung zu solchen Service Bureaus mit Hilfe von einfachen Wählverbindungen oder auch privaten Leitungen hergestellt[20].

1.2.2.3 Application Service Provider

Der nächste Schritt in Richtung Cloud Computing ist das Geschäftsmodell des Application Service Provider (ASP), das auf den Konzepten der Service Bureaus und somit auch auf denen des Utility Computing aufbaut. ASPs sind Anbieter von webbasierten Dienstleistungen zur Nutzung einer Anwendungssoftware. Dabei befindet sich diese Anwendungssoftware in einem zentralen Datenzentrum, von welchem aus die Software auch verwaltet wird. Die Kunden der ASPs können im Rahmen eines Mietvertrages auf die gemietete Software und Diensleistungen über Netzwerke zugreifen. Zu den Leistungen, die dem Kunden mit der Zahlung garantiert werden, zählen in erster Linie die Bereitstellung der Software, aber auch die Wartung, Pflege der Server im Datenzentrum, sowie Leistungen des Kundenservices.
Durch den Einsatz des ASP-Modells können für die Kunden IT-Kosten in Unternehmen deutlich gesenkt werden und somit kann die Wettbewerbsfähigkeit verbessert werden. Die Unternehmen können sich also auf ihr Kerngeschäft konzentrieren, ohne sich große Gedanken über die dafür erforderte Software verschwenden zu müssen. Im Vergleich zur klassischen Softwarenutzung, bei der Software erworben, installiert und gewartet werden muss, entfällt beim ASP-Modell die lokale Installation und Wartung der Anwendungssoftware und somit die damit verbundenen Kosten. Besonders Personalkosten, die in der Regel den größten Kostenfaktor einer IT-Abteilung ausmachen, können dadurch gesenkt werden, da die Aufgaben wie Installation, Wartung und Service durch die Application Service Provider durchgeführt werden[3].

1.2.3 Was ist neu an Cloud Computing?

Aus der historischen Entwicklung des Cloud Computing kann man erkennen, dass es bereits vor dem Auftauchen des eigentlichen Begriffs technologische und organisatorische Ansätze gab, die den Eigenschaften des Cloud Computing ähnlich waren. Da stellt sich natürlich die Frage, was an diesem Konzept, im Vergleich zu bereits vorher vorhandenen Konzepten, neu sei. Um das zu analysieren, wird als Erstes versucht Cloud Computing zu beschreiben. Und als Zweites wird ein Vergleich durchgeführt, bei dem die Eigenschaften des Cloud Computing den der anderen, bereits vorher vorhandener Konzepte, gegenübergestellt werden.

1.2.3.1 Definition

Für den Begriff Cloud Computing gibt es noch keine einheitliche oder gar eine standardisierte Definition. Es gibt jedoch zahlreiche Definitionen, deren Ansätze oder Interpretationen das Cloud Computing ziemlich treffend beschreiben. Das Marktforschungsunternehmen Forrester Research bezeichnet Cloud Computing als *einen Pool aus abstrahierter, hochskalierbarer und verwalteter IT-Infrastruktur, die Kundenanwendungen vorhält und falls erforderlich nach Verbrauch abrechnet*[21]. Das Unternehmen Gartner, das ebenfalls Markforschung betreibt, definiert Cloud Computing als *das Bereitstellen von skalierbaren IT-Services über das Internet für eine potenziell große Zahl externer Kunden*[13]. Zwar beschreiben diese, oft zitierte Definitionen Cloud Computing ziemlich treffend, ihnen fehlen jedoch einige Details. Die Definition von Baun, Kunze, Nimis und Tai ist etwas ausführlicher. In ihrem Buch wird Cloud Computing mit dem Einbezug der fehlenden Details wie folgt dargestellt und kann als eine treffende Definition für Cloud Computing verwendet werden:

Unter Ausnutzung virtualisierter Rechen- und Speicherressourcen und moderner Web-Technologien stellt Cloud Computing skalierbare, netzwerk-zentrierte, abstrahierte IT-Infrastrukturen, Plattformen und Anwendungen als on-demand Dienste zur Verfügung. Die Abrechnung dieser Dienste erfolgt nutzungsabhängig[7].

1.2.3.2 Cloud Computing im Vergleich

Bereits aus der Definition wird klar, dass Cloud Computing Ansätze und Konzepte aufweist, die es sowohl aus der technologischen Sicht, als auch aus der serviceorientierten Sicht bereits vor dem Cloud Computing gegeben hat. Im folgenden wird Cloud Computing anhand seiner Eigenschaften mit Konzepten, die in der historischen Herleitung aufgezeigt wurden, verglichen. Aus der technologischen Sicht werden zum Vergleich Cluster Computing und Grid Computing herangezogen, da diese Konzepte viele Ansätze des Cloud Computing bereits gehabt hatten. Und aus der serviceorientierten Sicht werden Utility Computing und ASP dem Cloud Computig gegenübergestellt.
Die erste Tabelle (Abbildung 1.2) zeigt den Vergleich der Eigenschaften von Cluster Computing[2], Grid Computing[4, 5] und Cloud Computing[7].

Eigenschaften	Cluster Computing	Grid Computing	Cloud Computing
Ziel	Nutzung von verteilten Ressourcen	Gemeinsame Nutzung von verteilten Ressourcen	Nutzung von verteilten Ressourcen
Umsetzung	Durch mehrere handelsübliche PCs	Durch Supercomputer, Server, Cluster	Durch Supercomputer, Server, Cluster
Benutzung	Nach aufwendigem Aufbau	Nach Zusammen-schluß zu einer VO und Bereitstellung der eigenen Ressourcen	In wenigen Minuten nutzbar
Einsatz-bereich	Wissenschaft, Unternehmen	Wissenschaft	Privat, Unternehmen, zum Teil Wissenschaft
Ressourcen	Rechenleistung	Rechenleistung, Daten, Anwendungen	Software, Entwicklungs-umgebungen, Infrastruktur
Dynamik	Theoretisch sind Erweiterungen möglich Hoher Aufwand bzw. Kosten	Theoretisch sind Erweiterungen möglich Hoher Aufwand bzw. Kosten	on-demand
Sicherheit	login/password	Absolute Sicherheit wird nicht benötigt	Hohe Sicherheit wird durch Provider garantiert
Kosten	Anschaffungs-kosten der Ressourcen, Nutzung kostenlos	Anschaffungs-kosten der eigenen Ressourcen, Nutzung kostenlos	Keine Anschaffungs-kosten, pay-per-use

Abbildung 1.2: Eigenschaften von Cluster, Grid und Cloud Computing

Eigenschaften	Utility Computing	Application Service Provider	Cloud Computing
Ziel	Anbieten von IT-Services	Anbieten von Anwendungen	Anbieten von IT-Services
Angebot	Rechenleistung, Speicher, Applikationen	Bereitstellung der Software, Wartung und Pflege der Server, Kunden-service	Software Entwicklungs-umgebungen Hardware
Abrechnung	pay-per-use	Mietgebühr	pay-per-use

Abbildung 1.3: Eigenschaften von Utility Computing, ASP und Cloud Computing

- **Ziel**
  Wie man sieht haben alle drei Konzepte als Ziel die Nutzung von verteilten Ressourcen. Es muss jedoch unterschieden werden, wie diese Nutzung im einzelnen gestaltet ist. Wie aus der historischen Herleitung bereits bekannt, ist Cluster Computing auf ein Unternehmen oder eine Institution beschränkt und ist innerhalb dieser zu nutzen. Beim Grid Computing ist die Ortsunabhängigkeit zwar ein großer Vorteil, die gemeinsame Nutzung jedoch ist nur auf die Mitglieder der Virtuellen Organisation beschränkt und es werden in der Regel auch eigene Ressourcen für die VO bereitgestellt. Cloud Computing verlangt keine Ressourcen als Voraussetzung und ist gleichzeitig ortsunabhängig.

- **Umsetzung**
  Bei der Umsetzung scheinen auch hier die Konzepte von Grid und Cloud Computing ziemlich identisch zu sein. Der große Unterschied ist, dass beim Cloud Computing zwar auch Supercomputer, Server und Cluster verwendet werden, diese jedoch vom Dienstanbieter zur Verfügung gestellt werden. Der Nutzer zahlt lediglich für die Nutzung dieser Ressourcen, wo beim Grid Computing hingegen auch Ressourcen, die der VO zur gemeinsamen Nutzung bereitgestellt wurden, angeschafft werden mussten.

- **Benutzung**
  Die nächste wesentliche Neuerung ist die Gestaltung der Benutzung. Beim Cluster Computing müssen die entsprechenden Knoten erst aufgestellt und dann miteinander verbunden werden. Dann könnte man mit entsprechendem Betriebssystem, das vorher installiert werden musste, die benötigte Rechenleistung nutzen. Zwar könnte das von einem Anbieter solcher Cluster übernommen werden, ist aber mit den entsprechenden Kosten- und Zeitaufwand verbunden. Auch beim Grid Computing konnte man erst nach der Bereitstellung eigener Ressourcen und dem Zusam-

menschluß zu einer VO die entsprechenden Ressourcen nutzen. Das Konzept des Cloud Computing sieht es vor, die Ressourcen nach einem Anmeldungsprozedere und einer kurzen Einarbeitung bereits nutzen zu können.

- **Einsatzbereich**
  Auch der Einsatzbereich der Ressourcen ist ein wesenlicher Punkt, in dem sich das Cloud Computing von anderen Konzepten unterscheidet. Cluster Computing wird in der Regel in Unternehmen eingesetzt, weil der Cluster aus den bereits vorhandenen Workstations aufgebaut werden kann und auch für die Wissenschaft nach den üblichen Arbeitszeiten genutzt werden kann. Beim Grid Computing werden die Ressourcen in der Regel für die Wissenschaft genutzt, da man gemeinsam innerhalb einer VO Forschung auf einem bestimmten Gebiet betreiben und somit die dafür benötigten Daten oder Anwendungen gemeinsam nutzen kann. Cloud Computing ist nicht nur für Unternehmen interessant, sondern auch für Privatpersonen, da in der heutigen Welt der digitalen Daten auch Dienste für Privatpersonen benötigt werden. Zwar ist Cloud Computing auch für den Einsatz in der Wissenschaft möglich, jedoch steigt hier die Begeisterung nur langsam.

- **Ressourcen**
  Bei der Ressourcenart, die bei den drei Modellen bereitgestellt wird, zeigt sich eine Entwicklung nach oben was die Angebotsbreite angeht. Wo beim Cluster in erster Linie Rechenleistung bereitgestellt wurde, ist beim Grid die Leistung um Daten und Anwendungen erweitert worden. Beim Cloud Computing gehen die Anbieter noch einen Schritt weiter und stellen ihren Kunden neben der abstrahierten Sicht auf Hardware, wie Rechner, Massenspeicher und Netzwerke auch Entwicklungsumgebungen und Software zur Verfügung.

- **Dynamik**
  Auch was die Dynamik betrifft, ist Cloud Computing, im Unterschied zu Cluster und Grid, vorteilhafter. Zwar ist beim Cluster und Grid eine Erweiterung beziehungsweise Minderung der Ressourcen möglich, die jedoch mit einem zeitlichen Aufwand und mit den enstehenden Kosten verbunden ist.
  Bei Cloud Computing wird der Begriff ”on-demand” verwendet, da der Nutzer die Ressourcen nach seinem Bedarf anpassen kann.

- **Sicherheit**
  Da Cloud Computing-Anbieter ihre Dienste über das Internet anbieten, ist die Sicherheit ein wichtiger Punkt und zum Teil ein heikles Thema. Beim Cluster und beim Grid ist die Sicherheit schon zum Teil dadurch gegeben, dass die Ressourcen sich im Unternehmen oder innerhalb der VO befinden. Beim Cloud Computing ist genau dies der Punkt, wegen dem sich viele Unternehmen dagegen entscheiden, ihre IT-Dienste aus der ”Wolke” zu beziehen, da hier die Ressourcen ausgelagert werden. Obwohl die Anbieter eine hohe Sicherheit garantieren, ist nicht bei allen Nutzern das Vertrauen in diese vorhanden – jedenfalls noch nicht.

- **Kosten**
  Der wichtigste Punkt, mit dem die Anbieter die potenziellen Kunden werben, ist

die Einsparung der Kosten durch die Nutzung von Cloud Computing. Zwar entstanden beim Cluster Computing und Grid Computing bei der reinen Nutzung von Ressourcen niedrige oder gar keine Kosten, jedoch war die Anschaffung mit großen Ausgaben verbunden. Beim Cloud Computing wird nach dem Prinzip "pay-per-use" abgerechnet. Das heißt, dass der Nutzer nur für die tatsächliche Nutzung der Ressourcen bezahlt.

In der zweiten Tabelle (Abbildung 1.3) werden die Geschäftsmodelle Utility Computing[6] und Application Service Provider[3] im Vergleich zu Cloud Computing[7], in wesentlichen Punkten, dargestellt. Hier wird ersichtlich, dass Cloud Computing zwar, wie oben beschrieben, viele technologische Neuerungen mit sich bringt, jedoch als Geschäftsmodell auf bereits vorhande Techniken zurückgreift. Als Ziel scheint Cloud Computing dasselbe zu verfolgen wie Utility Computing, nämlich das Anbieten von IT-Services, was das Anbieten von Anwendungen und somit das Ziel des ASP miteinschließt. Das Angebot ist im Gegensatz zu den anderen Geschäftsmodellen um Einiges erweitert worden. Auch die Abrechnung erfolgt, genau auf die gleiche Art wie es bei Utility Computing der Fall war, nämlich nach dem Prinzip "pay-per-use".
Insgesamt betrachtet hat das Cloud Computing zwar Ideen und Techniken von den Vorreitern übernommen, jedoch auch eine Menge neuer Konzepte, die den IT-Bereich deutlich vereinfachen und Kosten einsparen sollen, realisiert.

1.3 Abgrenzung zu wesentlichen Begriffen

Häufig werden die Begriffe Virtualisierung, Service-orientierte Architekturen, Web Services oder Distributed Computing mit Cloud Computing in Verbindung gebracht oder gar gleichgesetzt. In diesem Abschnitt werden diese Begriffe anhand ihrer Definition, Eigenschaften und Einsatzgebiete zu Cloud Computing abgegrenzt.

1.3.1 Virtualisierung

Bei den meisten Cloud-Architekturen kann die Virtualisierung als ein Grundbaustein angesehen werden. Dabei ist die Idee physische Ressourcen, wie Server, Daten, Netzwerke und Software, in Pools zusammenzufassen und gemeinsam zu verwalten. Dies ermöglicht seine individuellen Anforderungen aus diesem Ressourcen-Pool zu befriedigen. Bei der Virtualisierung wird hierfür statt einer realen Maschine eine virtuelle Maschine eingesetzt.
Der Oberbegriff Virtualisierung kann in Unterkategorien Betriebssystemvirtualisierung, Plattformvirtualisierung, Speichervirtualisierung, Netzwerkvirtualisierung und Anwendungsvirtualisierung unterteilt werden[7].

- **Betriebssystemvirtualisierung**
  Bei dieser Form, die auch als Container oder Jails bezeichnet wird, laufen unter einem Betriebssystemkern mehrere voneinander abgeschottete, identische Systemumgebungen. Nach außen treten diese virtuellen Umgebungen wie eigenständige Sys-

teme auf. Zwar verwenden alle aktiven Anwendungen den gleichen Betriebssystemkern, sehen jedoch nur die Prozesse, die sich auch in der selben virtuellen Umgebung befinden[7].

- **Plattformvirtualisierung**
  Bei der Plattformvirtualisierung wird die Ausführung beliebiger Betriebssysteme und Anwendungen in virtuellen Umgebungen ermöglicht. Dabei verteilt ein Monitor, der ein auf ein Minimum reduziertes Metabetriebssystem ist, die Hardwareressourcen unter den Gastsystemen und koordiniert die Zugriffe. Wird bei der Plattformvirtualisierung ein kompletter virtueller Rechner simuliert, so spricht man von einer vollständigen Virtualisierung. Steht den Gastbetriebsystemen keine emulierte Hardwareebene zur Verfügung, sondern nur eine Anwendungsschnittstelle, so spricht man von einer Para-Virtualisierung[7].

- **Speichervirtualisierung**
  Hier wird der physische Speicher in Pools zusammengefasst, damit die Anwendungen ihre Speicheranforderungen dynamisch aus diesen befriedigen können. Die Datentransfers laufen dabei über ein spezielles Speichernetzwerk (SAN) oder ein Firmennetzwerk (LAN)[7].

- **Netzwerkvirtualisierung**
  Bei der Netzwerkvirtualisierung werden die Ressourcen als Web-Objekte implementiert, damit die Services über eine virtuelle IP-Adresse zur Verfügung gestellt werden können. Es ist dann möglich durch die Weiterleitung von DNS-Requests Cloud-Ressourcen im Internet-Namensraum des Kunden einzublenden. Häufig werden auch virtuelle lokale Netze (VLAN) und virtuelle Switches verwendet. Dabei erscheinen die Cloud-Ressourcen direkt im Netzwerk des Kunden[7].

- **Anwendungsvirtualisierung**
  Bei diesem Modell werden dem Kunden Anwendungen, die zentral verwaltet werden, über ein Netzwerk angeboten. Somit ist eine übliche Software-Installation nicht mehr nötig. Es gibt zwei Verfahren, um die virtuellen Anwendungen bereitzustellen: Hosted Application und Virtual Appliance. Bei dem Verfahren Hosted Application steht die Anwendung im Internet bereit und wird zum Kunden transportiert. Bei Virtual Appliance hingegen wird die Anwendung heruntergeladen und kann auf einem eigenen Rechner betrieben werden. Dabei stehen in einer virtuellen Umgebung alle zur Anwendung gehörenden Dateien und Komponenten, die zum Ausführen benötig werden, bereit[7].

1.3.2 Service-orientierte Architekturen

Bei Service-orientierten Architekturen (SOA) handelt es sich um einen Architekturstil, welcher das Anbieten und Nutzen von Diensten definiert. Dabei können die Dienste sowohl von Kunden, als auch von anderen Diensten oder Applikationen genutzt werden. Da Dienste in unterschiedliche Programmiersprachen und auf unterschiedlichen Plattformen implementiert werden können, wird dem Kunden oder anderen Diensten eine plattform- und sprachenunabhängige Nutzung beziehungsweise Wiederverwendung solcher Dienste

ermöglicht.
Es gibt zwei Verbindungsmöglichkeiten zwischen den Dienstnutzern und den Dienstanbietern: Punkt-zu-Punkt-Verbindung und Hub-and-Spoke-Ansatz. Bei der Punk-zu-Punkt-Verbindung muss der Dienstnutzer den Endpunkt des erfoderlichen Dienstes genau kennen. Die Dienstanfrage geht dann direkt an den entsprechenden Anbieter. Beim Hub-and-Spoke-Ansatz kennt der Dienstnutzer die exakte Adresse des Dienstanbieters nicht. Hier gibt es für jeden Dienst einen symbolischen Namen und einen Vermittler, den sogenannten Enterprise Service Bus. Er hat die Aufgabe die Nachrichten zwischen den Diensten weiterzuleiten, die Daten von einem Format in ein anderes zu transformieren und das Dienstverzeichnis zu verwalten[7].

1.3.3 Web Services

Die W3C Working Group definiert einen Web Service wie folgt:

A Web service is a software application identified by a URI, whose interfaces and binding are capable of being defined, described and discovered by XML artifacts and supports direct interactions with other software applications using XML based messages via internet-based protocols[12].

Anders ausgedrückt heißt es, dass Web Services unabhängige, in sich abgeschlossene Anwendungen sind, die eine genau definierte Aufgabe erfüllen. Sie sind über programmierbare Schnittstellen erreichbar, die in erster Linie zur Anwendungskommunikation dienen und keine graphische Benutzeroberfläche haben. Den Web Service-Nutzern und Web Service-Anbietern bleiben die Details der Implementierung verborgen. Web Services können jederzeit und von jedem Ort aus aktiviert werden. Operationen und Nachrichten können mehrere Protokolle wie zum Beispiel HTTP (Hypertext Transfer Protocol) oder SMTP (Simple Mail Transfer Protocol) unterstützen. Web Services können in weitere Web Services zerlegt oder zu einem neuen Web Service zusammengestellt werden. Web Services können als ein Konsument, ein Anbieter oder ein Verzeichnis agieren[10].
Als Standards für die Formatierung und Bearbeitung von Nachrichten sowie für die Dienste-Schnittstellen werden bei den Web Services meist die Standards SOAP/WSDL und REST verwendet. WSDL (Web Service Description Language) bietet eine XML-Beschreibung der Fähigkeiten des Web Services. SOAP (Simple Object Access Protocol) widmet sich, unabhängig von der zugrunde liegenden Software-Architektur, der Intergration von Applikationen über das Internet. REST (REpresentational State Transfer) hingegen baut auf HTTP auf. Somit werden auch RESTful Services nur über die uniforme HTTP-Schnittstelle angesprochen. Zum Datenaustausch wird sowohl bei SOAP/WSDL, als auch bei REST das XML-Format genutzt. Bei dem Standard SOAP/WSDL wird es sogar vorgeschrieben[10, 8].

1.3.4 Distributed Computing

Wenn man allgemein vom verteiltem Rechnen (englisch: distributed computing) spricht, so handelt es sich um den Oberbegriff für alle Konzepte, die zur Lösung von Aufgaben ver-

teilte Ressourcen nutzen. Deshalb wird auch Distributed Computing (DC) oft mit Cluster, Grid oder Cloud Computing gleichgesetzt. Heute hat sich der Begriff Distributed Computing als ein Modell etabliert, das bei wissenschaftlichen Forschungen häufig eingesetzt wird.
Die Grundidee ist dieselbe wie bei anderen verteilten Systemen. Es soll die Rechenleistung eines Supercomputers, der in der Regel für wissenschaftliche Forschungen benötigt wird, erreicht werden, aber ohne solch einen Supercomputer anschaffen zu müssen. Die Ansätze von Cluster Computing und Grid Computing ermöglichen es. Jedoch ist beim Cluster Computing eine große Menge an gewöhnlichen Rechnern nötig, um dies zu bewerkstelligen. Und auch bei Grid Computing werden in der Regel vorhandene Ressourcen innerhalb einer Virtuellen Organisation gemeinsam genutzt. Hat man die entsprechenden Ressourcen nicht, so ist es normalerweise nicht möglich rechenintensive Forschungen zu betreiben.
Beim Modell Distributed Computing kommt die Rechenleistung von handelsüblichen PCs, die dem jeweiligen Projekt von normalen Haushalten zur Verfügung gestellt werden. Dabei wird ein Programm von einem Server heruntergeladen und auf dem PC installiert. Wenn der Computer im Betrieb ist und das entsprechende Programm läuft, sendet der Server über das Internet eine kleine Teilaufgabe des gesamten Rechenproblems. Diese Aufgabe wird vom Programm berechnet und anschließend wird die Lösung an den Server zurückgeschickt, der dann aus vielen eingesendeten Teillösungen die Komplettlösung zusammensetzt. Dabei können solche Berechnungen Minuten, Stunden oder sogar Tage auf dem PC im Hintergrund laufen.
Bekannte Projekte für DC sind unter anderem "SETI@home"[22] das sich mit der Suche nach außerirdischer Intelligenz beschäftigt, "Einstein@Home"[14], das auf der Suche nach Gravitationswellen ist und "Folding@home"[23], das die Faltung von Proteinen simuliert und neben der Rechenleistung von PCs auch die Rechenleistung von Sony Playstation 3 Spielkonsolen nutzt[24].

1.3.5 Abrgenzung zu Cloud Computing

Anhand der Beschreibung von Virtualisierung, SOA und Web Services wird klar, dass es sich bei diesen Konzepten nicht um Cloud Computing handelt, sondern um Techniken, die beim Cloud Computing zur Realisierung eingesetzt werden. Durch Virtualisierung können Ressourcen zum Beispiel in Pools zusammengefasst und gemeinsam verwaltet werden. SOA ermöglichen dann das Anbieten und Nutzen solcher virtualisierter Ressourcen. Und Web Services dienen dabei zur Anwendungskommunikation[7].
Distributed Computing hingegen kann eher als ein Spiegelbild von Cloud Computing betrachten werden. Es werden zwar bei DC verteilte Ressourcen zur Problemlösung herangezogen, jedoch werden diese von Nutzern bereitgestellt und nicht wie bei Cloud Computing von Nutzern bezogen. Man könnte sagen, dass die Rollenverteilung zwischen Nutzer und Anbieter hier genau umgekehrt ist.

1.4 Darstellung aus technischer und organisatorischer Sicht

Cloud Computing Architektur kann zum einen aus der technischen Sicht betrachtet werden und zum anderen aus der organisatorischen Sicht. Bei der technischen Sicht werden die drei Hauptvertreter des everything-as-a-service-Paradigmas dargestellt: Software-as-a-Service, Platform-as-a-Service und Infrastrukture-as-a-Service. Aus der organisatorischen Sicht werden die Clouds des Cloud Computing in vier Arten unterteilt dargestellt: Public Clouds, Private Clouds, Hybrid Clouds und Community Clouds.

1.4.1 Technische Sicht

Wenn man die technische Sicht der Cloud Computing Architektur betrachtet, kann man es sich als ein Schichtenmodell vorstellen, in dem die einzelnen Schichten nach ihrem Abstraktionsgrad angeordnet sind. Dabei können die oberen Schichten die Dienste aller unteren Schichten zur eigenen Dienstrealisierung nutzen. Die einzelnen Schichten in diesem Schichtenmodell werden durch ihre Eigenschaften charakterisiert und in weitere Unterschichten aufgeteilt. Falls es Schichten gibt, die Dienste und Schnittstellen aufweisen, die in mehrere Schichten eingeordnet werden können, werden diese der höchsten dieser Schichten zugeteilt. Die drei Hauptvertreter dieser Schichten sind Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) und Software-as-a-Service (SaaS). Dabei ist IaaS im Schichtenmodell ganz unten, PaaS in der Mitte und SaaS ganz oben[7].

1.4.1.1 Infrasturcture-as-a-Service

In der IaaS Schicht wird dem Benutzer eine abstrahierte Sicht auf Hardware wie Rechner, Massenspeicher, Netzwerke und so weiter angeboten. Der Nutzer bekommt also Ressourcen, die er dynamisch nach seinem Bedarf anpassen kann. IaaS teilt sich in die Resource Set-Unterschicht und die Infrastructure Services-Unterschicht auf.
In der Resource Set-Unterschicht wird dem Benutzer eine Benutzerschnittstelle zur Verwaltung einer Menge von Ressourcen bereitgestellt. Resource Set-Unterschicht lässt sich weiter in Physical Resource Set und Virtual Resource Set unterteilen. Der Unterschied zwischen diesen ist bereits an den Bezeichnungen ersichtlich. Physical Resource Set basiert auf einer physikalischen Hardware, die auch so angeboten wird. Virtual Ressource Set hingegen baut auf Virtualisierungstechnologien auf und stellt somit auch virtuelle Instanzen zur Verfügung.
Wie bereits erwähnt besteht IaaS neben der Ressource Set-Unterschicht auch aus der Infrastructure Services-Unterschicht. Dabei haben die Infrastructure Services einen engeren Anwenderfokus. Es gibt zum Beispiel Infrastructure Services für Berechnungsaufgaben, für Massenspeicher oder für Netzwerke[7, 8].

1.4.1.2 Platform-as-a-Service

Die PaaS-Schicht richtet sich an Entwickler. Es werden hier in den Unterschichten Programming Environments (PE) und Execution Environments (EE) den Entwicklern Umgebungen angeboten, um eigene Software in einer bestimmten Programmiersprache zu entwickeln. Die PEs erweitern bereits vorhandene Programmiersprachen um Elemente wie Klassenbibliotheken, die für die Entwicklung der Software relevant wären. Ein Beispiel für Programming Environments ist das von Sun Microsystems angebotene Project Caroline [25]. Die EEs dagegen bringen häufig ein eigenes Programming Environment mit. Ein Beispiel dafür ist das von Google angebotene App Engine[26][7, 11].

1.4.1.3 Software-as-a-Service

Im Gegensatz zu der PaaS-Schicht richtet sich die SaaS-Schicht direkt an die Endkunden. Hier werden dem Kunden Anwendungen, die vom Anbieter zentral verwaltet werden und auf die in der Regel über das Internet zugegriffen wird, bereitgestellt. Die Kunden müssen beim SaaS keine lokale Software-Installation für die entsprechende Software durchführen und die für die Software erforderlichen Ressourcen auch nicht bereitstellen. Die Verwaltung einer Anwendung wird vollständig durch den Anbieter selbst übernommen. Die SaaS-Schicht kann man in zwei Unterschichten gliedern: Application Services und Applications. Bei Application Services handelt es sich um Anwendungen, die auf einer einfachen Applikation basieren und bei Applications hingegen um vollwertige komplexe Anwendungen[7, 8]. In Abbildung 1.4 werden die drei Schichten mit ihren Unterschichten veranschaulicht dargestellt.

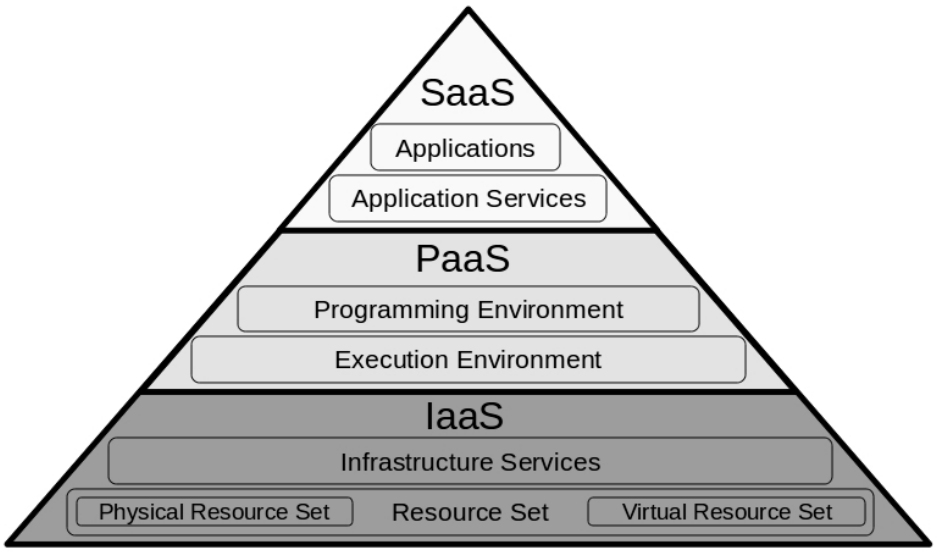

Abbildung 1.4: Das Schichtenmodell der Cloud Computing Architektur

1.4.2 Organisatorische Sicht

Neben der Architektur des Cloud Computing, die aus der technischen Sicht betrachtet worden ist, müssen nun auch die Cloud Computing-Typen erläutert werden. Durch diese Betrachtung aus der organisatorischen Sicht wird verdeutlicht, wie das Zusammenspiel zwischen dem Service Provider und seinen Kunden beim Cloud Computing organisiert ist. Dabei wird zwischen vier Arten von Cloud Computing unterschieden: Public Cloud, Private Cloud, Hybrid Cloud und Community Cloud.

1.4.2.1 Public Cloud

Bei der Public Cloud werden Ressourcen durch einen Service Provider über das Internet für die Öffentlichkeit bereitgestellt. Dabei gehören die Anbieter nicht derselben organisatorischen Einheit an wie die Benutzer. Die Nutzung dieser Dienste wird auf Basis der tatsächlich über die Zeit benutzten Ressourcen verrechnet. Die Kosten für Hardware, Anwendungen und Netzwerkanbindung, die dazu benötigt werden, werden durch den Anbieter abgedeckt. Da die Abrechnung für die wirklich genutzten Ressourcen erfolgt, werden somit auch keine Ressourcen verschwendet[7, 8].

1.4.2.2 Private Cloud

Der Ansatz von Private Cloud ist ähnlich wie bei der Public Cloud. Jedoch ist hier die Organisation für einen internen Gebrauch in einem Unternehmen und in einer kleineren Form gedacht. Denn bei Private Cloud gehören die Anbieter und Benutzer derselben organisatorischen Einheit an. Das kann das eigene Unternehmen oder aber auch eine Einbeziehung von anderen Unternehmensbereichen, Partnerunternehmen oder Lieferanten sein. Im Gegensatz zu der Public Cloud unterliegt die Private Cloud einer strikteren Kontrolle und höheren Sicherheitsanforderungen. Das heißt im Endeffekt, dass die Kontrolle über die Daten beim Benutzer beziehungsweise innerhalb dessen Organisation bleibt[7, 8].

1.4.2.3 Hybrid Cloud

Das dritte Modell des Cloud Computing ist die Hybrid Cloud. Dabei handelt es sich um eine Kombination aus der Public Cloud und der Private Cloud. Es werden sowohl lokale Anwendungen, als auch Anwendungen aus der Public Cloud genutzt. So kann ein Unternehmen die Kontrolle über seine Hauptanwendungen bewahren und das Cloud Computing nur dort einsetzen, wo es für das Unternehmen auch sinnvoll ist. Man kann sich somit erstmal schrittweise an das Cloud Computing annähern und vorerst unsensible Daten und Funktionen auslagern[7, 8].

1.4.2.4 Community Cloud

In diesem Konzept des Cloud Computing schließen sich mehrere Unternehmen beziehungsweise Organisationen zu einer Gemeinschaft zusammen und bilden mit ihren Private Clouds eine Community Cloud. Bei dieser Variante des Cloud Computing ist es nur den Mitgliedern dieser Community möglich auf die gemeinsamen Ressourcen zuzugreifen. Durch diese Abzweigung von der Private Cloud haben die Nutzer zwar ein breiteres Angebot an Ressourcen als bei der Private Cloud, jedoch steigt hier das Sicherheitsrisiko, da Daten und Prozesse verschiedene administrative Bereiche, in denen unterschiedliche Sicherheitsrichtlinien gelten, durchlaufen können[9]. Anhand der Abbildung 1.5 sollen die vier Cloud Computing-Typen bildlich veranschaulicht werden.

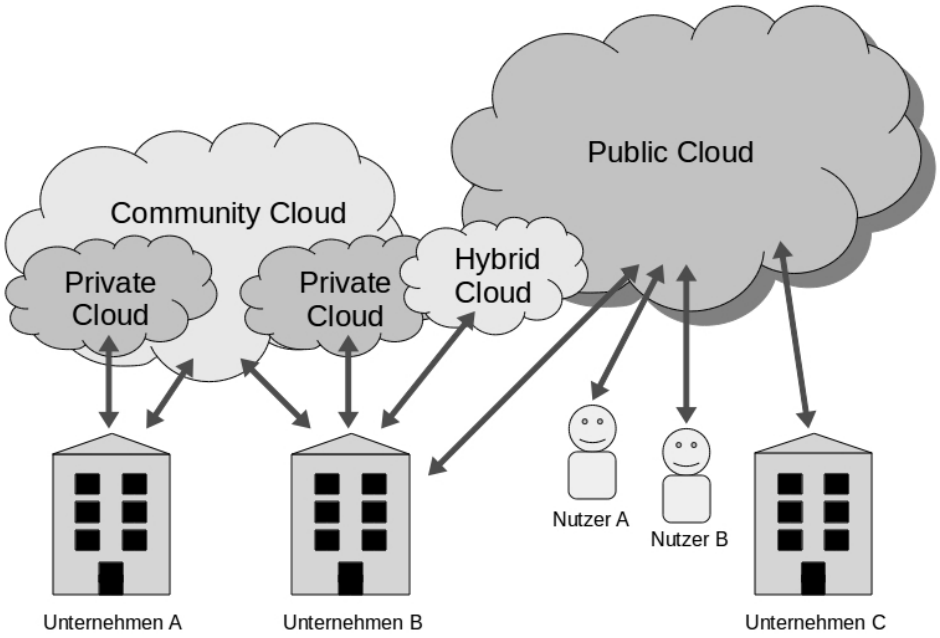

Abbildung 1.5: Public, Private, Hybrid und Community Clouds

1.5 Fazit

Die Entwicklung des Cloud Computings hatte schon bereits in den 1960er Jahren ihren Anfang. Dabei können aus der Sicht der technologischen Entwicklung die Konzepte von Supercomputer, Cluster Computing und Grid Computing als Grundbausteine für das Entstehen des Cloud Computings gesehen werden. Aus der Sicht der serviceorientierten Entwicklung waren es die Konzepte von Utility Computing, Service Bureau und Application Service Provider. Zwar hat Cloud Computing viele Techniken von diesen Vorreitern übernommen, jedoch auch eigene Ideen und innovative Konzepte realisiert.
Das Angebot, das den Nutzern des Cloud Computing zur Verfügung steht, ist ziemlich breit und bietet vielen Zielgruppen neue Möglichkeiten im Bereich der IT. So kann der Nutzer die Software, die gerade benötigt wird, über einen Provider beziehen und nur für

die tatsächliche Nutzung bezahlen. Ein Softwareentwickler kann seine eigenen Software entwerfen und dabei auf die Entwicklungsumgebungen zurückgreifen, die ebenfalls beim Cloud Computing angeboten werden. Auch Ressourcen wie Rechenleistung oder Massenspeicher können beim Cloud Computing bezogen und dynamisch verwendet werden. Ein weiterer Punkt, der Cloud Computing besonders für Unternehmen interessant macht, ist die Organisation der einzelnen Clouds. So kann ein Unternehmen entscheiden, ob es das Cloud Computing im vollen Umfang nutzt, nur auf sein eigenes Unternehmen beschränkt oder sich für eine Kombination dieser Konzepte entscheidet.
Insgesamt betrachtet ist Cloud Computing ein innovatives Konzept, das viele Vorteile mit sich bringt und zukunftsweisende Möglichkeiten für die IT-Branche aufzeigt.

Literaturverzeichnis

[1] H. Adeli. *Supercomputing in Engineering Analysis*, Marcel Dekker, New York, 1992.

[2] G. Bengel, C. Baun, M. Kunze, K.Stucky. *Masterkurs Parallele und Verteilte Systeme*, Vieweg+Teubner, Wiesbaden, 2008.

[3] G. Tamm. *Webbasierte Dienste*, Physica-Verlag, Heidelberg, 2005.

[4] D. Fey (Hg.). *Grid-Computing*, Springer-Verlag, Berlin Heidelberg, 2010.

[5] T. Barth, A. Schüll (Hgg.). *Grid Computing*, Friedr. Vieweg & Sohn Verlag, Wiesbaden, 2006.

[6] H. Kircher (Hg.). *IT. Technologien, Lösungen, Innovationen*, Springer-Verlag, Berlin Heidelberg, 2007.

[7] C. Baun, M. Kunze, J. Nimis, S. Tai. *Cloud Computing*, Springer-Verlag, Berlin Heidelberg, 2010.

[8] R. Vogel, T. Kocoglu, T. Berger. *Desktopvirtualisierung*, Vieweg+Teubner Verlag, Wiesbaden, 2010.

[9] B. Furht, A. Escalante (Hgg.). *Handbook of Cloud Computing*, Springer Science+Business Media, New York, 2010.

[10] U. Bettag. *Web-Services*, Informatik-Spektrum, Band 24, Heft 5, Seite 302-304, Springer, Berlin, 2010.

[11] A. Lenk, M. Klems, J. Nimis, S. Tai, T. Sandholm. *What's inside the Cloud? An architectural map of the Cloud landscape*, ICSE 2009 Workshop on Software Engineering Challenges of Cloud Computing, pp.23-31, 2009.

[12] D. Austin, A. Barbir, S. Garg. *Web Services Architecture Requirements*, `http://www.w3.org/TR/2002/WD-wsa-reqs-20020429`, besucht am 24.02.2011.

[13] W. Herrmann. *Dynamic IT mit Cloud Computing*, `http://www.tecchannel.de/server/cloud_computing/1759881/dynamic_it_mit_cloud_computing/`, besucht am 24.02.2011.

[14] B. Alle. *About Einstein@Home*, `http://einsteinathome.org/`, besucht am 24.02.2011.

[15] Cluster - Informatik Projekt. *Geschichte der Supercomputer/Cluster*, http://www.derneuepopel.de/cluster/clusterinfo.html#Geschichte, besucht am 24.02.2011.

[16] Top 500 Supercomputing Sites. *Top 500 List*, http://www.top500.org/list/2010/11/100, besucht am 24.02.2011.

[17] ECE Lab. *Table of Supercomputers (1961 to 2009)*, http://ecelab.com/supercomputers-list.htm, besucht am 24.02.2011.

[18] IT Wissen. *Supercomputer*, http://www.itwissen.info/definition/lexikon/Supercomputer-supercomputer.html, besucht am 24.02.2011.

[19] WordPress.com. *Utility (Cloud) Computing...Flashback to 1961 Prof. John McCarthy*, http://computinginthecloud.wordpress.com/2008/09/25/utility-cloud-computingflashback-to-1961-prof-john-mccarthy/, besucht am 24.02.2011

[20] PC Magazine Encyclopedia. *Definition of: service bureau*, http://www.pcmag.com/encyclopedia_term/0%2C2542%2Ct%3Dservice+bureau&i%3D51180%2C00.asp, besucht am 24.02.2011

[21] Cloud Computing Report. *Definition Cloud Computing*, http://www.cloud-computing-report.de/definition/, besucht am 24.02.2011.

[22] SETI@home. *Die Wissenschaft hinter SETI@home*, http://setiathome.berkeley.edu/sah_about.php, besucht am 24.02.2011.

[23] Folding@home. *The science behind Folding@home*, http://folding.stanford.edu/English/Science, besucht am 24.02.2011.

[24] Folding@home. *About Folding@home*, http://folding.stanford.edu/English/About, besucht am 24.02.2011.

[25] Oracle. *About Project Caroline* http://labs.oracle.com/projects/caroline/, besucht am 24.02.2011.

[26] Google. *Google App Engine* http://code.google.com/intl/de-DE/appengine/, besucht am 24.02.2011.

Kapitel 2

Sicherheitsmanagement in Cloud Computing

Matthias Oehme

Dieses Kapitel befasst sich mit dem Sicherheitsmanagement im Cloud Computing. Es soll aufgezeigt werden welche Besonderheiten beim Cloud Computing das Sicherheitsmanagement beeinflussen. Dabei wird ein Fokus auf das Identitätsmanagement gelegt. Es werden mehrere Authentifizierungsdienste vorgestellt und das Sicherheitsmanagement von Amazon Web Services genauer betrachtet.

Inhaltsverzeichnis

2.1 Was ist Sicherheitsmanagement?

Sicherheitsmanagement befasst sich mit der Entwicklung eines Sicherheitskonzeptes für Unternehmen. Jedes Unternehmen ist verpflichtet für die Sicherheit der eigenen IT Verantwortung zu übernehmen. Durch ein umfassendes Sicherheitsmanagement lassen sich Datenverluste, Hackerangriffe, Viren- und/oder Trojanerbefälle und vieles mehr verhindern beziehungsweise einschränken. Die Erstellung des Sicherheitskonzept sollte dabei nicht nur der IT-Abteilung des Unternehmens unterliegen, sondern auch von der Führungsetage des Unternehmen gesteuert werden. Da es beim Sicherheitsmanagement um die Zukunft eines Unternehmens geht, sollte diesem auch die entsprechende Beachtung entgegen gebracht werden. Die Aufgaben des Sicherheitsmanagement werden in zwei Bereich unterteilt: operative Aufgaben und strategische Aufgaben. In den Bereich der strategischen Aufgaben gehören:

- strategische Analysen (Bedrohungsanalyse, Schwachstellenanalyse),
- Planung von Sicherheitszielen, Strategien und Sicherheitsmaßnahmen,
- Erstellung eines Sicherheitskonzepts,
- Festlegung von Verantwortung für die Sicherheit in allen unterschiedlichen Bereichen, sowie Vergabe der benötigten Kompetenzen an die verantwortlichen Stellen und Mitarbeiter,
- strategische Kontrolle, d. h. Überprüfung von Prämissen des Sicherheitskonzepts, der gesetzten Sicherheitsziele sowie der Wirksamkeit der geplanten Strategien.

[15]

In den Bereich der operativen Aufgaben gehören die folgenden:

- operative Analysen (Risikoanalyse)
- operative Planung von Maßnahmen und Projekten zur Umsetzung des Sicherheitskonzepts,
- Organisation von Schulungen und Übungen, in denen sicherheitsrelevante Informationen vermittelt, das richtige Verhalten der Mitarbeiter im Hinblick auf Gefahren erläutert und geübt sowie auf diese Weise Akzeptanz für Sicherheitsmaßnahmen geschaffen wird,
- operative Kontrolle, d. h. Überprüfung der Umsetzung des Sicherheitskonzepts, der Durchführung der geplanten Maßnahmen, der Einhaltung der Sicherheitsrichtlinien sowie der Wirksamkeit der umgesetzten Sicherheitsmaßnahmen.

[15]

Das Sicherheitsmanagement hat die folgenden Schutzziele:

- Integrität - Die Information erreicht den Empfänger unverändert.
- Authentizität - Die Information stammt wirklich vom angegebenen Absender.
- Vertraulichkeit - Die Information kann nur der vorgesehene Empfänger lesen.
- Verfügbarkeit - Die Kommunikation zwischen Absender und Empfänger ist unbeeinträchtigt.
- Anrechenbarkeit - Das Absenden beziehungsweise Empfangen einer Nachricht kann unbestreitbar nachgewiesen werden.

[16]

Nach der Aufstellung eines Sicherheitsmanagementkonzepts ist der Bereich Sicherheitsmanagement jedoch noch nicht abgeschlossen. IT-Sicherheit ist ein Prozess bei dem auf neue Bedrohungen auch entsprechend reagiert werden muss. Deshalb sollte IT-Sicherheit ein kontinuierlicher Prozess innerhalb des Unternehmens sein. Eine Schulung der Mitarbeiter sollte in regelmäßigen Abständen durchgeführt werden. Die Mitarbeiter sollten vor allem auf neue Techniken und neue Gefahren aufmerksam gemacht werden. Vor allem im Hinblick auf die Einführung neuer Techniken sollten die Mitarbeiter entsprechend darauf vorbereitet werden. Jedem Mitarbeiter sollte bewusst sein, das Sicherheitsmanagement jeden etwas angeht.

2.1.1 Sicherheitsmanagement in Cloud Computing

Im Cloud Computing spielt das Sicherheitsmanagement eine ebenso wichtige Rollen, wie bei den technischen Lösungen die vor dem Cloud Computing genutzt wurden. Schon bei der Auswahl eines Anbieters sollte darauf geachtet werden, dass der Anbieter den eigenen Anforderungen im Sicherheitsmanagementkonzept entspricht und das dieses gegebenenfalls entsprechend angepasst werden muss. Besonders im Bereich der Risikoanalyse müssen entsprechende Änderungen vorgenommen werden. Durch das Konzept des Cloud Computing werden neue Risiken im Unternehmensablauf eingegangen. Es muss geprüft werden welche Daten überhaupt in der Cloud abgelegt werden dürfen und welche nicht. Wie die Zugriffssicherheit gewährleistet werden kann. Wo und wie die Daten abgelegt werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI))hat sich mit dem neuem Paradigma Cloud Computing befasst und ein Eckpunktepapier veröffentlicht, welches die Mindestanforderungen an einen Cloud-Anbieter definieren soll. [18] Für die Zukunft ist eine Zertifizierung für Sicherheit in der Cloud angedacht. Ein führendes Unternehmen in der Forschung über Sicherheitsmanagement in der Cloud ist KuppingerCole. Das von Martin Kuppinger geführte Unternehmen hat 10 Regeln für die Sicherheit in der Cloud veröffentlicht, welche den Umgang mit Sicherheitsmanagement beim Cloud Computing etwas genauer definieren.

1. Durchgängige Richtlinien und Prozesse für die Informationssicherheit: Es gibt nicht die interne und die externe Informationssicherheit! Es muss einen konsistenten Ansatz mit

organisatorischem Rahmen, Regelwerken, Richtlinien und Prozessen für die gesamte IT geben.

2. Risikoorientierte Vorgehensweise und Schutzbedarfsanalyse: Die Entscheidung darüber, wo welche Informationen liegen und welche spezifischen Anforderungen an Cloud Provider zu stellen sind, muss strukturiert erfolgen. Das geht nicht ohne ein Risikomanagement-Konzept und es geht nicht ohne Schutzbedarfsanalyse.

3. Strukturierte, risikoorientierte Prozesse für die Auswahl von Dienstanbietern: Die Auswahl von Cloud Providern muss standardisiert und zentralisiert erfolgen. Sie darf nicht dezentral und unkoordiniert vorgenommen werden.

4. Klar definierte Service Level Agreements: Was die Anbieter zu liefern haben, muss vorab definiert sind (eindeutig und messbar).

5. Nachvollziehbarkeit der Service-Erbringung und -Qualität: Entsprechend muss auch gemessen werden, was die Anbieter liefern.

6. Gezielte Verschlüsselung von Transportwegen und Informationen: Dort, wo eine Verschlüsselung machbar ist und wo sie aufgrund des Risikos erforderlich ist, muss sie auch umgesetzt werden.

7. Durchgängiges Identitäts- und Berechtigungsmanagement: Das Management von Benutzern und Autorisierungsregeln muss konsistent sein. Standards wie SAML, SPML oder XACML helfen dabei. Noch wichtiger ist aber das Konzept dahinter.

8. Management und Kontrolle von privilegierten Benutzern: Privilegierte Zugriffe müssen kontrolliert werden und das nicht nur in der Cloud. Was können die Operatoren und Administratoren machen? Und welche potenziellen Schäden können die privilegierten Benutzer des Cloud Providers anrichten?

9. Nutzung von Anonymisierungs- und Maskierungstechnologien: Nicht immer müssen die echten Daten in der Cloud liegen. Neue Technologien im Bereich der Anonymisierung und Maskierung von Daten gewinnen an Gewicht.

10. Vordefinierte Fallback- und Migrationsszenarien: Schließlich muss man die Daten auch zuverlässig und vollständig zurück bekommen. Das hat auch mit Sicherheit und nicht nur mit Verfügbarkeit zu tun, weil dazu von vornherein die Regeln gehören, die sicherstellen, dass keine Daten beim Provider verbleiben.

[17]

Die oben genannten Regeln sollten bei dem Umstieg beziehungsweise bei der Nutzung von Cloud Computing beachtet werden. Viele Regeln sind von organisatorischer Art und nicht von technischer Art. Die technische Umsetzung wird vor allem durch ein Identitätsmanagement und ein Credential Management erbracht. Diese Bereiche werde ich im weiteren Verlauf meiner Arbeit genauer betrachten. Darüber hinaus sollten Daten nicht nur während des Transports sondern auch in der Cloud verschlüsselt werden.

Zusätzlich zu den besonderen Regeln für Sicherheit im Cloud Computing sollten natürlich auch die anderen Anforderung an ein Sicherheitsmanagement erfüllt werden.

2.2 Identitätsmanagement in Cloud Computing

Identitätsmanagement befasst sich mit der Speicherung, Prüfung und Verwaltung von digitalen Identitäten. Identitäten sind eine Sammlung von Attributen einer Einheit. Unter einer Einheit können Menschen, Maschinen oder Gegenstände fallen. Der genaue Zusammenhang wird in der Grafik 2.1 aufgezeigt.

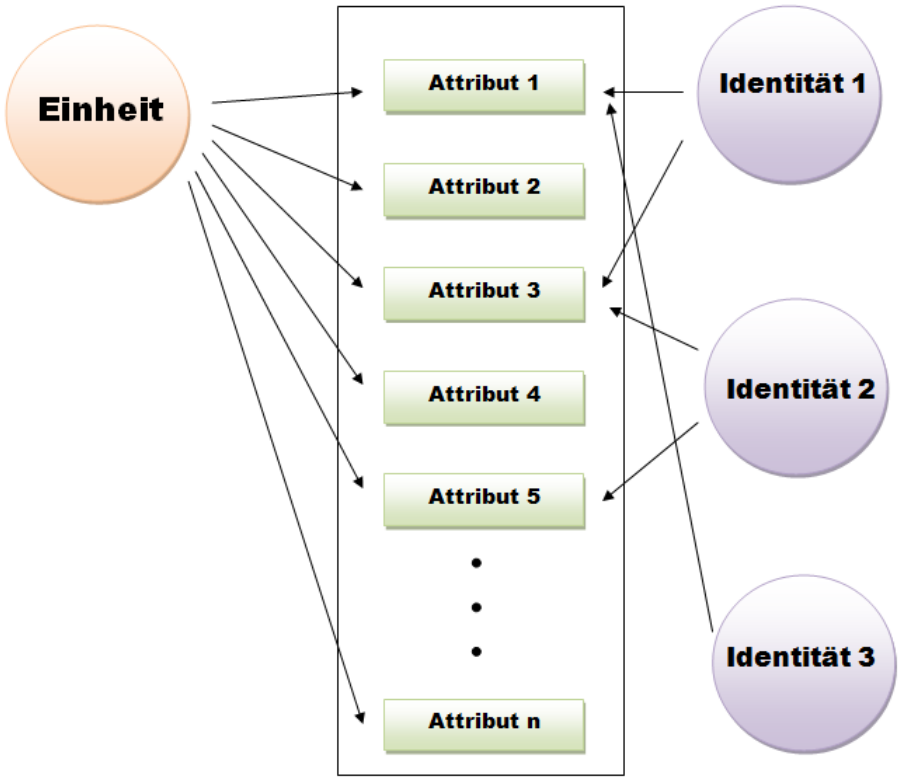

Abbildung 2.1: Zusammenhang zwischen Einheit, Attributen und Identitäten (eigene Abbildung)

Aufgaben des Identitätsmanagement sind:

- Verwaltung von Identitäten
- Authentifizierungsprozess einer Einheit (Entität)
- Authentisierung von Einheiten
- Rollenmanagement
- Protokollierung

Die Anforderungen an das Identitätsmanagement sind abhängig vom Sicherheitskonzept. Falls man sich zum Beispiel auf eine *starke Authentifizierung* festgelegt hat, dann muss

das Identitätsmanagement diese auch unterstützen. Unter einer *starken Authentifizierung* versteht man, dass ein Nutzer mindestens zwei Schlüssel haben muss um Zugriff auf die gewünschten Ressourcen zu bekommen. Es wird etwas was man weiß und etwas was man hat abgefragt. Zu den Punkten die man weiß zählen: Passwörter und Pins. Etwas was man hat, kann zum Beispiel eine Chipkarte, das Mobiltelefon oder Fingerabdruck sein.

Durch das Identitätsmanagement sollten alle getätigten Aktionen protokolliert werden.

2.2.1 Protokolle zur Übertragung von Identitätsdaten

2.2.1.1 SAML

SAML steht für Security Assertion Markup Language. Es wurde von OASIS Security Services Technical Committee (SSTC) entwickelt und 2002 in Version 1.0 veröffentlicht. Es handelt sich dabei um eine XML basierte Sprache zum Austausch von Identitätsdaten zwischen Sicherheitsdomänen. Der Standard wurde vorwiegend zur Lösung des Single-Sign-On- Usecases entwickelt. Die bis dahin vorliegenden Lösungen wurden über Cookies im Web-Browser realisiert, die aber nicht die gewünschte Sicherheit lieferten. Das folgende Sequenzdiagramm 2.2 veranschaulicht den Usecase.

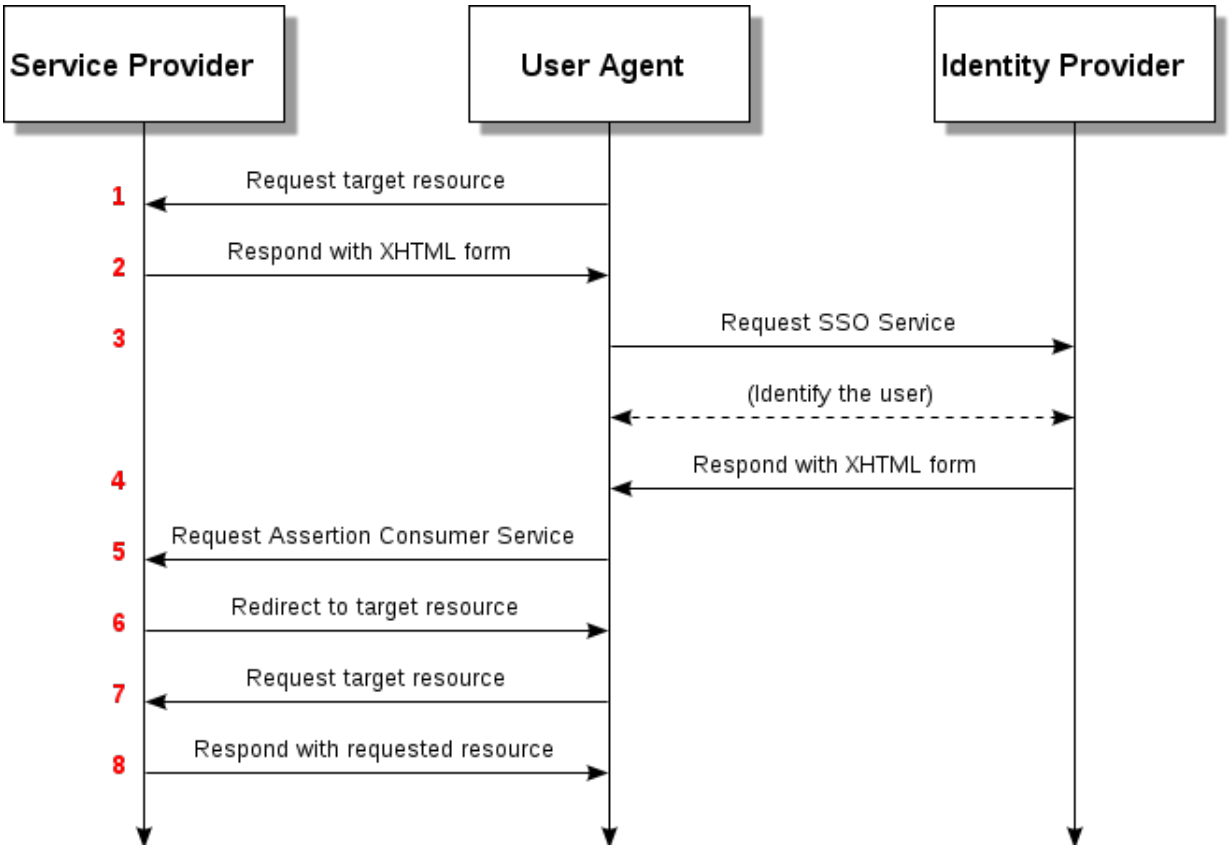

Abbildung 2.2: SAML Usecase [12]

Der Security Assertion Markup Language (SAML) 1.0 Standart wurde von der *Liberty Alliance*, ein Zusammenschluss von Firmen, Non-Profit- und Regierungsorganisation,

durch Liberty Identity Federation Framework (LIFF) erweitert. Dieses Framework beinhaltet die gleichen Funktionen wie SAML 1.0 wurde aber um den sogenannten *Circle of Trust*, zu deutsch *Kreis des Vertrauens*, erweitert. Der *Circle of Trust* repräsentiert einen Zusammenschluss von Sicherheitsdomänen in denen sich die einzelnen Domänen untereinander vertrauen und die gleichen Standards benutzen. Im Jahr 2003 wurde SAML 1.1 Standard veröffentlicht. Dieser Standard wurde von den meisten Identitätsmanagementsystemen unterstützt. Im September 2005 würde der SAML 2.0 Standard veröffentlicht. Der Standard vereint die Konzepte von SAML 1.1, Shibboleth und LIFF.

2.2.1.2 SOAP

SOAP ist die Abkürzung für Simple Object Access Protocol. Das Protokoll entstand als Weiterentwicklung vom XML-RPC, welches von Microsoft und Dave Winer 1998 veröffentlich und 1999 in der Version 0.9 heraus gebracht wurde. Der Aufbau einer Simple Object Access Protocol (SOAP)-Nachricht entspricht dem folgenden Muster:

```
<?xml version="1.0"?>
<s:Envelope xmlns:s="">
    <s:Header>
    </s:Header>
    <s:Body>
    </s:Body>
</s:Envelope>
```

[13]

Das Protokoll wird zur Koppelung von Systemen verwendet. Das sehr flexible Format bringt Nachteile in Form von Rechenaufwand bei der Generierung und Auswertung und durch die Größe, die im Vergleich zu den übertragenen Informationen sehr groß ist, mit sich.

2.2.1.3 WS-*

Bei *WS-** handelt es sich nicht um einen einzelnen Standard sondern um einen Sammelbegriff für alle Standards, die nach dem Muster "WS-*" benannt wurden. Bei der Entwicklung dieser Standards wurde nach zwei Grundprinzipien verfahren: Zusammensetzbarkeit und Interoperabilität. Zusammensetzbarkeit bedeutet, dass sich beliebige WS-* Standards gemeinsam nutzen lassen und Interoperabilität, dass sich durch Nutzung der Standards Systeme über Domänengrenzen hinaus errichten lassen. Es gibt 150 verschiedene WS-* Standards. Anbei eine Auflistung einiger dieser Standards.

- WS-Federation
- WS-Policies

- WS-Security
- WS-Trust

Die WS-* Protokolle legen ihre Daten in den Headern von SOAP-Nachrichten ab.

2.2.1.4 Shibboleth

Bei Shibboleth handelt es sich um einer Erweiterung des SAML-Protokolls und dient zur Authentifizierung und Autorisierung für Webanwendungen und Webservices. Die Software unterteilt sich in drei Bereiche:Identity Provider (IdP), Service Provider (SP) und optional einen Lokalisierungsdienst. Es sind mindestens ein IdP und ein SP gefordert, dass Shibboleth funktionieren kann. Die Kommunikation zwischen Identity Provider und Service Provider erfolgt über SAML. Der Ablauf einer Shibboleth Autorisierung erfolgt in fünf Schritten:

1. Eine Benutzer versucht Zugriff auf eine geschützte Ressource zu erlangen.

2. Der Service Provider ermittelt den Identity Provider oder gibt dem Benutzer die Möglichkeit diesen aus einer Liste zu wählen.

3. Der Service Provider sendet eine Authentifizierunganfrage an den Identity Provider. Der Benutzer authentifiziert sich.

4. Der Identity Provider stellt eine Zusammenstellung von Attributen des authentifizierten Benutzers zusammen. Bei der Authentifizierunganfrage war eine Liste der benötigten Attribute dabei. Die Daten werden in einer SAML Nachricht zusammen gefasst und an den Service Provider gesendet.

5. Der Service Provider entschlüsselt die Nachricht und wertet die Information aus. Zusätzlich werden eine Sicherheitskontrollen durchgeführt. Sollte die Prüfung positiv sein, wird eine Benutzersession angelegt und der Nutzer bekommt Zugriff auf die angeforderte Ressourcen.

2.2.2 Ping-Identity

Der Dienstanbieter Ping-Identity bietet zwei unterschiedliche Lösungen für das Identitätsmanagement an. Diese Lösung lässt sich mit wenig Aufwand in bestehende Firmennetzwerke implementieren.

2.2.2.1 PingFederate

Der von PingIdentity angebotene Dienst PingFederate liefert die folgenden drei Services:

- Internet Single-Sign-On

- Internet User Account Management
- Secure Web APIs

Durch diese drei Services wird ein Rundumpaket für Identitätsmanagement geliefert.

Internet Single-Sign-On

Dieser Service ermöglicht es dem Nutzer durch einmaliges Einloggen Zugang zu allen angeschlossenen Diensten zu erhalten. Der Nutzer meldet sich einmalig beim IdP an und kann danach alle Dienste der zugehörigen SP nutzen. Der Austausch von Daten zwischen IdP und SP erfolgt über SAML oder WS-Federation Standard. Der genaue Ablauf wird im Abschnitt *Ablauf des Zugriffs und der Authentifizierung* erklärt.

Internet User Account Management

Das *User Account Management* ist für die Speicherung und Verwaltung aller Benutzerdaten zuständig. Hierzu werden beim Einrichten des Dienstes Datenbanken in einer sicheren Zone des IdP angelegt. Das Anlegen der Datenbank erfolgt automatisch durch *Ping Federate*. Es ist möglich bestehende Nutzerdaten zu integrieren. Durch die automatische Erstellung und Verwaltung der Benutzerdaten wird der administrative Aufwand verkleinert und die Sicherheit des Netzes erhöht.

Viele Cloud-Computing Dienste besitzen eigene Verzeichnisdienste, die von außerhalb nicht erreichbar sind. Da für die Nutzung dieser Dienste die Nutzer über einen Eintrag im Verzeichnisdienst des Dienstes verfügen müssen, bietet das *User Account Management* Möglichkeiten um diesen zu erzeugen. Dier Dienst bietet die *Express Provisioning* und *SaaS Provisioning*. Bei *Express Provisioning* handelt es sich um eine SP-seitige Lösung. Bei Nutzung eines Clouddienstes werden die entsprechenden Verzeichnisdiensteinträge erstellt, falls diese noch nicht vorhanden sind. Die erforderlichen Daten werden über SAML vom IdP and den SP übertragen. Die zweite Lösung *SaaS Provisioning* ist IdP-seitig und sorgt dafür, dass bei bei neuen Nutzern die entsprechenden Einträge bei den Verzeichnisdiensten der einzelnen Anwendungen erstellt werden. Die zweite Lösung bietet den Vorteil, dass bei Löschung von Accounts oder Änderung von Nutzerrechten die entsprechenden Einträge in den Verzeichnisdiensten der einzelnen Anwendungen auch gelöscht werden.

Secure Web APIs

Der Service *Secur Web APIs* bietet verschiedene Schnittstellen zur Übertragung Identitätsdaten. Ein Bestandteil der *Secure Web APIs* sind die *Secure Token Services*. Diese Dienste sind für die Kommunikation zwischen IdP und SP zuständig. Wenn die Systeme unterschiedliche Standards bei der Identitätsdatenübertragung nutzen, werden die Identitätsdaten durch sog. *Security Token Translators* in SAML und zurück übersetzt. Somit werden auch Portale und Anwendungen unterstützt die standardmäßig kein SAML unterstützen. Darüber hinaus werden *Software Developement Kits* angeboten, die es ermöglichen zusätzlich zu den von *Ping Federate* angebotenen *Security Token Translators* eigene Übersetzer zu erstellen.

Ablauf des Zugriffs und der Authentifizierung

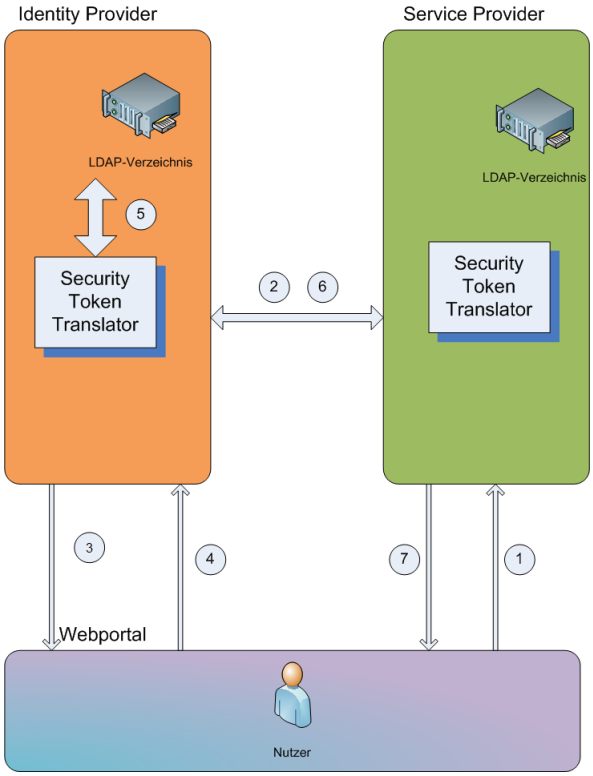

Abbildung 2.3: Ablauf des Zugriffs und der Authentifizierung (eigene Abbildung)

Anhand der Grafik 2.3 werde ich den Ablauf des Zugriffs auf einen Clouddienst mit der dazugehörigen Authentifizierung erklären.

1. Der Nutzer fordert über das Webportal die Nutzung des Clouddienstes an. Dies wird über einen HTTPS Aufruf an den SP realisiert.
2. Anhand dieses Aufrufes erkennt das System, ob der Nutzer sich bereits einmal angemeldet hat (weiter mit Schritt 6) oder sich erstmalig anmeldet.
3. Das System leitet den Nutzer auf das Anmeldeportal des IdP weiter.
4. Der Nutzer gibt die Anmeldedaten ein.
5. Der IdP überprüft die Anmeldedaten und übersetzt die gegebenenfalls durch den *Security Token Translator*
6. Die Daten werden durch den Authentifizierungsendpunkt an den SP weitergeleitet
7. Der Benutzer erhält Zugriff auf den angeforderten Dienst.

Nach einer erfolgreichen Authentifizierung ist keine weitere nötig um Zugriff auf die Dienste zu bekommen. Während dieses Ablaufs werden auch, falls erforderlich, entsprechende Einträge im Verzeichnisdienst des Dienstes erstellt wie im Abschnitt *Internet User Account Management* erwähnt.

Weitere Funktionen *PingFederate* bietet zu den bereits vorgestellten Funktionalitäten noch weitere Dienste an. Alle getätigte Aktionen werden automatisch protokolliert. Dies erhöht die Sicherheit und bietet die Möglichkeit zu prüfen wer wann Zugriff auf welche Dienste und Daten hat. Der Administrator hat die Möglichkeit festzulegen welche Aktionen protokolliert werden und kann die Daten einsehen und daraus Berichte erstellen. Darüber hinaus bietet *PingFederate* sog. *Cloud Identity Connectors*, die eine Schnittstelle zu Diensten wie Facebook, Google, Yahoo oder AOL bilden, um diese als Cloud Identity Provider zu nutzen.

PingConnect

Der Dienst *PingConnect* hat ähnlich Funktionen wie *PingFederate*, ist jedoch ein Service on Demand. Zu Nutzung dieses Dienstes werden keine eigenen Hardwareressourcen benötigt. Die Nutzer des Dienstes benötigen nur einen Account und bekommen somit Zugriff auf alle in das System eingepflegten Dienste. Das *User Account Management* ist in den Dienst integriert und sorgt dafür, dass die Anwendungen alle erforderlichen Daten erhalten. Bisher unterstützt der der Dienst *PingConnect* bereits bis zu 60 Software as a Service (SaaS) Anbieter. Der Ablauf wird in der folgenden Abbildung 2.4 verdeutlicht.

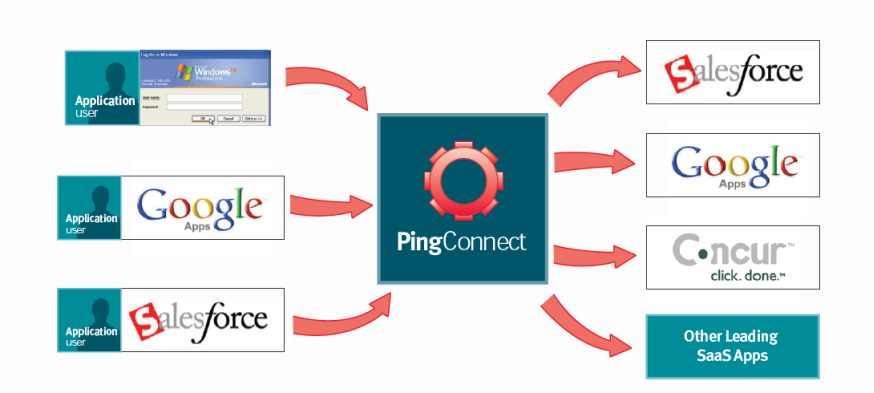

Abbildung 2.4: Ping Connect [10]

2.2.3 OpenID

Bei dem Dienst OpenID handelt es sich um ein dezentrales Identitätssystem. Die Nutzer des Dienstes können sich mit einem Benutzernamen und einem Passwort bei allen Diensten anmelden, die OpenID unterstützen. Der Nutzer kann sich bei neuen Diensten mit seinem Benutzernamen und Passwort einmalig registrieren. Der Nutzer kann selbst frei entscheiden, welche Nutzerdaten an die einzelnen Dienste übertragen werden. Bei der Änderung von persönlichen Daten, müssen diese nur bei dem OpenID-Provider geändert werden und nicht bei den einzelnen Diensten. Eine OpenId-Identität ist nach dem folgenden Muster aufgebaut: *benutzername.example.com*. Das OpenId-Protokoll ist ein freies Protokoll, welches von verschiedenen Firmen umgesetzt wurde. Deshalb existieren eine Vielzahl unterschiedlicher OpenId-Provider zum Beispiel: MyOpenID.comm Yahhoo!, Blogger.com oder Google. Das Verfahren ist anfällig für Phishingattacken. Deshalb sollte bei der Nutzung die Echtheit der Anmeldeseite durch den Nutzer geprüft werden.

[25] [26]

2.2.4 FireID

FireID ist ein führendes Unternehmen für Authentifizierung für Webanwendungen. Das Unternehmen bietet Techniken für eine starke Authentifizierung bei Nutzung von gewöhnlichen Mobiltelefonen. FireID unterstützt Einmal-Passwörter und Hardware-Token. Die Einmal-Passwörter können entweder auf dem eigenen Mobiltelefon generiert werden oder per SMS an dieses gesendet werden. Die Anwendung wird schon für eine Vielzahl an unterschiedlichen Mobiltelefonen angeboten. Für die Generierung der Schlüssel mit dem Mobiltelefon muss keine Verbindung zum Handynetz bestehen. FireId bieter auch die Software für die Verwalten der Schlüssel. Somit ist man unabhängig, was die Wahl es Ortes angeht. Somit wird nach dem Muster *etwas was man weiß und etwas was man hat* verfahren. Das Authentisierungsverfahren kann leicht in die bestehende Infrastruktur eingebunden werden.

2.3 Credential Management

Unter Credential Management versteht man die Verwaltung von Berechtigungsnachweisen. Ein Berechtigungsnachweis wird für die Authentifizierung von Benutzern oder Systemen gegenüber anderen Systemen verwendet. Dafür werden meist eine Benutzerkennung und ein oder mehrere weitere Berechtigungsnachweise verwendet. Zu den Berechtigungsnachweise zählen zum Beispiel Ausweispapiere, Zeugnisse, Passwörter oder auch Ergebnisse kryptografischer Verfahren. Darüber hinaus können auch Chipkarten oder technische Geräte verwendet werden. Das Credential Management sollte vor dem Zugriff durch den Cloudanbieter geschützt sein. Der Nutzer sollte Berechtigungen entfernen, erstellen und bearbeiten können. Nach der Löschung beziehungsweise Deaktivierung von Berechtigungen dürfen diese nicht mehr für die Authentifizierung akzeptiert werden.

2.4 Verschlüsselung in der Cloud

Identitätsmangement und Credential Management sind nicht ausreichend um eine sichere Cloud zu bekommen. Besonders der Punkt Datenschutz steht noch im Raum. Ein Unternehmen kann nicht davon ausgehen, dass wenn die Daten in Cloud gelöscht werden, diese auch wirklich weg sind. Es besteht die Möglichkeit, dass nur der Verweis auf diese gelöscht wurde under beziehungsweise oder noch Backups von den Daten existieren. Deshalb sollten die Daten verschlüsselt in der Cloud abgelegt werden. Die Firma Trend Micro bietet den Service *SecureCloud* als SaaS an, der die Verschlüsselung der Daten in der Cloud ermöglicht. Der Service unterstützt 128,156 und 192 Bit AES Verschlüsselung. Es werden zur Zeit die folgenenden Cloud Anbieter unterstützt: Amazon EC2, Eucalyptus, vCloud und TCloud.

2.5 Umsetzung bei Amazon

Die Amazon Web Services wurden erfolgreich einer SAS70-Prüfung unterzogen. Der Zugang von Mitarbeitern in die Rechenzentren wird streng kontrolliert und durch zweifache Zwei-Faktor-Authentifizierungen sichergestellt. Der Zutritt ist den Mitarbeitern nur mit einem legitimen Geschäftsgrund gestattet. Sobald dieser nicht vorliegt, werden die Zugriffsberechtigungen wieder entzogen. Somit ist physische Sicherung der Infrastruktur sichergestellt.

Amazon bietet den Kunden von Clouddiensten das *AWS Identity and Access Management* an. Dieses Modul fasst Identitätsmanagement und Credential Management zusammen. Das AWS IAM bietet Unternehmen die Möglichkeit unter Nutzung von nur einem AWS-Konto mehrere Benutzer anzulegen. Die wichtigsten Funktionen sind:

- Benutzer verwalten - Benutzer erstellen, löschen und auflisten
- Gruppen verwalten - Gruppen erstellen, löschen, auflisten und Benutzer zuweisen
- User-Sicherheitsnachweise verwalten - AWS Access Key, X.509 Zertifikat, Kennwort, Multi-Factor Authentication (MFA)-Gerät
- Benutzerberechtigungen festlegen - die Fähigkeit von Einzelpersonen oder Gruppen zum Aufrufen von Web Service APIs oder spezifischen Ressourcen wie S3 Buckets, SQS Warteschlangen, SimpleDB Domänen usw. steuern.
- Benutzerzugriffe auf Amazon Web Services zulassen - Daten unter Kontrolle des AWS-Kontos erstellen, unter dem der Benutzer erstellt wurde.

[19]

Für die einzelnen Benutzer können unterschiedliche Sicherheitsnachweise festgelegt werden. AWS IAM kann derzeit mit den folgenden Diensten genutzt werden: Amazon EC2, Amazon S3, Amazon VPC, Amazon SQS, Amazon SNS, Amazon RDS, Amazon SimpleDB, Auto Scaling und Elastic Load Balancing. Bei der derzeit angebotenen Version handelt es sich noch um eine Preview-Beta, die noch keine Protokollierung unterstützt. Dies soll aber bei zukünftigen Versionen durchgeführt werden.

Jede Benutzer hat einen Zugriffsschlüssel (Access Key) und einen geheimen Zugriffsschlüssel (Private Access Key). Mit diesem Schlüsselpaar werden die Anfragen an die Web-Dienste erstellt. Der Zugriffsschlüssel ist dabei öffentlich und wird für die Identifizierung genutzt. Mit dem geheimen Zugriffsschlüssel wird aus der Anfrage und dem geheimen Schlüssel eine Signatur berechnet. Diese Signatur wird zusammen mit der Anfrage und dem Zugriffsschlüssel an den Dienst übermittelt. Somit wird sichergestellt das die Anfrage bei der Übertragung weder verändert noch gefälscht wurde. Eine Anfrage kann so eindeutig einem Kundenkonto zugeordnet werden. Man kann eine automatische Schlüsselrotation einstellen um in einem festen Intervall neue Schlüssel generieren zu lassen. Amazon schlägt dafür ein Intervall von 90 Tagen vor. Neben den vorher beschrieben Zugriffsschlüsseln gibt es noch Schlüsselpaare für EC2 und CloudFront. Diese Schlüsselpaare bestehen jeweils aus einem privatem und einem öffentlichem Schlüssel.

Amazon bietet derzeit noch nicht für alle Dienste eine Verschlüsselung der Daten an, dies kann jedoch über den Service *SecureCloud* von TrendMicro durchgeführt werden. Amazon bietet auch eine Multi-Faktor-Authentifizierung an. Dabei werden Geräte von Gemalto genutzt, die die Einmal-Passwörter generieren. Somit ist auch bei den Amazon Web Services eine starke Authentifizierung gesichert. Zusammen mit der Verschlüsselungssoftware von TrendMicro kann Amazon eine durchaus sichere Cloudumgebung liefern.

Nach einer genaueren Analyse der White-Paper von den Amazondiensten ist mir eine Sache besonders aufgefallen:

> Wird ein Objekt aus Amazon S3 gelöscht, wird die Zuordnung zwischen dem öffentlichen Namen und dem Objekt sofort gelöscht. Dieser Vorgang wird normalerweise innerhalb weniger Sekunden im gesamten verteilten System durchgeführt. Sobald die Zuordnung gelöscht ist, besteht kein Fernzugriff mehr auf das gelöschte Objekt. Der so gewonnene Speicherplatz wird dann wieder vom System verwendet.

[20]

Somit wird bei der Löschung von Daten nur der Verweis auf diese gelöscht. Die Daten befinden sich jedoch weiterhin für eine unbestimmt Zeit in der Cloud. Erst ein Überschreiben der Daten löscht diese dauerhaft. Dieser Punkt sollte besonders beachtet werden, falls sich für die Lösung von Amazon entschieden wird. Man sollte deshalb die Daten nur verschlüsselt abspeichern.

> F: Werden mit Amazon S3 die Datenschutzbestimmungen der EU eingehalten?
> In der Region EU (Irland) gespeicherte Objekte verlassen die EU nicht, es sei denn, sie werden durch Sie selbst übertragen. Dennoch liegt es in Ihrer Verantwortung, sicherzustellen, dass Sie die Datenschutzbestimmungen der EU einhalten.

[21]

Wie das oben angegebene Zitat zeigt übernimmt Amazon keine Verantwortung für die Durchsetzung des Datenschutzes. Es ist aber sichergestellt, dass die Daten an einem vorher bestimmten Ort verbleiben. Auch aus diesem Grund sollten die Daten zusätzlich durch eine Verschlüsselung geschützt werden.

2.6 Fazit

Der Umstieg auf eine cloudbasierte Technik sollte wohl überlegt geschehen und die Tragweite einer solchen Entscheidung sollte dem Unternehmen bewusst sein. Der Umstieg muss in das Sicherheitsmanagement des Unternehmens eingearbeitet werden. Mit den derzeit auf dem Markt angebotenen Lösungen kann ein sicherer Zugriff auf Ressourcen in der Cloud gewährleistet werden. Selbst wenn Daten unter das Bundesdatenschutzgesetz fallen,

können diese durch Verschlüsselung vor dem unbefugten Zugriff geschützt werden. Durch geeignetes Identitätsmanagement, Credential Management und Verschlüsselung kann das Cloud Computing sogar hohen Sicherheitsanforderung nachgekommen. Das BSI arbeitet noch an einer Zertifizierung für Cloud-Anbieter. Diese Zertifizierung soll in die Norm ISO 27001 eingearbeitet werden. Sobald solch ein Zertifikat existiert sollte natürlich auch auf die Zertifizierung geachtet werden bei der Auswahl des Anbieters.

Meiner Ansicht nach keine bei Beachtung der im Bereich Sicherheitsmanagement aufgeführten Regeln ein sichere Nutzung der Cloud gewährleistet werden und einem Umzug der Dienste in die Cloud steht nicht entgegen. Besonders für kleinere Unternehmen eröffnen sich durch die Cloud neue Welten. Eine Erweiterung der Infrastruktur kann durch Cloud Computing ohne hohe Kosten durchgeführt werden. Die Sicherheit kann auf dem gleichen Level beibehalten werden.

Im Mai 2011 wird die *Eurepean Identity Conference* in München stattfinden bei der die führenden Hersteller zusammen neue Lösungsansätze vorstellen werden. Ein Thema welches dort behandelt wird ist: *"In Cloud we Trust" - kein Cloud Computing ohne Vertrauen und ohne solide Strategie für die Informationssicherheit.*

Am Beispiel der Amazon Web Services ist klar erkennbar, dass die angebotenen Techniken für Cloud Computing durchaus schon nutzbar sind ohne große Einschnitte im Bereich Sicherheit einzugehen.

Literaturverzeichnis

[1] Wikipedia - Identitätsmangement http://de.wikipedia.org/wiki/Identit%C3%A4tsmanagement, 10.02.2011

[2] Jens Pälmer, *Privileged User Management schützt Firmen vor ihren Admins* , http://www.searchsecurity.de/themenbereiche/identity-und-access-management/user-management-und-provisioning/articles/258071/index2.html24.02.2011

[3] Digital Identity Glossary, http://blog.onghome.com/glossary.htm, 24.02.2011

[4] Frederik Weishaeupl, *Interoperabilitätsanalyse föderierter Identitätsmanagement-Systeme*, Diplomarabeit, LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN, http://www2.pms.ifi.lmu.de/publikationen/diplomarbeiten/Frederik.Weishaeupl/DA_Frederik.Weishaeupl.pdf

[5] Institut für Internet-Sicherheit, http://www.internet-sicherheit.de/forschung/aktuelle-forschungsprojekte/identity-management/ 24.02.2011

[6] Wolfgang Hommel, Helmut Reiser *Federated Identity Management: Die Notwendigkeit zentraler Koordinationsdienste*, http://www.mnm-team.org/pub/Publikationen/hore05/PDF-Version/hore05.pdf

[7] Antonio Celesti, Francesco Tusa, Massimo Villari and Antonio Puliafito, *Security and Cloud Computing: InterCloud Identity Management Infrastructure*, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5541971

[8] Ping Federate - Productguide http://www.pingidentity.com/support-and-downloads/downloads/6B54C707-C293-2D59-A2980CF0967760D6/PingFederate-Product-Guide-2010.pdf, 24.02.2011

[9] Ping Federate - Datasheet http://www.pingidentity.com/support-and-downloads/downloads/6B539D78-C293-2D59-A64994980878AC08/PingFederate_6-4_DataSheet.pdf, 24.02.2011

[10] Ping Connect http://www.pingidentity.com/our-solutions/pingconnect.cfm, 24.02.2011

[11] Anu Gopalakrishnan, *Cloud Computing Identity Management*, http://www.infosys.com/research/publications/setlabs-briefings/Documents/cloud-computing-identity-management.pdf, 24.02.2011,

[12] Wikipedia, *Security Assertion Markup Language* http://de.wikipedia.org/wiki/Security_Assertion_Markup_Language 24.02.2011

[13] Wikipedia *SOAP*, http://de.wikipedia.org/wiki/SOAP, 21.02.2011

[14] Tobias Mogk, *Analyse und Modellierung einer Collaborative Cloud Umgebung*, Bachelorarbeit, Universität der Bundeswehr München

[15] Wikipedia - Sicherheitsmanagement http://de.wikipedia.org/wiki/Sicherheitsmanagement, 14.03.2011

[16] Dr. Christoph Thiel, *IT-Sicherheitsmanagement* http://www.competence-site.de/downloads/e4/e2/i_file_4818/it_sicherheitsmanagement.pdf, 14.03.2011

[17] Martin Kuppinger, *10 Grundregeln für mehr Sicherheit beim Cloud Computing* http://www.kuppingercole.com/articles/mk_cloud_regel_sicherheit28022011, 14.03.2011

[18] Bundesamt für Sicherheit in der Informationstechnik, *BSI-Mindestsicherheitsanforderungen an Cloud-Computing-Anbieter* , https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Sonstige/Cloud_Computing_Mindestsicherheitsanforderungen.pdf?__blob=publicationFile#download=1, 15.03.2011

[19] Amazon, *AWS Identity and Access Management (IAM)* , http://aws.amazon.com/de/iam/, 15.03.2011

[20] Amazon - Whitepaper, *Amazon Web Services - Sicherheitsprozesse im Überblick*, http://awsmedia.s3.amazonaws.com/de/Whitepaper_AWS_Security_Whitepaper(DE).pdf, 14.03.2011

[21] Amazon - S3 FAQ, *Amazon Simple Storage Service - Häufig gestellte Fragen*, http://aws.amazon.com/de/s3/faqs/#Can_I_comply_with_EU_data_privacy_regulations_using_Amazon_S3, 14.03.2011

[22] FireId, *Two-Factor Authentication*, http://www.fireid.com/solutions/two-factor-authentication.html, 18.03.2011

[23] Justin Stanford, *FireID goes SaaS with FireID Cloud Services*, http://www.justinstanford.com/2010/01/fireid-goes-saas-with-fireid-cloud-services/, 18.03.2011

[24] TrendMicro, *Trend Micro SecureCloud*, http://us.trendmicro.com/us/solutions/enterprise/security-solutions/virtualization/securecloud/, 18.03.2011

[25] OpenID - was muss man darüber wissen?, http://www.agenturblog.de/2007-03/openid-was-muss-man-darueber-wissen/, 15.03.2011

[26] OpenID - Spezifikation, http://openid.net/specs/openid-authentication-2_0.html, 15.03.2011

Kapitel 3

Untersuchung und Bewertung von Security-as-a-Service-Diensten

Pascal Staudenrauß

Security-as-a-Service (SecS-Dienste), als Teil von Software-as-a-Service (SaaS) des Cloud Computings, bieten Firmen die Möglichkeit die Sicherheit ihrer IT „in die Cloud“ auszulagern. Da zu diesem Thema noch kein einheitlicher Sprachgebrauch existiert, wird zunächst definiert was SecS-Dienste sind und eine Taxonomie entworfen. Anhand dieser Taxonomie werden einige SecS-Dienste untersucht und auf die Frage hin, welche Sicherheitsaufgaben in einem IT-Umfeld denn tatsächlich durch solche Dienste abgedeckt werden, untersucht.

Inhaltsverzeichnis

3.1 Einleitung

3.1.1 Beschreibung der Thematik und Vorgehen

Der Begriff Cloud Computing ist eines der derzeit aktuellsten Themen der IT. In kürzester Zeit wurden zu diesem Thema unzählige Konferenzen abgehalten, wissenschaftliche Abhandlungen verfasst und Blogs gegründet. Außerdem stützen zahlreiche namhafte Anbieter ihre Portale auf Cloud-Architekturen ab: etwa Amazon oder Google. Cloud Computing gilt als neues Paradigma der verteilten Systeme und hat zum Ziel verschiedene Dienste über Netzwerk zu verteilen. Die beliebige Verteilung von Diensten über die Cloud haben die Skalierbarkeit und Dynamik eben dieser zur Folge. Weiterhin sind Ressourcen in der Cloud in der Regel virtualisiert. Dies hat den Vorteil, dass ein Nutzer eine beliebige Sicht auf seine IT-Infrastruktur hat, wodurch systembedingte Abhängigkeiten für Anwendungen entfallen [2]. Dieses neue Paradigma hat jedoch nicht nur technische Ausmaße sondern auch wirtschaftliche, da Cloud Computing den Ideen des Utility Computing folgt. Dabei wird zu jedem Zeitpunkt lediglich die aktuell benötigte Menge an Ressourcen zur Verfügung gestellt und bezahlt. Die weiteren betriebsökonomischen Implikationen, die dadurch entstehen, sind klar.
Diese Seminararbeit beschäftigt sich schwerpunktmäßig mit einem speziellen Aspekt des Cloud Computings, nämlich mit Sicherheitsdiensten (Security-as-a-Service-Diensten) als Teil von Software-as-a-Service (SaaS). Ziel dieser Arbeit ist es, einen einheitlichen Sprachgebrauch zu diesem Thema zu schaffen und einige Dienste bezüglich der Frage, inwiefern solche Dienste eine umfassende Sicherheitslösung für IT-Systeme darstellen, zu untersuchen und zu bewerten. Dazu werden im weiteren Verlauf dieses Kapitels zunächst unterschiedliche Definitionen des Cloud Computings wiedergegeben und die wesentlichen Unterschiede aber auch Gemeinsamkeiten zu den Paradigmen Service-Oriented Computing (SOC) und Grid Computing identifiziert.
In Kapitel 3.2 werden die technischen Grundlagen des Cloud Computings behandelt. Anschließend wird in Kapitel 3.3 eine Definition von Security-as-a-Service-Diensten und eine Taxonomie erarbeitet. Diese Taxonomie ist Grundlage für die Untersuchung und Bewertung derzeitiger Security-as-a-Service-Dienste, welche in Kapitel 3.4 erarbeitet wird.

3.1.2 Was ist Cloud-Computing?

In diesem Abschnitt werden zunächst einige Definitionen des Cloud Computings wiedergegeben und deren Gemeinsamkeiten herausgestellt. Dies ist wichtig, um zu verstehen inwiefern sich die „Cloud“ von anderen Formen des verteilten Rechnens, wie etwa Grid, SOC oder Peer-to-Peer abhebt.

Definition und Charakteristika

Eine erste grobe Definition liefert *wikipedia*. Diese reicht aus, um grob die Charakteristika des Cloud Computings zu erkennen:

> *Cloud Computing (deutsch etwa Rechnen in der Wolke) ist primär der Ansatz, abstrahierte IT-Infrastrukturen (z. B. Rechenkapazität, Datenspeicher-, fertige Software- und Programmierumgebungen als Service) dynamisch an den Bedarf angepasst über ein Netz zur Verfügung zu stellen.*
>
> [Quelle: wikipedia]

Eine weitaus detailliertere Definition, die sowohl die Aspekte Architektur, Sicherheit als auch Verteilungsstrategien berücksichtigt, liefert das National Institute of Standards and Technology (NIST):

> *Cloud computing is a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*
>
> [Quelle: National Institute of Standards and Technology]

Hieraus lassen sich nach [9] nun folgende Schlüssel-Charakteristika des Cloud Computing ableiten:

On-demand self-service: Ein Nutzer kann zu jedem Zeitpunkt und auf Wunsch Ressourcen (wie etwa Rechenzeit, Software, Speicherkapazität usw.) nutzen ohne dass hierfür menschliche Interaktion (etwa mit unterschiedlichen Dienstanbietern) nötig ist.

Bereitstellung über das Netzwerk: Ressourcen werden über ein Netzwerk (bspw. Internet) bereitgestellt und können auf heterogenen Plattformen (etwa unterschiedlichen Endgeräten) genutzt werden.

Ressourcen-Zusammenschluss: Die Ressourcen des Dienstanbieters bilden einen Pool. Jede einzelne Ressource dieses Pools kann dynamisch unterschiedlichen Benutzern zugewiesen werden (Multi-Mandanten-Fähigkeit). Somit „gehört“ die Ressource dem Nutzer nicht. Der Nutzer weiß generell nicht, wo sich diese Ressource befindet, noch hat er Kontrolle hierüber.

Kurzfristige Skalierbarkeit: Die zugewiesene Menge einer Ressource kann je nach Bedarf des Nutzers kurzfristig skaliert werden.

Kostenpflichtig: Die Bereitstellung von Ressourcen ist kostenpflichtig, um die Optimierung der Ressourcen-Nutzung zu fördern.

Vergleich mit Service-Oriented Computing und Grid Computing und Peer-to-Peer

In diesem Abschnitt werden die Beziehungen zwischen Cloud Computing und den Paradigmen Grid Computing und Service-Oriented Computing (SOC) und Peer-to-Peer beschrieben.

Cloud und Grid Computing: Sowohl die Motivation zum Grid Computing als auch der Ansatz zur Umsetzung unterscheiden sich gänzlich vom Cloud Computing. Beim Grid Computing werden Ressourcen gemeinschaftlich genutzt, um reale und fortgeschrittene (wissenschaftliche) Probleme (bspw. aufwändige Berechnungen) effektiv lösen zu können. Eine zentrale Steuerung gibt es hierbei nicht [14]. In der Cloud werden meist mehrere unabhängige Instanzen einer Ressource bereit gestellt. Der Nutzer soll nicht wissen, dass er sich Ressourcen (bzw. Instanzen davon) mit anderen teilt. Während es bei Grid Computing darum geht gemeinschaftlich mehr Kapazitäten (bspw. Speicher oder Rechenleistung) zu erhalten, fokussiert die Cloud den „on-demand self-service".

Cloud und Service-Oriented Computing: Das Paradigma des Service-Oriented Computing (SOC) liefert substantielle Prinzipien für die technische Umsetzung des Cloud Computing, wie etwa die Beschreibung von Web Services über die Web Services Description Language (WSDL) oder die „Service Discovery". Im Gegensatz zu SOC zielt Cloud Computing darauf ab gerade für kleine und mittelständische Unternehmen kosteneffektive und skalierbare IT-Lösungen bereitzustellen. Cloud Computing beschäftigt sich somit weitaus mehr mit betriebswirtschaftlichen Aspekten als SOC.

Cloud und Peer-to-Peer: Prinzipiell ähneln sich die Konzepte des Cloud Computing und Peer-to-Peer. Die Grundintentionen sind jedoch verschieden. Beim Peer-to-Peer soll eine bestimmte Rechenlast auf möglichst viele Rechner verteilt werden, während beim Cloud Computing die Rechenlast ausgelagert wird [14].

3.1.3 Vorteile und Risiken

Cloud Computing ist eines der derzeit dynamischsten Forschungsgebiete der IT-Industrie. Namhafte Firmen wie IBM, Amazon und Google treiben die Entwicklung mit großem Engagement voran. Diese Tatsache zeigt, dass Cloud Computing das Potenzial hat unser Verständnis über die Bereitstellung und Nutzung von IT-Diensten grundlegend zu verändern [2]. Wie jede neue Technologie ist auch dieses Paradigma mit Zweifeln, aber auch potentiellen Vorteilen behaftet. So beschäftigen sich einige wissenschaftliche Artikel mit eben diesem Thema: Welche Herausforderungen und Vorteile bringt Cloud Computing mit sich?
Eine von der IDC im Jahr 2008 durchgeführte Umfrage zeigt, welche möglichen Vorteile und Problemfelder von den 244 befragten CIOs (Chief Information Officer) als signifikant für deren jeweiliges Geschäftsfeld eingeschätzt werden. Das Ergebnis ist in Grafik 3.7 bzw.

Grafik 3.2 zusammengefasst. Die Umfrage zeigt vor allem, dass das Potenzial des Cloud Computing erkannt wurden, jedoch Sicherheitsbedenken (bspw. Verlust der Kontrolle über die physikalische Sicherheit der Daten) eine große Rolle spielen.

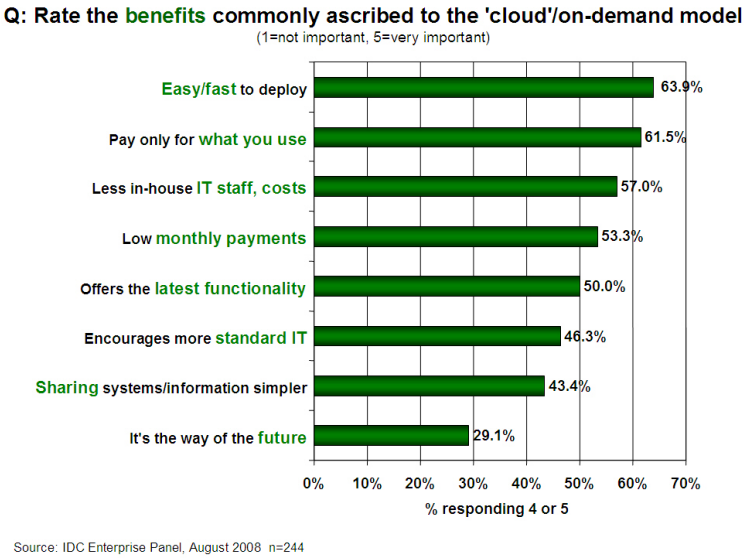

Abbildung 3.1: Mögliche Vorteile des Cloud Computings in Firmen [Quelle: IDC Umfrage 2008]

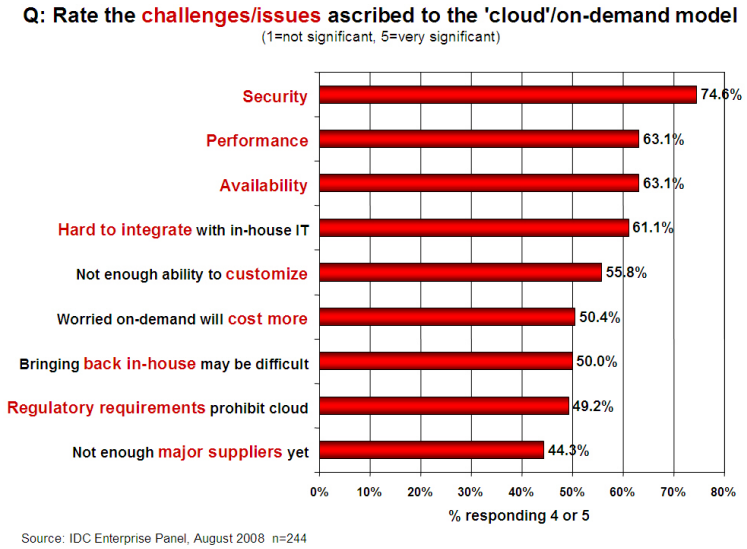

Abbildung 3.2: Herausforderung bei der Einführung des Cloud Computings in Firmen [Quelle: IDC Umfrage 2008]

3.2 Grundlagen

In diesem Kapitel werden die wesentlichen technischen Konzepte, auf denen das Cloud Computing aufbaut, vorgestellt. Diese Technologien - Virtualisierung, Serviceorientierte

Architektur (SOA) und Web Services - abstrahieren jede für sich die Komplexität der dahinter liegenden IT-Systeme. Es ist genau diese Abstraktion, die den Erfolg des Cloud Computings ausmacht.

3.2.1 Virtualisierung

Nach [2] ist die Virtualisierung von Ressourcen die wesentliche Grundlage der meisten Cloud-Architekturen. Dieses Konzept erlaubt eine abstrakte Sicht auf physikalische Ressourcen, wie etwa Speicher, Server, Netzwerke und Software. Die Idee ist, Ressourcen in Pools zusammenzufassen und zentral zu verwalten. Dies bringt sowohl für die Betreiber von IT-Diensten als auch für deren Nutzer Vorteile mit sich. Beispielsweise kann ein Betreiber einer Server Farm einfach Ressourcen aus dem Pool allokieren, anstatt seine Server aufwändig nachzurüsten. Der Bedarf des Nutzers kann aus diesem Ressourcen-Pool dynamisch befriedigt werden.

Virtualisierungskonzepte

Virtualisierung ist stellvertretend für eine Vielzahl anderer Konzepte, die jedoch immer die selbe Grundidee verfolgen, zu sehen. Diese Konzepte unterscheiden sich meist in ihrer technischen Umsetzung und Praxisrelevanz.

Im Folgenden sind die - bezüglich des Cloud Computings - wichtigsten Konzepte dargestellt, die die Grundlage für die in Abschnitt 3.2.4 erläuterte Architektur darstellen.

Plattformvirtualisierung: Diese Art der Virtualisierung erlaubt die Ausführung unterschiedlicher Betriebssysteme in einer virtuellen Umgebung. Prinzipiell ist zwischen zwei Arten von Plattformvirtualisierungen zu unterscheiden: Vollständige Virtualisierung und Para-Virtualisierung. Beide Arten werden technisch gesehen mit einem sogenannten Hypervisor umgesetzt. Dieser verwaltet die Hardware-Ressourcen und koordiniert die Zugriffe der verschiedenen Gast-Betriebssysteme [2].

Netzwerkvirtualisierung: Die Abstraktion der Netzinfrastruktur ist ein essentieller Aspekt beim Cloud Computing und wird hauptsächlich durch Techniken der Netzwerkvirtualisierung umgesetzt. Zu diesen Techniken zählt die Repräsentation von Ressourcen als Web-Objekte, auf die mit virtuellen IP-Adressen zugegriffen werden kann. Eine weitere Technik ist die Verwendung virtueller lokaler Netze (VLAN) und virtueller Switches, welche es ermöglichen, dass Ressourcen direkt im Netz des Nutzers erscheinen [2].

Anwendungsvirtualisierung: Bei diesem Konzept handelt es sich um ein Modell, welches es ermöglicht Anwendungen zentral zu verwalten und an die Kunden zu verteilen. Dabei gibt es grundsätzlich zwei verschiedene Herangehensweisen: *Hosted Applications* stehen im Internet bereit und werden beispielsweise über SOAP (bei Web Services) zum Kunden transportiert, während bei *Virtual Appliance*-Anwendungen, diese heruntergeladen werden können und auf dem Rechner des Kunden betrieben werden. Im Wesentlichen beruht die Verteilung von Anwendungen im Sinne des Cloud Computing jedoch auf Hosted Applications.

3.2.2 Service-orientierte Architektur

Bei der Service-orientierten Architektur (SOA) handelt es sich zunächst um einen reinen Architekturstil, welcher definiert, wie Dienste angeboten und genutzt werden können. Dabei stellen sich folgende Herausforderungen [2]:

- die Dienste sind verteilte Komponenten
- die heterogenen Nutzer und Anbieter dieser Dienste sind miteinander interoperabel
- Dienste können in unterschiedlichen Programmiersprachen implementiert sein
- Dienste sind lose gekoppelt und werden dynamisch zur Laufzeit gebunden

SOA lässt sich insgesamt wie folgt definieren:

> *Unter einer SOA versteht man eine Systemarchitektur, die vielfältige, verschiedene und eventuell inkompatible Methoden oder Applikationen als wieder verwendbare und offen zugreifbare Dienste repräsentiert und dadurch eine plattform- und sprachenunabhängige Nutzung und Wiederverwendung ermöglicht.*
>
> [Quelle: [3]]

In Abbildung 3.3 ist das prinzipielle Zusammenspiel von Dienstanbietern und Dienstnutzern in einer SOA dargestellt.

3.2.3 Web Services

Während die Service-orientierte Architektur (SOA), wie im vorigen Abschnitt erläutert, ein generelles Architektur-Paradigma darstellt, handelt es sich bei Web Services um eine konkrete Art der Umsetzung einer SOA. Für die Implementierung von Web Services stehen verschiedene Standards zur Verfügung, die das Finden des Dienstes und den eigentlichen Dienstaufruf umsetzen:

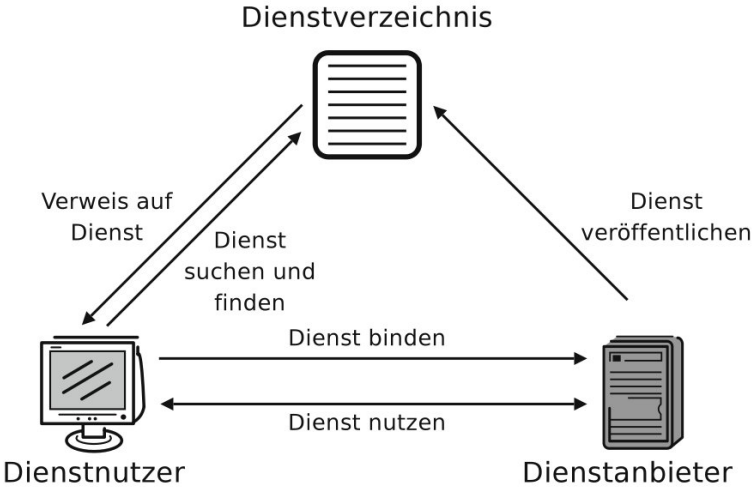

Abbildung 3.3: Beteiligte und Aktionen in einer SOA [Quelle: [2]]

- UDDI (Universal Description, Discovery and Integration): ein Verzeichnisdienst zur Registrierung von Web Services.
- WSDL (Web Service Definition Language): beschreibt, die Funktionen die ein Dienst anbietet.
- SOAP (Simple Object Access Protocol): dient der Kommunikation zwischen Anbieter und Nutzer des Dienstes und startet den eigentlichen Aufruf.

Das Zusammenspiel dieser Standards ist in Abbildung 3.4 dargestellt.

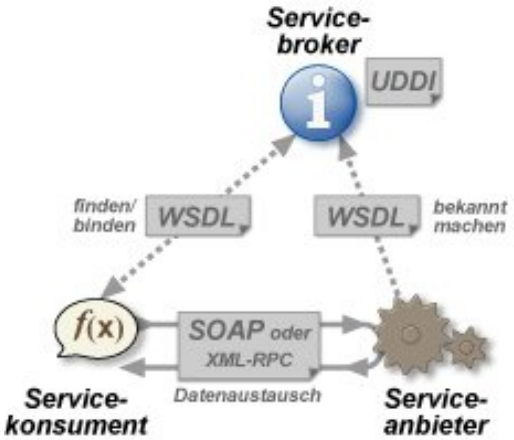

Abbildung 3.4: Web Service Standards und deren Funktionsweise [Quelle: wikipedia]

3.2.4 Cloud-Architekturen

In den letzten drei Abschnitten wurden die dem Cloud Computing zugrunde liegenden Architekturen und Konzepte vorgestellt. In diesem Abschnitt werden Cloud-Architekturen

betrachtet. Diese Betrachtung kann nach [2] aus zwei verschiedenen Blickwinkeln erfolgen: Die organisatorische Sicht unterteilt eine Cloud-Architektur in organisatorische Einheiten von Nutzern und Anbietern, während die technische Sicht nach funktionalen Schichten trennt.

Organisatorische Sicht: Public, Private und Hybrid Cloud

Die organisatorische Sicht auf eine Cloud-Architektur (siehe auch Abbildung 3.5) unterscheidet unterschiedliche Arten von Clouds: public, private und hybrid.

Public Cloud Dieser Cloud ordnet man alle Angebote zu, bei denen Anbieter und Nutzer nicht derselben organisatorischen Einheit (bspw. Firma) angehören. Diese Cloud ist öffentlich zugänglich, bietet Nutzern also Dienste über ein Web-Portal oder ähnlichem an.

Private Cloud Im Kontrast zur Public Cloud steht die Private Cloud. Hier gehören Anbieter und Nutzer derselben organisatorischen Einheit an. Grund für den Einsatz einer Private Cloud sind meist Sicherheitsbedenken: Nutzt man Dienste dieser Cloud bleiben Daten innerhalb einer Organisation und werden nicht an einen externen Dienstanbieter weitergeben.

Hybrid Cloud Setzt man als Nutzer seine Dienste aus Private und Public Cloud zusammen, spricht man von einer Hybrid Cloud. Ein mögliches Szenario, das deren Einsatz rechtfertigt, ist, dass der Regelbetrieb einer Firma über die Private Cloud abgewickelt wird und bei Lastspitzen Ressourcen aus der Public Cloud alokiert werden.

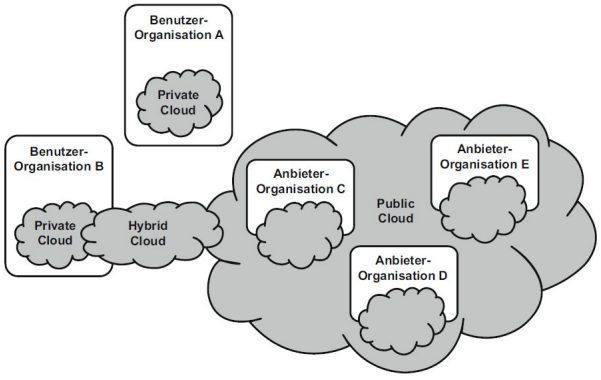

Abbildung 3.5: Organisatorische Sicht: public, private und hybrid Cloud [Quelle: [2]]

Technische Sicht: der Cloud Service Stack

Die technische Sicht auf eine Cloud-Architektur trennt diese in ihre funktionalen Bestandteile. Hieraus resultiert der Cloud Service Stack. Derzeit existieren viele unterschiedliche

Cloud-Angebote von IT-Firmen wie etwa Google, Amazon, Microsoft und IBM. Die Tatsache, dass jede dieser Firmen ihr Cloud Angebot anders aufbaut und auch das Paradigma Cloud Computing teilweise anders definiert, beziehungsweise verwendet, machen eine solche einheitliche Sicht sinnvoll und notwendig und ermöglichen erst eine vergleichende Betrachtung dieser Anbieter. Grundlage dieses Cloud Service Stacks (siehe Abbildung 3.6) ist wiederum die Service-orientierte Architektur, welche zusammen mit den weiteren Konzepten des Cloud Computing zur Service-orientierten Cloud Computing Arcitektur (SOCCA) verschmilzt. Übergeordnetes Ziel ist es, verschiedene Cloud-Angebote miteinander interoperabel zu machen.

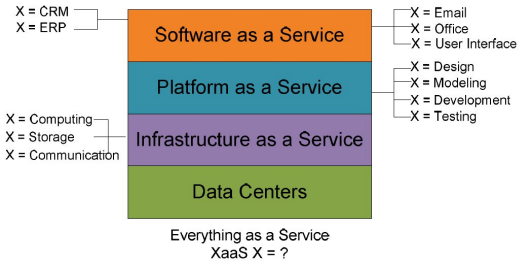

Abbildung 3.6: Technische Sicht: der Cloud Service Stack [Quelle: [5]]

Data Center: Hier wird die Hardware auf der eine Cloud läuft bereitgestellt.

Infrastructure-as-a-Service: Auf der Ebene IaaS werden üblicherweise die virtualisierten Ressourcen des Data Centers bereitgestellt, so dass diese dem Kunden als Dienste zur Verfügung stehen. Übliche Funktionen dieser Schicht sind das Skalieren eines Ressourcenbedarfs (bspw. Speicher) und das Bereitstellen von Kommunikations-Infrastruktur (etwa einem mail-Server)[10]. Beispiel für Dienste dieser Schicht sind etwa GoogleFS (Speicherkapazität) und OpenFlow (Netz).

Plattform-as-a-Service: Die Funktionen der Schicht PaaS lassen sich in die Kategorien *Programmierumgebungen* und *Ausührungsumgebungen* unterteilen [10]. Auf dieser Schicht werden also Dienste bereitgestellt, die den gesamten Anwendungs-Entwicklungszyklus (Desing, Entwicklung, Tests und Verteilung) unterstützen. Beispiele von PaaS Angeboten sind die App Engine von Google und Microsoft Azure.

Software-as-a-Service: In der Schicht SaaS wird dem Nutzer allgemeine Anwender-Software (E-Mail, Textverarbeitung) als Dienst bereitgestellt. Vorteile eines solchen Angebots sind, dass der Nutzer weder die Installation noch Updates vornehmen muss. Beispielhaft für einen Dienst der Schicht SaaS lässt sich derzeit Google Maps nennen.

Die Unterteilung einer Cloud-Architektur in die Funktionsbereiche IaaS, PaaS und SaaS ist keinesfalls abschließend. Teilweise wird als oberste Schicht zusätzlich noch *Human-as-a-Service (HaaS)* [10] angegeben. Hier stehen Dienste zur Verfügung, die lediglich durch Menschen bereitgestellt werden können, etwa die Bereitstellung von wichtigen Nachrichten oder aktuellen Vorhersagen und Umfragen.

3.3 Security-as-a-Service

In diesem Abschnitt wird eine relativ neue, konkrete Ausprägung des Software-as-a-Service Modells vorgestellt: Security-as-a-Service (SecS). Hierbei geht es nicht um Sicherheit innerhalb der Cloud, sondern um Sicherheit, die durch Cloud-Dienste geleistet wird. SecS-Produkte liefern Sicherheitsfunktionen (Viren-Scanner, Firewall etc.), die von einem oder mehreren unterschiedlichen Anbietern bereitgestellt werden [11]. Ziel dieses Abschnittes ist es, grundlegendes Verständis für die besondere Anforderungen und Ausprägungen an bzw. von SecS-Produkte zu schaffen. Hierfür wird zunächst im folgenden Abschnitt ein Definitionsversuch erarbeitet, welcher im Sinne dieser Arbeit als gültige Definition erachtet wird. Im darauf folgenden Abschnitt werden Vor- und Nachteile des SecS-Modells erläutert. In Abschnitt 3.3.3 wird mit Hilfe eine Taxonomie erarbeitet, um eine gemeinsame Sprachbasis zu schaffen.

3.3.1 Definition

Um definieren zu können was im Sinne dieser Arbeit ein Securtiy-as-a-Service (SecS-) Dienst ist, werden zunächst die bisherigen Ansätze zur Gewährleistung der IT-Sicherheit in Unternehmen und Cloud-Angeboten betrachtet. Diese Ansätze sind herkömmliche, installierbare Sicherheitslösungen (bspw. Antivirus-Programme), Managed Security Services und Sicherheitsmechanismen in den jeweiligen Cloud-Angeboten (bspw. Amazon EC2 Security).

Sicherheit in Cloud-Angeboten Wie bereits erwähnt gibt es viele Cloud-Angebote von namenhaften IT-Firmen. Da die Sicherheitsbedenken bei der Nutzung der Cloud-Angebote eine große Rolle spielen, müssen vertrauenswürdige Sicherheitsmechanismen geschaffen werden. Generell sind all diese Cloud-Angebote jedoch in sich abgeschlossen woraus folgt, dass die Sicherheitsmechanismen lediglich auf dieses abgeschlossene, Angebote angewendet werden können. Beispielhaft können hier die Amazon Web Services (AWS) betrachtet werden. Nutzt man einen der AWS-Dienste, ist die Sicherheit der Dienstnutzung gewährleistet. Im Amazon Whitepaper zur AWS-Sicherheit [1] heißt es: „[...] werden vor allem die physische und betrieblichen AWS-Sicherheitsverfahren für das von AWS verwaltete Netzwerk und die verwaltete Infrastruktur sowie dienstspezifische Sicherheitsimplementierungen beschrieben“. Diese Sicherheitsverfahren können also lediglich in Zusammenhang mit einem AWS-Dienst genutzt werden. SecS-Dienste sind im Gegensatz hierzu jedoch eigenständige Dienste.

Managed Security Services Das Modell der Managed Security Services (MSS) lässt sich nur schwer von SecS-Diensten abgrenzen. Beides sind extern erbrachte Dienste. Der Unterschied besteht jedoch in der Art, wie Dienste angefordert werden und ihre Security Level Agreements (SLAs) definiert werden [6]. Dem MSS geht meist eine Ausschreibung voraus, in der der zukünftige Dienstnutzer seine Leistungsanforderungen und SLAs vorgibt. Im Gegensatz dazu sind SecS-Dienste standardisierte Dienste, die vom Nutzer sofort

in Anspruch genommen werden können. Der Dienstanbieter hat meist eine vollständige Security-Infrastruktur bei sich aufgebaut; dennoch nutzt der Kunde selektiv lediglich die Dienste, die er auch tatsächlich benötigt.

Herkömmliche, installierbare Sicherheitslösungen Unter herkömmlichen, installierbaren Sicherheitslösungen versteht man gängige Antivirus-Programme, Firewall-Software, Spam-Filter und ähnliches. Nutzt eine Firma solche Software, muss diese meist auf allen Geräten installiert und konfiguriert werden. Meist ist dafür die IT-Abteilung des Unternehmens zuständig. SecS als Instanz des Software-as-a-Service Modells setzt im Gegensatz dazu jedoch auf Outsourcing. SecS-Dienste müssen nicht auf den Endgeräten des Nutzers installiert werden, sondern sind - nach Buchung - meist über Browser nutzbar. Problematisch bei herkömmlichen, installierbaren Sicherheitslösungen ist auch die Interoperabilität mit Sicherheitslösungen anderer Anbieter. Meist mussten nach Installation eines neuen Sicherheitsprogramms die bisherigen nachträglich konfiguriert und integriert werden. Eine wesentliche Anforderung an SecS-Dienste ist hingegen, dass diese zu bestehenden Diensten hinzugefügt werden können, ohne dass Änderungen vorgenommen werden müssen [12].

Aus den Abgrenzung zu bisherigen IT-Sicherheitslösungen erfolgt nun eine Definition von SecS-Diensten.

Definition: Security-as-a-Service-Dienst

> *Security-as-a-Service-Dienste sind vorgefertigte, eigenständige IT-Sicherheitslösungen, die selektiv aus einem Angebots-Pool gebucht werden, gemäß des Software-as-a-Service Modells verteilt werden und nutzbar sind, ohne, dass eine Änderung am bisherigen System oder den momentan in Anspruch genommenen Diensten vorgenommen werden muss.*

3.3.2 Chancen und Risiken

Derzeit gelten SecS-Dienste als neues, vielversprechendes Paradigma. Jedoch ist die Nutzung von SecS-Diensten auch mit Risiken behaftet. In diesem Abschnitt werden Chancen und Risiken aufgezeigt.

Chancen

Sicherheit trotz knappem IT-Budget Kleine und mittelständische Unternehmen stehen oft dem Problem gegenüber, dass sie zwar schützenswerte Konzepte und Produkte entwickeln, jedoch nicht das nötige IT-Budget haben um Sicherheitslösungen mit marktüblichen Technikstandards zu implementieren [11]. SecS-Dienste bringen den Vorteil mit sich, dass ein Unternehmen für das bezahlt was es auch nutzt. Weiterhin können eventuell bestehende IT-Abteilungen entlastet oder minimiert werden.

Sicherheit als Kernkompetenz von SecS-Anbietern Während Anwender IT-Sicherheit meist als Kostenfaktor sehen, gehört Sicherheit zu den Kernkompetenzen eines SecS Anbieters. Solche Anbieter sind langfristig nur dann profitable und überlebensfähig, wenn sie den Sicherheitsanforderungen des Kunden genügen. Dieser kann sich darauf verlassen, dass ein Anbieter alles tut, um sein „Sicherheits-Know-How“ aktuell zu halten [11].

Sicherheit on Demand und schneller Rollout Die Bereitstellung von SecS-Diensten erfolgt unmittelbar über das Internet. Weiterhin können einzelne Sicherheitsfunktionen von Diensten flexibel zu- oder abgeschalten werden [11]. Ein schneller Rollout neuer Sicherheitsfunktionen ist vor allem bei einer Veränderung der Bedrohungslage (beispielsweise bei neuen Viren) von Relevanz.

Risiken

Konflikte zwischen SecS-Diensten und proprietärer IT Problematisch bei derzeitigen SecS-Diensten ist laut [11], dass diese stark standardisiert sind und daher nur eingeschränkt in die proprietärer IT des Anwenderunternehmens eingefügt werden können. Daraus ergibt sich die Gefahr, dass SecS-Dienste im Vergleich mit traditionellen Sicherheitslösungen die Anforderungen nur ungenügend erfüllen können.

Sicherheit in der Cloud Wie bereits in Abschnitt 3.1.3 erwähnt, wird derzeit die Sicherheit innerhalb der Cloud als kritischer Punkt angesehen. Dies liegt daran, dass - im Gegensatz zu herkömmlichen IT-Lösungen - Anwendungsdaten (etwa Konfigurationsdateien) beim Dienstanbieter gespeichert sind. Insbesondere bei SecS-Diensten führt dies zu Problemen, da der Zugriff auf Konfigurationsdaten (beispielsweise die einer Firewall) durch Angreifer den gezielten Angriff auf das Nutzerunternehmen ermöglichen und sogar erleichtern. Ein weiteres Risiko stellt die Möglichkeit von Single-Point Attacken dar. Da ein SecS-Anbieter mehrere Nutzer bedient, hat ein erfolgreicher Angriff auf den Anbieter gleichzeitig die Verwundbarkeit aller Nutzer zur Folge.

Sicherheitsverlust bei Netzausfall oder -schwankung Die Leistungsfähigkeit von SecS-Diensten hängt im wesentlichen von der Verfügbarkeit und Leistung der Internetanbindung des Nutzers ab. Fällt die Internetanbindung aus, werden die Sicherheitsfunktionen des Dienstes nicht mehr bereitgestellt. Auch eine Schwankung in der Leistung des Netzes ist problematisch, da dann bestimmte Funktionen des SecS-Dienstes nur noch teilweise erbracht werden können.

Fazit

SecS-Dienste stellen für kleine und mittelständische Unternehmen eine vielversprechende Möglichkeit dar, jede benötigte Sicherheitsfunktion - durch externe Anbieter erbracht - nutzen zu können. Generell können die Dienste auch mit herkömmlichen IT-Sicherheitslösungen

kombiniert werden. Es gilt durch einen potentiellen Nutzer also abzuwägen, welche Dienste extern erbracht werden sollten und welche Sicherheitsfunktionen er selbst durch herkömmliche Sicherheitsimplementierungen in seine Systeme einbindet. Obwohl noch Risiken bestehen, ist zu erwarten, dass diese in Zukunft auf Grund des Engagements bekannter Anbieter (beispielsweise McAfee, siehe Kapitel 3.4) gelöst werden.

3.3.3 Taxonomie für Security-as-a-Service-Dienste

Nach der Erarbeitung der Definition von SecS-Diensten, erfolgt nun die Einführung einer Taxonomie von SecS-Diensten. Ziel ist es, die wichtigsten Aspekte dieses Themas aufzuzeigen und zu beschreiben. Weiterhin soll so eine gemeinsame Sprachbasis für das Thema geschaffen werden.
Für die Erarbeitung dieser Taxonomie wurden verschiedene Arbeiten zur Thematik betrachtet (etwa [12], [4]), die einen ersten Überblick über das Thema ermöglicht haben. Weiterhin wurden einige aktuelle SecS-Angebote bezüglich ihrer Unterschiede und Gemeinsamkeiten untersucht und wichtige Aspekte herausgefiltert. Die allgemeinen Sicherheitsaufgaben entstammen der Taxonomie aus [15].

Aufbau der Taxonomie

Der Aufbau der Taxonomie umfasst folgende Aspekte:

- Aufbau und Integration: Beschreibt den Aufbau der SecS-Dienste bezüglich der Funktionen und deren Integrationsmöglichkeiten.
- Schutzziele: Was sind die Schutzziele des Dienstes?
- Sicherheitsaufgaben: Allgemeine Aufgabenbereiche der IT-Sicherheit.
- Compliance: Rahmenbedingungen, die bei der Verwendung von SecS-Diensten beachtet werden müssen.

Aufbau und Integration

Einzelfunktion versus komplexe Funktionalität SecS Angebote unterscheiden sich teilweise erheblich in ihrem Funktionsumfang. So ist zwischen Diensten, die Einzelfunktionen umsetzen - etwa Single-Sign-On[1] - und Diensten die einen komplexen Funktionsumfang haben, zu unterscheiden. Ein Dienst mit komplexem Funktionsumfang ist beispielsweise der Endpoint Protection Service von McAfee (siehe Abschnitt 3.4.1).

[1]Ermöglicht es bei einmaliger Anmeldung an einem Arbeitsplatz auf alle (je nach Rolle) vorgesehenen Dienste und Daten ohne weitere Anmeldung zugreifen zu können.

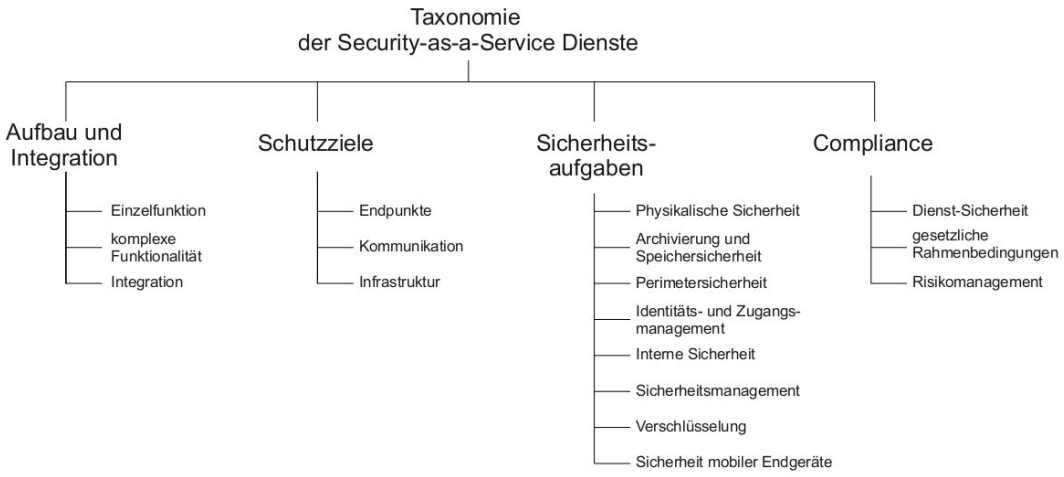

Abbildung 3.7: Aufbau der Taxonomie der Security-as-a-Service-Dienste

Integration Ein weiterer wichtiger Aspekt ist die Einbindung von Diensten in die Systemlandschaft des Nutzers. Hierbei gilt es *Virtual Appliance*-Anwendungen und *Hosted Applications* zu unterscheiden (siehe „Anwendungsvirtualisierung“ in Abschnitt 3.2.1). Prinzipiell ist der Einsatz von Hosted Applications mit einem erhöhten Maße an Flexibilität verbunden, da keine Installation erfolgen muss. Die Einbindung solcher Dienste erfolgt meist über Webportale.

Schutzziele

Aktuelle SecS-Dienste konzentrieren sich auf die Sicherheit dreier Schutzziele (Endpunkte, Kommunikation und Infrastruktur). Die Abdeckung dieser Schutzziele bietet jedoch keinen Schutz im Sinne einer vollständigen Sicherheitsarchitektur, da nicht alle Aufgabenfelder der IT-Sicherheit abgedeckt sind (siehe folgender Abschnitt: „Sicherheitsaufgaben“). Diese Schutzziele beschreiben die Sicht von SecS-Anbietern auf das Netz eines Kunden.

Endpunkte Unter dem Begriff „Endpunkte“ versteht man alle Endgeräte einer IT-System Landschaft (etwa Desktop-Arbeitsplätze). Je nach Dienstanbieter werden auch (mail-) Server zu dieser Kategorie gezählt. Diese Kategorie deckt jedoch mobile Endgeräte nicht ab, da beispielsweise für die Verschlüsselung von Mobiltelefonen spezielle Hardware notwendig ist.

Infrastruktur Der Begriff Infrastruktur umfasst alle Geräte in einem Netz, die zu dessen Betrieb beitragen - beispielsweise Router. Dienste, die dieses Schutzziel abdecken, setzen meist eine Firewall-Funktionalität um oder schützen Server. Ein vollständiger Schutz der Netzinfrastruktur sollte jedoch auch eine Bedrohungsanalyse eines Netzes umfassen.

Kommunikation Unter dem Schutzziel Kommunikation versteht man den Schutz jeglicher Kommunikation über das Netz. Dies umfasst die Bereitstellung von Virtual Private Networks (VPNs), Anti-Spam Funktionen und Content-Filterung. Der Schutz von Kommunikation dient letztlich dem Schutz von Endpunkten und wird von einigen Dienstanbietern nicht explizit aufgeführt.

Sicherheitsaufgaben

Da die zuvor beschriebenen Schutzziele nur Teile einer IT-Infrastruktur schützen, soll nun ein Überblick über allgemeine Sicherheitsaufgaben bei IT-Systemen gewonnen werden. Dies dient im Weiteren dazu, aufzuzeigen, welche Sicherheitsaufgaben durch SecS-Dienste nur teilweise oder gar nicht erfüllt werden.

Physikalische Sicherheit Die physikalische Sicherheit hat zur Aufgabe die IT-Infrastruktur vor tatsächlichen, physikalischen Zugriffe durch Unbefugte zu schützen. Im Sinne des Cloud Computing ist damit der gebäudetechnische Schutz des Data Centers (siehe Abschnitt 3.2.4) gemeint. Funktionen, die zur physikalischen Sicherheit beitragen sind die Zugangsbeschränkung zu bestimmten Bereichen, (Video-) Überwachung und ähnliches. Generell ist bei der Nutzung von Cloud Diensten die Sicherheit des Data Centers aber auch allgemein die innerbetriebliche physikalische Sicherheit von besonderer Relevanz.

Archivierung und Speichersicherheit Ein weiteres, im Rahmen der IT-Sicherheit relevantes Aufgabenfeld ist die Archivierung und Speichersicherheit. Zu diesem Aufgabenfeld gehört die Aufstellung von Archivierungsrichtlinien und deren Umsetzung. Funktionen, die der Speichersicherheit dienen, sind beispielsweise Verschlüsselungen von Festplatten und anderen Speichermedien. Bei Nutzung von Cloud Diensten - im Speziellen SecS-Diensten - muss klar sein, welche Daten besonders geschützt werden und welche Daten regelmäßig archiviert werden.

Perimetersicherheit Die Perimetersicherheit dient der Sicherheit des organisatorischen und technischen Umfeldes eines Unternehmens. Die Sicherheit des organisatorischen Umfeldes setzt beispielsweise Maßnahmen gegen Identitätsdiebstahl, etwa durch Betriebsausweise, aber auch Maßnahmen gegen Betrug, voraus. Solche Maßnahmen werden jedoch nicht von SecS-Diensten umgesetzt und müssen von einer Organisation selbst wahrgenommen werden. Die Sicherheit des technischen Umfeldes meint im Sinne der oben genannten Schutzziele meist Sicherheit der IT-Infrastruktur. Zugehörige Funktionen sind zum Beispiel Firewalls und Intrusion Prevention Systeme. Im weiteren Verlauf dieser Arbeit meint Perimetersicherheit die Sicherheit des technischen Umfeldes einer Organisation.

Identitäts- und Zugangsmanagement In dieses Aufgabenfeld fallen Funktionalitäten wie etwa Single-Sign-On, Rollen- und Rechteverwaltung in einem Dateisystem oder eine Identitätsverwaltung über einen zentralen Verzeichnisdienst (etwa durch LDAP).

Interne Sicherheit Die interne Sicherheit setzt unter anderem Funktionen, die Endpunkte schützen sollen (so etwa Antivirus-Funktionen) um. Im erweiterten Sinne gehören zum Aufgabenfeld der internen Sicherheit jedoch auch die Umsetzung von Sicherheits-Policies oder die Überwachung des Netzes.

Sicherheitsmanagement In dieses Aufgabenfeld fallen alle Tätigkeiten, die der allgemeinen Verwaltung des Aspektes IT-Sicherheit dienen. Dazu gehört das Management und die Weitergabe von generellen Sicherheitsinformationen, aber auch das Erfassen („mitloggen“) von sicherheitsrelevanten Vorgängen.

Verschlüsselung Das Aufgabenfeld Verschlüsselung beschreibt allgemeine (Mindest-) Funktionen, die (je nach Größe einer Organisation) vorhanden sein sollten. Dazu kann der Aufbau einer Public-Key-Infrastructure, beziehungsweise allgemeine Schlüsselverwaltung zählen. Weiterhin sollten generelle Mechanismen zur Verschlüsselung kritischer Daten vorhanden sein.

Sicherheit mobiler Endgeräte Zu diesem Aufgabenfeld zählen Funktionen, die allgemein die Sicherheit von mobilen Endpunkten bzw. Endgeräten umsetzen. Zu solchen mobilen Endgeräten gehören nicht nur Laptops sondern auch Mobiltelefone. Beispielhafte Funktionen sind die mobile Nutzerauthentifizierung, mobile VPNs und die Verschlüsselung der Datenübertragung mobiler Endgeräte.

Compliance

In den Bereich Compliance fallen alle regulatorischen Themen, die Auswirkungen auf die Entscheidung eines Verantwortlichen - etwa hinsichtlich der Frage ob SecS-Dienste genutzt werden sollen - haben. Eine zentrale Frage ist hier, wie sicher Cloud-Dienste sind und welche gesetzlichen Rahmenbedingungen es bezüglich der Nutzung von Cloud Diensten gibt.

Dienst-Sicherheit Ein kritischer Punkt bei der Verwendung von SecS-Diensten ist die Frage, ob diese Dienste selbst sicher sind oder einem Angreifer weitere potentielle Angriffspunkte (evtl. durch Schwachstellen in verwendeten Protokollen) bieten. Die Sicherheit von Diensten hängt hierbei im Allgemeinen von den folgenden Faktoren ab:

- Physikalische Sicherheit des Data Centers, in welchem die Dienste laufen.
- Datensicherheit: Schutz der Konfigurations- und Metadaten, die zwischen Nutzer und Anbieter des Dienstes ausgetauscht werden. Dabei kann es sich beispielsweise auch um Vertragsdaten handeln, die vertrauliche Informationen bezüglich der Dienstnutzung beinhalten.

- Anwendungssicherheit: Dieser Bereich fordert Verfahren zur Sicherstellung der Integrität, Authentizität und Verfügbarkeit eines Dienstes. Dazu gehört beispielsweise die Verschlüsselung der übertragenen Nachrichten (etwa durch Webservice-Sicherheitsstandards) oder das Signieren von Nachrichteninhalten [12].

- Plattformsicherheit: Der Aspekt der Plattformsicherheit zielt darauf ab, dass ein sicherer Dienst schon bei der Entwicklung durch Verwendung von bestimmten Entwicklungsumgebungen und Sicherheitsverfahren entsteht. Zur Plattformsicherheit zählen auch Sicherheitsdokumentationen über den Dienst.

Gesetzliche Rahmenbedingungen Die rechtlichen Aspekte bei der Nutzung von Cloud Diensten sind derzeit insgesamt noch unzureichend beleuchtet. Generell finden alle Datenschutzgesetze Anwendung. Weiterhin gilt, dass Daten, die durch Gesetze besonders geschützt sind, wie etwa Gesundheitsdaten oder Daten bestimmter Berufsgruppen, und die Grenzen eines geographischen Ortes nicht verlassen dürfen, auf Cloud Computing Systemen nicht gespeichert werden können [12]. Diese Problematik spielt in der Regel jedoch bei der Verwendung von SecS-Diensten eine untergeordnete Rolle. Ein weitaus wichtigerer Aspekt ist die Frage der Dienstfortsetzung, wenn ein Anbieter einen Dienst einstellt oder nicht mehr fortsetzen kann. Ein weiteres Szenario ist auch, dass ein Dienst von einem anderen Anbieter übernommen wird. Diese beiden Fragen müssen bei der Entscheidung, ob SecS-Dienste - oder allgemein Cloud-Dienste - verwendet werden sollen, miteinbezogen werden.

Risikomanagement Bei der Nutzung von Cloud Diensten lagert der Nutzer des Dienstes allgemein einen Geschäftsprozess oder einen Teil davon aus. Daher ist es für einen Nutzer wichtig, einen Prozess zu entwickeln, der die mit einem Dienst verbundenen Risiken behandelt und auf eine daraus resultierende Entscheidung abbildet. Solche Risiken sind etwa der Ausfall eines Dienstes oder Sicherheitsvorfälle, die den Dienst betreffen. Was für Cloud-Dienste im Allgemeinen gilt, gilt in erhöhtem Maße für SecS-Dienste, da die Sicherheit der IT-Infrastruktur Grundlage für alle Geschäftsprozesse ist. Die Risikoeinschätzung als zentraler Punkt eines Risikomanagements sollte sich auf konkrete Vereinbarungen (etwa Service-Level-Agreements) mit dem Dienstanbieter stützen.

3.4 Untersuchung ausgewählter Security-as-a-Service-Dienste

In diesem Kapitel werden einige Security-as-a-Service (SecS) Dienste hinsichtlich ihrer Funktionalität, Zielsetzung und Funktionalität untersucht. Dabei wird die im vorigen Abschnitt erarbeitete Taxonomie zu Grunde gelegt.

3.4.1 McAfee Security-as-a-Service

McAfee bietet eines der momentan umfassendsten SecS Angebote. Das SecS Gesamtangebot setzt sich hierbei aus unterschiedlichen Diensten für verschiedene Unternehmensgrößen (klein, mittel, groß) zusammen. Weiterhin werden Dienste, die eine Einzelfunktion (etwa E-Mail-Archivierung) umsetzen, angeboten. Diese Dienste bzw. Funktionen werden teilweise zu einer kompletten Suite mit komplexen Funktionsumfang aggregiert. Insgesamt deckt McAfee folgende Schutzziele ab: Endgeräte, Kommunikation und Netzinfrastruktur. Hervorzuheben ist, dass McAfee jedoch auch Dienste anbietet, die Bedrohungsanalysen des Kundensystems durchführen. Diese Dienste konzentrieren sich insbesondere auf die Netzinfrastruktur, so dass McAfee als einziger Anbieter dieses Schutzziel abdeckt.

Im Folgenden sind einige angebotenen SecS-Dienste für Großunternehmen kurz beschrieben [13]. Die hier nicht aufgeführten Dienste setzen sich aus diesen „Grundtypen“ zusammen.

PCI Certification Service Dieser Dienst hilft dem Nutzerunternehmen dabei ihr Payment Card Industry Security Standard (PCI) Zertifikat zu prüfen. Der Dienst umfasst weiterhin Unterstützung bei der Fehlerbehebung, technischen Support und Sicherheitseinschätzungen. PCI ist ein Regelwerk im elektronischen Zahlungsverkehr.

E-Mail Protection Service Die McAfee SaaS E-Mail Protection ist eine gehostete Sicherheitslösung für die E-Mail-Kommunikation und schützt vor Spam, Viren, Würmern und anderen Bedrohungen. Eingehende E-Mails werden durch den Dienst zunächst auf einen McAfee-Server umgeleitet und überprüft.

Vulnerability Management Service Dieser Dienst führt eine Bedrohungsanalyse der über Internet zugänglichen Ressourcen / Netzinfrastruktur durch. Die Überprüfung erfolgt vom McAfee Rechenzentrum aus über ein Webportal und zeigt Schwachstellen des Systems auf. Durch den Dienst erfolgt ebenfalls eine Risikobewertung für alle gefundenen Schwachstellen.

Endpoint Protection Bei der McAfee Endpoint Protection werden mehrere Funktionen aggregiert: Webseiten-Blockierung und Content-Filterung, Desktop-Firewall und Mail-Server Sicherheit etc. Insgesamt soll der Dienst die Endgeräte des Nutzers vor Bedrohungen durch das Internet schützen.

3.4.2 Panda Security Cloud Protection

Das SecS-Angebot von Panda deckt lediglich zwei Schutzziele ab: Endpunkte und Kommunikation (E-Mail und Web). Das Angebot richtet sich an kleine und mittelständische

Unternehmen. Es werden hierfür drei Dienste, die jeweils Einzelfunktionen beinhalten, angeboten. Der **Office Protection Dienst** schützt Endpunkte durch eine Firewall und Antivirus Funktion. Der **E-Mail Protection Dienst** setzt im Wesentlichen einen Spam Filter um, während der **Internet Protection Dienst** eine Verwaltung von Web 2.0 Anwendungen (etwa zur Sperrung einzelner Applikationen), URL Filter und Internetverkehrs-Analyse bietet.

3.4.3 Symantec Hosted Services

Bei den Hosted Services von Symantec handelt es sich um ein Angebot, das sich aus insgesamt 7 Diensten mit (teilweiser) komplexer Funktionalität zusammensetzt. Insgesamt sollen Endpunkte und Kommunikation (E-Mail, Web und Instant Messaging) geschützt werden [16].

Im Folgenden werden wieder die grundlegenden Dienste beschrieben:

Hosted Endpoint Protection Dieser Dienst schützt Desktop-Arbeitsplätze und Laptops durch eine Antivirus-Funktion, Firewall und einen Malware-Schutz. Zu beachten ist, dass bei diesem Angebot lediglich Endpunkte mit Windows-Betriebssystem geschützt werden.

Hosted E-Mail Archiving Der Dienst ermöglicht es E-Mails zu archivieren. Dabei werden zusätzlich erweiterte Suchfunktionen angeboten und es können Archivierungs-Richtlinien erstellt werden.

Hosted E-Mail Continuity Falls eigene E-Mail Server ausfallen, kann dieser Dienst aktiviert werden und dient als Ersatzsystem. Nach dem Ausfall werden die E-Mail Server wieder vollständig synchronisiert.

Hosted E-Mail Encryption Mit Hilfe dieses Dienstes findet eine Policy basierte Verschlüsselung von E-Mails statt. Policies können dabei vom Nutzer selbst definiert und konfiguriert werden.

Hosted E-Mail Security Der Dienst setzt im Wesentlichen einen Spam-Filter um und hilft bei der Einrichtung von Verteilerlisten und zugehörigen Nutzungsrichtlinien.

3.4.4 PingIdentity Single-Sign-On

Der Dienst von PingIdentity ist kein Dienst der eines der beschriebenen Schutzziele schützt sondern dient der Identitätsverwaltung bei anderen Cloud Diensten beziehungsweise Software-as-a-Service Diensten. Der Dienst kommuniziert bei der Anmeldung im Firmennetz die Identität sicher zu allen spezifizierten Diensten. Dadurch entfällt die Verwaltung mehrere Passwörter und Nutzernamen.

Weitere Angebote

Es existieren zahlreiche weitere Angebote, die sich ebenfalls auf die drei Schutzziele, Endpunkte, Kommunikation und Infrastruktur, konzentrieren. Dabei unterscheiden sich die Dienste nur durch kleinere Funktionen.

3.5 Bewertung der Security-as-a-Service-Dienste

In diesem Abschnitt werden die zuvor vorgestellten Dienste der verschiedenen Anbieter anhand einer Bewertungsmatrix dahingehend bewertet, inwiefern sie die in der Taxonomie vorgestellten Sicherheitsaufgaben erfüllen. Ziel ist es zum einen, die zuvor untersuchten Dienste untereinander vergleichbar zu machen, zum anderen soll aufgezeigt werden welche Sicherheitsaufgaben überhaupt durch die hier beschriebenen SecS-Dienste abgedeckt werden. Die Bewertungsmatrix ist in Abbildung 3.8 zu sehen. Zur Bewertung werden die Farbwerte weiß, rot, gelb und grün mit folgender Bedeutung verwendet:

- weiß: Auf Grund mangelnder Einsicht in den Dienst oder in die anbieterinternen Abläufe ist keine Bewertung möglich oder eine Bewertung des Dienstes ist bezüglich dieser Sicherheitsaufgabe nicht sinnvoll.
- rot: Eine Sicherheitsaufgabe wird durch keinen Dienst des Anbieters abgedeckt.
- gelb: Der Dienst trägt indirekt zur Erfüllung einer Sicherheitsaufgabe bei.
- grün: Der Dienst trägt direkt (durch eine oder mehrere Funktionen) zur Erfüllung einer Sicherheitsaufgabe bei.

Insgesamt zeigt sich, dass die Sicherheitsaufgaben in einer Organisation durch das derzeitige Angebot an SecS-Diensten nur teilweise abgedeckt werden. Die Untersuchung und Bewertung der genannten SecS-Dienste hat im Einzelnen zu den folgenden Erkenntnissen geführt:

- Bei keinem Anbieter ist der zentrale Aspekt der physikalischen Sicherheit des Data Centers ersichtlich.

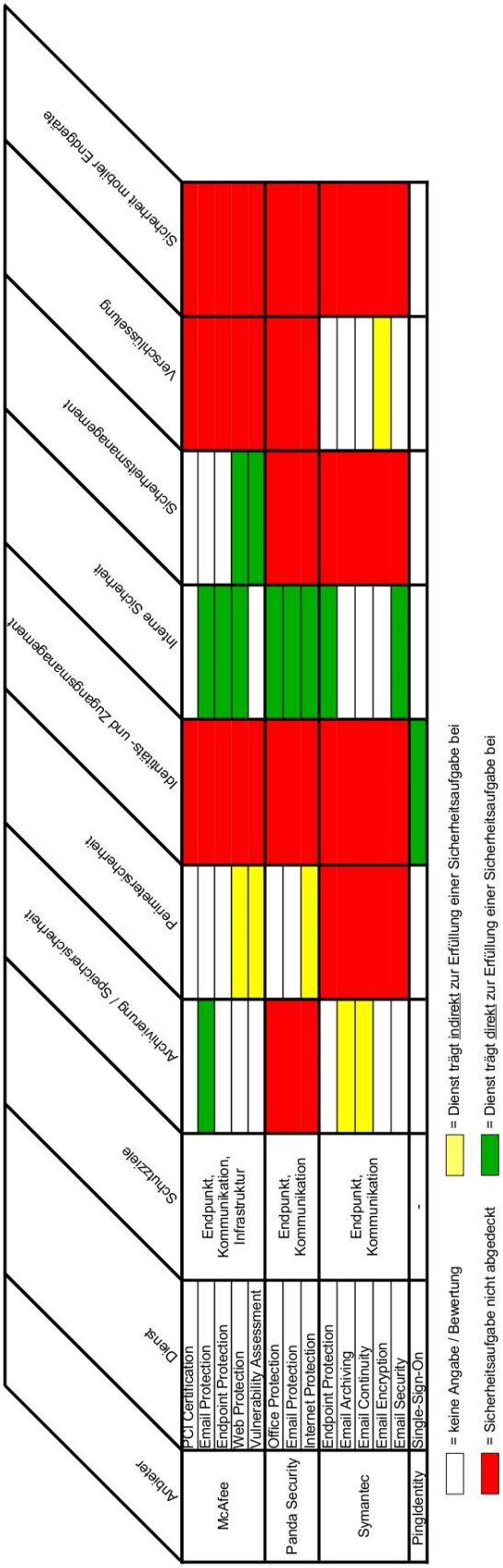

Abbildung 3.8: Bewertung von Security-as-a-Service-Diensten bezüglich relevanter Sicherheitsaufgaben

- Einige Sicherheitsaufgaben werden durch keinen der betrachteten SecS-Dienste abgedeckt.
- Obwohl die Dienstanbieter angeben, die Kommunikation eines Unternehmens zu schützen, wird zumeist keine Verschlüsselung der Kommunikation umgesetzt. Gemeint ist mit dem Schutz der Kommunikation meist der Schutz vor Malware oder der Schutz von Kommunikation über Web 2.0 Anwendungen.
- Die Netz-Infrastruktur wird von lediglich einem Anbieter als Schutzziel angegeben. Tatsächlich wird die Perimetersicherheit - welche die Sicherheit der Netz-Infrastruktur mit einschließt - lediglich indirekt unterstützt.
- Das derzeitige Angebot der betrachteten Dienstanbieter konzentriert sich auf den Schutz von Endpunkten beziehungsweise der internen Sicherheit.
- Es hat sich als schwierig herausgestellt die tatsächliche Funktionalität, die hinter einem Dienst steht, anhand der Informationen, die der Dienstanbieter bereitstellt, zu evaluieren. Meist behandeln die Whitepapers zu einem Dienst größtenteils die generelle Idee von SecS-Diensten und beschreiben tatsächliche Funktionalität nur vereinzelt und verstreut.

3.6 Zusammenfassung

In diesem Kapitel wurden zunächst die Grundlagen des Cloud Computing aufgezeigt. Es wurde verdeutlicht, dass Security-as-a-Service-Dienste (SecS-Dienste) untrennbar von den grundlegenden Konzepten - Virtualisierung, Service-orientierte Architektur und Web-Services - sind. In Abschnitt 3 wurden zunächst bisherige Sicherheitslösungen für IT-Systeme besprochen und voneinander abgegrenzt. Zentraler Bestandteil dieses Abschnittes ist die Definition von SecS-Diensten und die Taxonomie, die einen einheitlichen Sprachgebrauch ermöglichen. Die erarbeitete Taxonomie macht außerdem deutlich, dass eine vollständige Sicherheitsarchitektur mehr umsetzen muss, als lediglich den Schutz von Endpunkten, Kommunikation und Infrastruktur. Eine umfassende Sicht auf eine vollständige Sicherheitsarchitektur bietet die Beschreibung der Sicherheitsaufgaben. Im Hinblick auf die Risiken und Bedenken, die der Einsatz von SecS-Diensten mit sich bringt, ist die Tatsache, dass diese Dienste erfolgreich angeboten werden, überraschend. In Abschnitt 4 wurden die Dienste einiger Anbieter auf ihre Funktionalität hin untersucht. Die Bewertung, welche in Abschnitt 5 vorgenommen wurde, hat gezeigt, dass derzeitige SecS-Dienste die Sicherheitsaufgaben in einem Unternehmen nur teilweise abdecken und sich größtenteils auf die Sicherheit von Endpunkten (Desktop- und Laptoparbeitsplätze) konzentrieren. Eine weitere Fragestellung bezüglich des Themas SecS-Dienste ist, welche weiteren Sicherheitsaufgaben überhaupt durch solche Dienste erbracht werden können. Sicherlich ist nicht jede der beschriebenen Sicherheitsaufgaben dazu geeignet, durch einen externen Dienstanbieter erbracht zu werden.

Literaturverzeichnis

[1] AmazonWebServices. *Amazon Web Services - Sicherheitsprozesse im Ueberblick*, http://awsmedia.s3.amazonaws.com/de/Whitepaper_AWS_Security_Whitepaper%28DE%29.pdf, eingesehen am 10. November 2010.

[2] C. Baun and M. Kunze, J. Nimis, S. Tai. *Cloud Computing - Web-basierte dynamische IT-Servicesstbuch*, Springer-Verlag, 2010.

[3] W. Dostal, M. Jeckle, I. Melzer, B. Zengler. *Service-orientierte Architektur mit Web Services*, Spektrum, 2005.

[4] L. M. Kaufmann. *Can a Trusted Environment Provide Security?* in Security Privacy, IEEE, S. 50-52, 2010.

[5] Alexander Lenk, Markus Klems, Jens Nimis, Stefan Tai, Thomas Sandholm. *CLOUD: What's Inside the Cloud? An Architectural Map of the Cloud Landscape*, 2009.

[6] Interview von Sabine Prehl mit Dror-John Roecher: *Security-as-a-Service ist für Mittelstaendler ideal*, 2010, http://www.computerwoche.de/security/1903672/, eingesehen am 17. November 2010.

[7] John W. Rittinghouse. *Cloud Computing - implementation, management, and security*, CRC Press, 2010.

[8] Matt Sarrel: *Cloud Computing - Evaluating Security-as-a-Service*, 2010, http://www.cioupdate.com/trends/article.php/3893521/Cloud-Computing---Evaluating-Security-as-a-Service.htm, eingesehen am 17. November 2010.

[9] Tharam Dillon, Chen Wu, Elizabeth Chang: *Cloud Computing: Issues and Challenges* in 24th IEEE International Conference on Advanced Information Networking and Applications, 2010.

[10] Wei-Tek Tsai, Xin Sun, Janaka Balasooriya. *Service Oriented Computing, Cloud Computing, Multi-tenacy* in Seventh International Conference on Information Technology, 2010.

[11] Iryna Tsvihun, Philipp Stephanow: *Sicherheit aus der Cloud: Pro und kontra Security-as-a-Service*, 2010, http://www.computerwelt.at/detailArticle.asp?a=130686&n=4, eingesehen am 15. Oktober 2010.

[12] Werner Streitberger, Angelika Ruppel. *Cloud Computing Sicherheit - Schutzziele.Taxonomie.Marktuebersicht*, Fraunhofer SIT, 2009.

[13] Website: *McAfee Security-as-a-Service*, `http://www.mcafee.com/de/enterprise/products/hosted_security/index.html`, eingesehen am 1. Dezember 2010.

[14] Wikipedia: *Cloud Computing*, `http://de.wikipedia.org/wiki/Cloud_Computing`, eingesehen am 20. Oktober 2010.

[15] Website: *the451group, Security Taxonomy*, `http://www.451group.com/security/451_security.php`, eingesehen am 19. Dezember 2010.

[16] Website: *Symantec Hosted Services*, `http://www.symantec.com/business/services/hosted_services.jsp`, eingesehen am 19. Dezember 2010.

Kapitel 4

Standardisierung in Cloud Computing

Patrick Schaffrath

Diese Arbeit gibt einen Überblick über die aktuelle Entwicklung der Standardisierung in Cloud Computing. Dem Leser werden die wichtigsten Standardisierungsorganisationen und deren Arbeit vorgestellt. Zusätzlich werden konkrete Konzepte für Standards veranschaulicht. Für eine kritische Betrachtung der Wichtigkeit von Standards wird der Bereich der Sicherheit detaillierter betrachtet.

Inhaltsverzeichnis

4.1 Einleitung

Diese Arbeit wird zum Ausdruck bringen wozu Standards in Cloud Computing interessant werden können. Vorweg ein negatives Beispiel, welches einen realen Bezug zu bereits ausgereiften IT-Anwendungen besitzt. Wir nehmen an es gäbe nur proprietäre Schnittstellen, dann wird ein Umzug zu einem anderen Anbieter nahezu unmöglich beziehungsweise mit sehr hohem Kostenaufwand verbunden sein. Um Einschränkungen zu vermeiden beschäftigen sich mehrere Organisationen mit der Standardisierung für verschiedene Ebenen des Cloud Computing. Es werden in dieser Arbeit der Großteil an Organisationen genannt, jedoch wird auf einzelne nur dann ausführlicher eingegangen, wenn konkretere Ausarbeitungen für Standards existieren. Diese Standards beschränken sich auf die Bereiche Data as a Service (DaaS) und SaaS, denn sie sind aktuell am meisten fortgeschritten.

Grundsätzlicher Ansatz zur Standardfindung ist die Veröffentlichung von Vorschlägen für die Herangehensweise. Mit anderen Worten, es werden Anforderungen erarbeitet, die ein bestimmter Bereich in Cloud Computing abdecken muss. Anhand von Anwendungsfällen wird nun versucht eine Spezifikation aufzustellen die möglichst praxisnah ist, damit sie eventuell umgesetzt werden kann.

Wir unterscheiden bei der Standardisierung verschiedene Bereiche mit jeweils mehreren Ebenen. Zum einen ist die Seite der Verwaltung von Cloud-Schnittstellen zu vereinheitlichen, zum anderen ist die Sicht der Anwender solcher Cloud-Dienste mit einheitlich definierten Schnittstellen zu versehen.

Solche einheitlichen Schnittstellen werden von den meisten Organisationen für Cloud-Standards mit schon vorhandenen Standards realisiert und mit Metadaten erweitert. Somit wird die Client-Sicht auf ein Interface deutlich vereinfacht. Cloud-Dienste sind global erreichbare Dienste, die über das Internet erreicht werden können und somit über vorhandene Protokolle angesprochen werden. Dabei hat jeder Dienst eine Adresse, über welche seine Cloud-Angebote nutzbar gemacht werden. Würde man nun die gesamte Adresse um einen Befehlssatz erweitern, dann hätte man eine Möglichkeit mit dem Dienst zu kommunizieren.

In den folgenden Abschnitten soll herausgestellt werden, warum Standards in Cloud Computing von Vorteil sind. Dazu wird damit begonnen, wie ein nicht standardisiertes Umfeld den Benutzer von Cloud-Diensten einschränken kann.

Danach wird auf die wichtigsten Organisationen eingegangen, die sich mit dem Prozess der Standardfindung beschäftigen. Zugleich werden konkrete Vorschläge und Implementierungen der Organisationen beschreiben, die aus meiner Sicht wichtig und zukunftsweisend sind.

Der dritte Abschnitt befasst sich mit den Sicherheitsstandards. Hier werden die Risiken in Cloud Computing behandelt. Es soll dem Leser einen kurzen Einblick geben, welchen Anforderungen der Bereich Sicherheit unterliegt und welche Ansätze einer Umsetzung bereits gemacht wurden. Am Ende dieses Abschnittes wird noch darauf eingegangen, in welchem Maße eine vertragliche Bindung an einen Cloud-Anbieter mit der Sicherheit zu tun hat. Abschließend wird ein Fazit zu meiner Ausarbeitung abgegeben.

4.2 Abhängigkeit vom Anbieter

Dieser Teil beschäftigt sich mit der Problematik einer Bindung an einen Anbieter für Cloud-Dienste.

Im Englischen wird vom Effekt des „Vendor Lock-In“ gesprochen. Er beschreibt ganz allgemein die Bindung an einen Hersteller beziehungsweise Anbieter. Damit meint es für den konkreten Fall Cloud Computing proprietäre Schnittstellen. Im Gegensatz zu offenen beziehungsweise standardisierten Schnittstellen implementieren die großen Cloud-Dienst-Anbieter wie Google derzeit ihre eigenen Schnittstellen. Das mag natürlich einzelne Dienste bis ins Detail angepasst machen, aber es schränkt den Kunden in der Zukunft seines Unternehmens ein. Erfahrungen aus der Vergangenheit zeigen, dass solch strikte Bindungen auf Dauer zu kostspielig werden. Es ist ratsam sich dem Bereich des Cloud Computing langsam anzunähern um somit mögliche Risiken besser abschätzen zu können. Kunden sollten also mit kleineren Projekten, die über einen Cloud-Dienst laufen, Erfahrungen sammeln. Oftmals wird es sich anbieten niedrig priorisierte Strukturen in eine Cloud auszulagern.

Die gegenläufige Bewegung stellt Open Source-Schnittstellen zur Verfügung. Durch gemeinschaftliche Weiterentwicklung sollen aus diesen Projekten Standards für die Kommunikation in Cloud Computing entstehen. Durch die Offenheit der Projekte ist eine umfassende Anpassungsfähigkeit gewährleistet. Der Kunde ist weniger abhängig von der Implementierung des Anbieters. Mit dieser Variante bekäme der Kunde einen Zuwachs an Transparenz und könnte sogar Anpassungen vornehmen, um eventuelle Defizite zu beseitigen.

4.3 Organisationen

Die folgenden Abschnitte werden die wichtigsten Organisationen für die Standardisierung in Cloud Computing behandeln. Dabei wurde sich nach den Inhalten der Webseite Cloud Standards Wiki gerichtet.

4.3.1 Cloud Security Alliance (CSA)

Die Cloud Security Alliance (CSA) ist eine nicht kommerzielle Organisation, die sich mit dem gesamten sicherheitsrelevanten Teil des Cloud Computing beschäftigt. Dazu werden nicht nur selbständige Forschungen betrieben, sondern es gibt auch einen lehrenden Zweig, welcher der sicherheitstechnischen Aufklärung von Unternehmen dient. Damit ist die Organisation fähig Unternehmen, die an Cloud Computing interessiert sind, im Bereich Sicherheit weiterzubilden und kann somit eine Sensibilisierung für den Bereich Sicherheit erreichen.

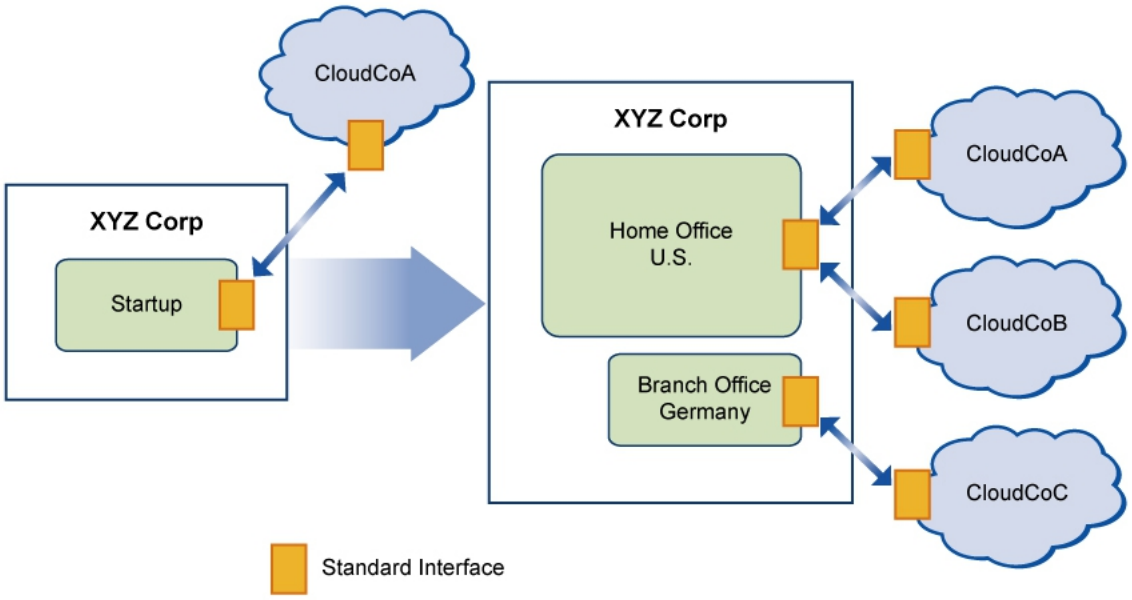

Abbildung 4.1: Erster Anwendungsfall [6]

4.3.2 Distributed Management Task Force (DMTF)

Die Distributed Management Task Force (DMTF) ist eine Gruppe mit 160 Mitgliedern aus Unternehmen und Organisationen. Sie wird von 15 führenden Technologieunternehmen geführt und entwickelt Standards für ein interoperables IT-Management.

Die DMTF besitzt die Cloud Management Working Group (CMWG) für Cloud-Management, welche damit beauftragt ist das Zusammenspiel in der Cloud-Umgebung zu standardisieren. Dazu sollen Spezifikationen erarbeitet werden, aus denen Implementierungsdetails hervorgehen.

Im Folgenden werden Vorschläge der CMWG beschrieben, aus denen Standards hervor gehen könnten.

4.3.2.1 Anwendungsfälle

Die CMWG unterscheidet drei Anwendungsfälle, die jeweils Beziehungen zwischen Anbieter und Kunde abbilden.

Der erste Anwendungsfall (vgl. Abb. 4.1) beschreibt die Bedeutung von Standards für Flexibilität, die einem Kunden, der einen neuen Cloud-Dienst nutzen möchte, zugute kommt. Eine standardisierte Schnittstelle soll es dem Kunden ermöglichen einfach und kostensparend seine Kapazitäten durch Hinzunahme von neuen Cloud-Diensten zu erweitern. Durch die standardisierte Schnittstelle werden dem Kunden nicht nur Dienste eines Anbieters zur Verfügung stehen, sondern auch die Dienste aller weiteren Anbieter, die eine solche Schnittstelle anbieten.

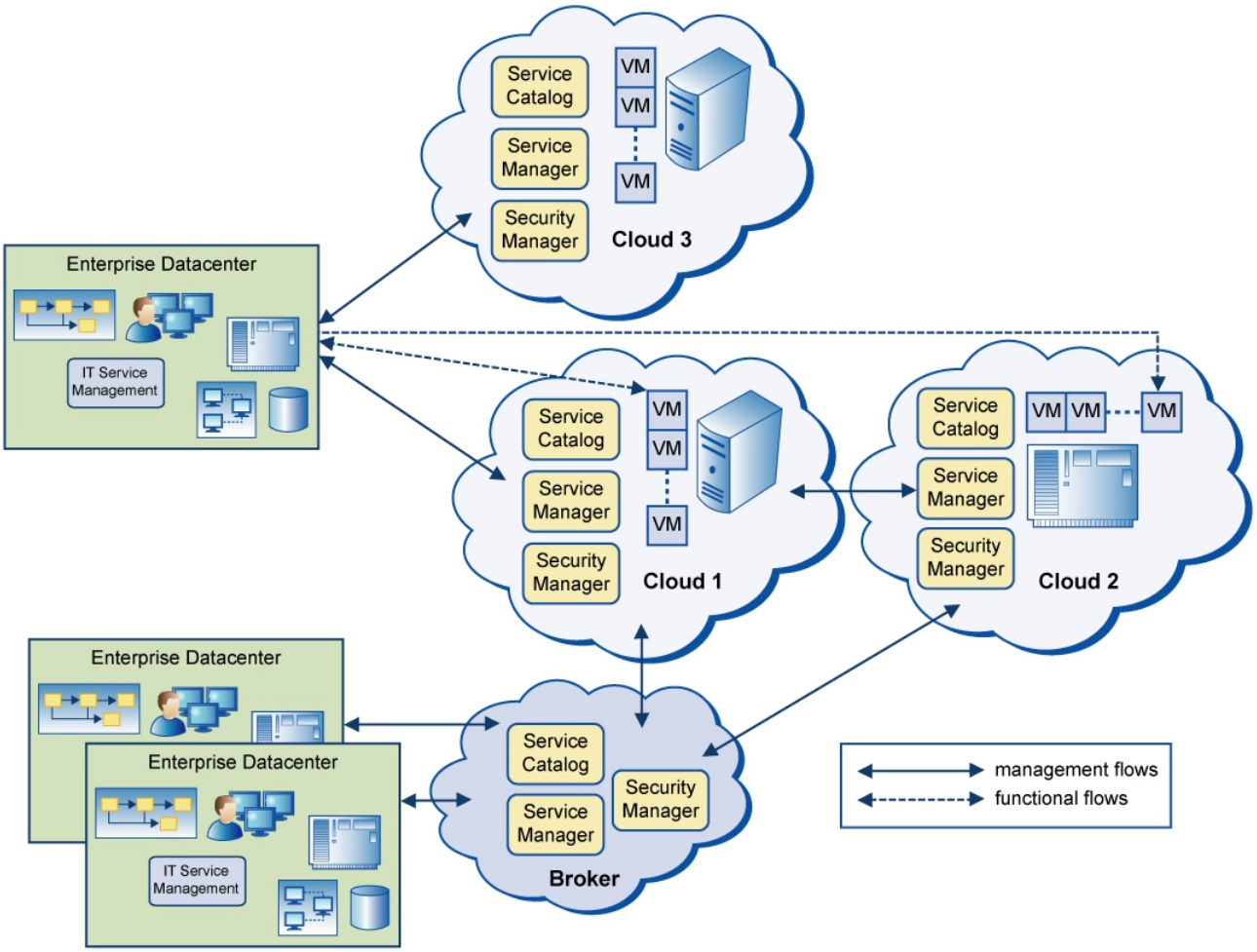

Abbildung 4.2: Zweiter Anwendungsfall [6]

Der zweite Anwendungsfall (vgl. Abb. 4.2) beschreibt die Nutzung von föderativen Cloud-Dienst-Anbietern. Föderative Cloud-Anbieter sind in der Lage ihre Kapazitäten dynamisch zu erweitern. Dazu fordern sie Ressourcen, die ihre Kapazität überschreiten würden, bei weiteren Cloud-Anbietern an. Der Kunde merkt nichts von diesem Prozess, weder eine Kapazitätsbarriere, noch dass Leistung über einen weiteren Cloud-Anbieter bezogen wird. Die Vermittlung von benötigten Schnittstellen soll bei diesem Prinzip über sogenannte Service Manager geschehen. Diesen wird eine Anforderung für die gewünschte Leistung übermittelt und danach wird die Leistung bereitgestellt.

Der dritte Anwendungsfall (vgl. Abb. 4.3) beschreibt die Anpassung von Diensten nach aktuellem Bedarf. Hierbei ist eine weitere Schnittstelle zwischen Cloud-Anbieter und Kunde vonnöten. Angeforderte Daten werden über eine sichere Zweigstelle vom Cloud-Dienst zum Kunden weitergegeben. Dabei wird ein Vertrag eingegangen, welcher sicherstellt, dass die gewünschten Daten über einen sicheren Weg und nur durch Autorisierung beim Kunden ankommen. Des Weiteren müssen angeforderte Daten jederzeit schnell und zuverlässig übertragen werden können und wenn keine Daten mehr zwischengespeichert werden sollen, dann müssen alle temporären Daten unverzüglich und unwiederbringlich gelöscht werden.

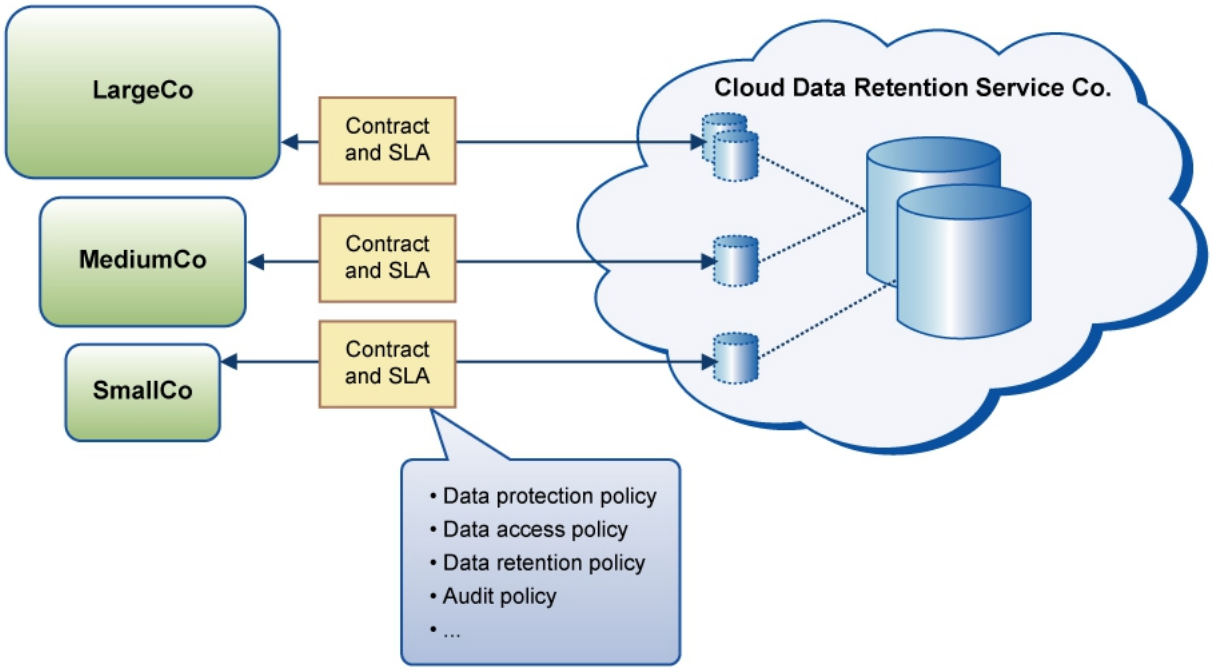

Abbildung 4.3: Dritter Anwendungsfall [6]

4.3.2.2 Lebenszyklus eines Cloud-Dienstes

Jede Nutzung eines Cloud-Dienstes ist über einen Lebenszyklus nachvollziehbar. Dabei gibt es die folgenden Stufen:

- Beschreibung eines Cloud-Dienstes über eine Vorlage
- Bereitstellung des Dienstes durch eine Cloud-Struktur
- Unterbreitung des Angebots
- Kunde geht einen Vertrag für die Nutzung ein
- Nutzung und Verwaltung des Dienstes
- Angebotsende

4.3.3 Storage Networking Industry Association (SNIA)

Der Storage Networking Industry Association (SNIA) ist ein nicht profitabler Verein, dessen Mitglieder Standards entwickeln und veröffentlichen. Wie bereits aus dem Vereinsnamen ableitbar, ist der Bereich für die Standardfindung auf Speichermöglichkeiten über Netzwerke beschränkt. Somit wird der Teil DaaS breit durch die Forschung des Vereins

abgedeckt. Ziel des Vereins ist es, neue Technical Working Groups zu gründen und diese bei ihrer Forschung nach neuen Standards für Netzwerkspeicher zu fördern. Dazu ist anzumerken, dass der SNIA die Vorteile von Bündnissen mit anderen Organisationen für Standardisierung nutzt.

Eine Technical Working Group beschäftigt sich bereits mit dem Cloud-Standard des Cloud Data Management Interface (CDMI), welches als Schnittstelle zu Daten innerhalb der Cloud dient. Detaillierte Informationen zur Realisierung und zum Fortschritt folgen in den nächsten Abschnitten.

4.3.3.1 Der Entwurf eines Datenmanagements

Der Hauptunterschied zu bisherigen, Cloud unabhängigen Speicherschnittstellen ist die Nutzungsart. Der Cloud-Speicher soll dynamisch sein, dass heißt er soll jederzeit erweiterbar sein und seine Nutzung wird zum wesentlichen Faktor der Bezahlung. Für die Nutzungsweise sollen jedoch bereits vorhandene Standards die Richtung vorgeben.

Der SNIA unterscheidet für eine mögliche Implementierung zwei verschiedene Modelle. Für jeweils beide Modelle wird der existierende Standard Create, Retrieve, Update, Delete (CRUD) genutzt.

Das erste Modell adressiert seinen Speicher über Tabellen. Dieses Modell scheidet jedoch für den SNIA aus, denn es gibt für dieses Modell noch zu rasch aufeinander folgende Weiterentwicklungen, als dass es für einen Cloud-Standard ausgereift wäre.

Das zweite Modell adressiert seinen Speicher mittels Uniform Resource Identifier (URI) und erlangt dadurch Zugriff auf einzelne Elemente, welche in separaten Containerstrukturen untergebracht sind. Dieses Modell ist zugleich die Referenz für die weitere Beschreibung.

Da Cloud-Speicher komplexer sind als einfache Festplattenspeicher, werden zusätzliche Informationen benötigt um einen solchen anzusprechen. Hier ist die Idee, die vorhandene CRUD Schnittstelle um Metadaten zu erweitern, welche dem Kunden und dem Anbieter mehr Informationen geben sollen.

Auf Kundenseite können Metadaten eine Protokollfunktion haben, sodass nachvollzogen werden kann, was mit den gespeicherten Objekten passiert. Der Kunde kann nach erfolgreicher Authentifizierung für ein Editieren von Metadaten auch Zugriffsrechte für Objekte festlegen. Durch die Metadaten soll also erreicht werden, dass der Kunde mit den Objekten im Cloud-Speicher ähnlich umgehen kann, so als ob er sie direkt auf einer lokalen Festplatte hätte.

Auf Anbieterseite werden die Metadaten durch Statistiken über ein gespeichertes Objekt erweitert. Solche Informationen enthalten zum Beispiel die Zeit wann ein Objekt zuletzt editiert wurde oder wie oft darauf zugegriffen wurde. Dem Kunden stehen diese Informationen lediglich für einen lesenden Zugriff zur Verfügung.

4.3.3.2 Der Entwurf von CDMI

Die Schnittstelle CDMI wird von Programmen des Kunden genutzt um mit einer Cloud-(Daten)Verwaltung zu kommunizieren. Dazu nutzt CDMI den Web-Standard Representational State Transfer (REST). Das Interface wird nicht nur in der Lage sein rudimentäre Operationen auf Dateien durchzuführen, sondern es kann zur Verwaltung von Datencontainern, für Einstellungen der Sicherheit und zur Informationsgewinnung von Überwachung und Abrechnung genutzt werden.

Die zusätzliche Funktionalität wird auch hier durch Metadaten bereitgestellt. Dabei unterteilen sich diese Metadaten in folgende Felder. Zum einen stützt sich die Schnittstelle, wie schon erwähnt, auf REST ab. Weiterhin sind Dateisystemmetadaten enthalten, die seitens des Kunden erstellt werden. Diese Metadaten enthalten Informationen über angeforderte Datencontainer oder Datenobjekte. Zuletzt sind Benutzerdaten enthalten, welche mit den angeforderten Daten in Verbindung gebracht werden.

Zugriffe auf Datenobjekte erfolgen über eindeutige und bei der Erstellung angelegte Objekt-IDs.

Der Punkt, der als nächstes betrachtet wird, ist die Sicherheit der CDMI. Die Schnittstelle beinhaltet zwei Aspekte der Sicherheit, die bei der Implementierung als obligatorisch angesehen werden. Bei dem ersten Aspekt handelt es sich um die Sicherheit, die bei einem Transport von Daten sichergestellt sein muss und der zweite Aspekt ist die Abfrage von Sicherheitsfähigkeiten. Der konkrete Umfang von Sicherheitsmaßnahmen unterscheidet sich schließlich von Implementierung zu Implementierung.

4.3.3.3 Umsetzung von CDMI

Eine Beispielumsetzung wird in Zusammenarbeit mit dem Open Grid Forum (OGF) entwickelt. Ein Zusammenschluss, der gemeinsame Entwicklungen forciert, indem an Open Source-Projekten gearbeitet wird. Dieser Zusammenschluss liefert einen Beitrag aus dem Bereich Infrastructure as a Service (IaaS) namens Open Cloud Computing Interface (OCCI).

Beide Standards sollen untereinander kompatibel sein. Damit wird ermöglicht, dass über OCCI adressierte Infrastruktur mit Speicherressourcen, die über CDMI verwaltet werden, kommuniziert werden kann.

Ein Beispielszenario (vgl. Abb. 4.4) würde so aussehen, dass ein Client über OCCI mit einer virtuellen Maschine arbeitet, der eine Virtual Machine ID (VM ID) zur weiteren Kommunikation zugeteilt wird. Diese Maschine erhält über Objekt-IDs, die durch CDMI zugeteilt wurden, indirekten Zugriff auf Speicherressourcen, welche zum Beispiel als virtuelle Festplatten zur Verfügung gestellt werden könnten. Andererseits besteht über CDMI die Möglichkeit Daten zu exportieren und damit neue Container anzulegen.

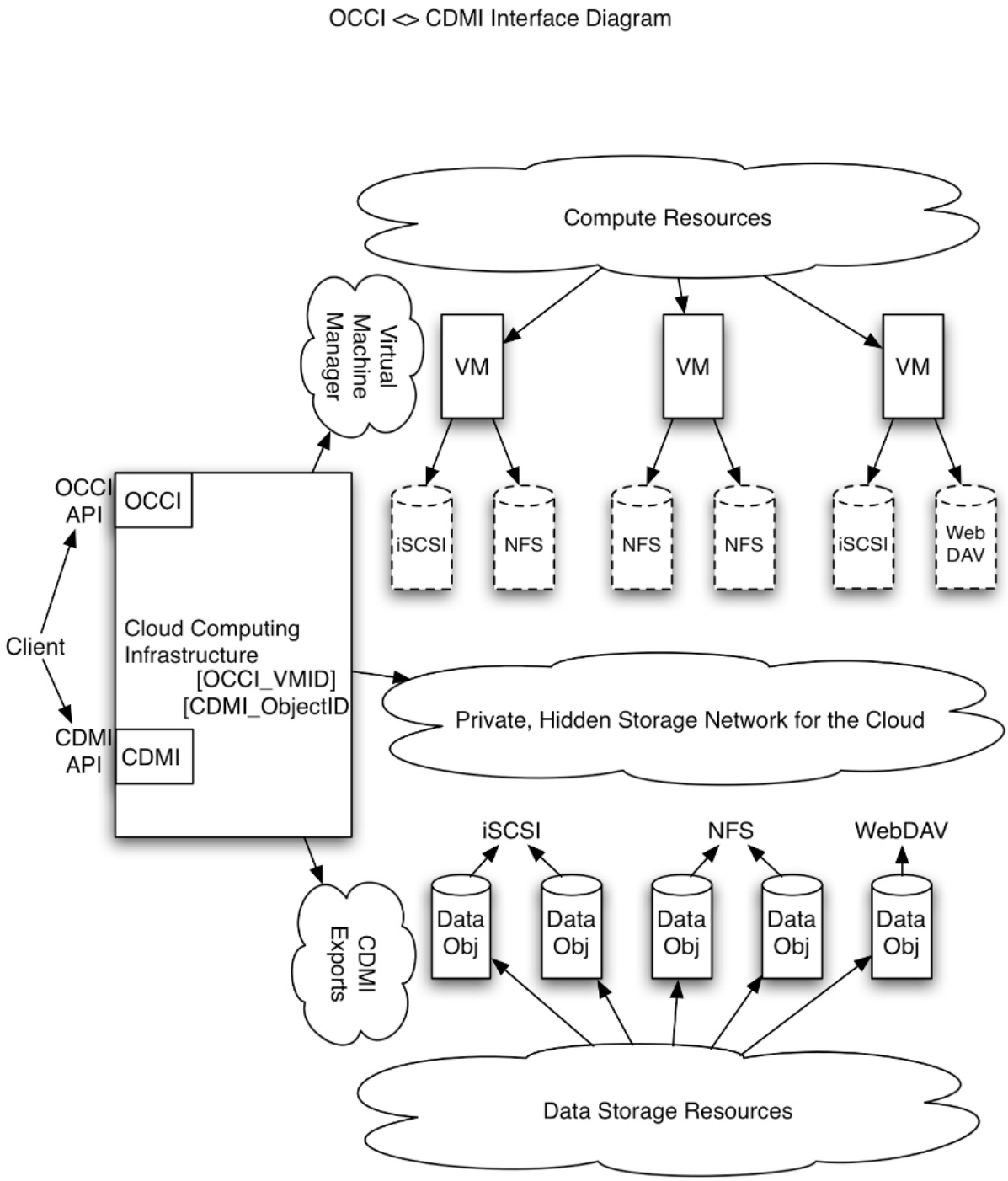

Abbildung 4.4: Zusammenwirken von OCCI und CDMI [15]

4.3.4 Open Grid Forum (OGF)

Das OGF ist eine Gemeinschaft von Anwendern, Entwicklern und Händlern, die sich der Standardisierung im Bereich Grid Computing, eine Form des verteilten Rechnens, bei der ein virtueller Supercomputer aus einem Cluster lose gekoppelter Computer erzeugt wird, widmen.

Die eigentliche Entwicklung eines Standards wird von Zusammenschlüssen gemeinschaftlicher Arbeitsgruppen und führenden Organisationen für Standardisierung betrieben. Obwohl Grid und Cloud Computing nicht gleichzusetzen sind, gibt es eine Arbeitsgruppe, welche sich mit einer Schnittstelle für die Cloud befasst.

4.3.4.1 OCCI Arbeitsgruppe

Ziel der Arbeitsgruppe ist es, eine Schnittstelle zu entwickeln, über welche eine Kommunikation mit einer Cloud-Infrastruktur möglich wird. Es handelt sich dabei also um eine praktische Umsetzung aus dem Bereich IaaS.

Im Fokus der Entwicklung steht eine Umsetzung für die Beschaffung, Überwachung und Definition von Cloud-Diensten. Diese Funktionalität soll der Anwender in Form einer Fernverwaltung erhalten. Konkret wird das OCCI die Funktionalität für die Lebenszyklus Verwaltung virtueller Maschinen zur Verfügung stellen. Ähnlich dem CDMI nutzt das OCCI den bereits existenten Standard REST. Einzelne Ressourcen werden jedoch bei dieser Implementierung über einen Uniform Resource Locator (URL) angesprochen werden.

4.3.5 Open Cloud Consortium (OCC)

Das Open Cloud Consortium (OCC) ist eine Organisation, welche offen für jegliche Mitglieder ist. Sie spielt eine besondere Rolle für Cloud-Standards, denn das OCC stellt seinen Mitgliedern eine Testumgebung zur Verfügung. Diese Testumgebung soll eine möglichst umfangreiche Cloud-Struktur widerspiegeln, an der verschiedene Abläufe des Cloud Computing getestet werden können. Somit liefert das OCC eine wichtige Struktur um geplante Standards ausführlich zu testen.

Des Weiteren bietet das OCC ein Benchmark an, welches für den Einsatz in Cloud Computing vorgesehen ist. Es liefert die Möglichkeit verschiedene Analysen auf eine Cloud-Struktur anzuwenden.

4.3.6 Organization for the Advancement of Structured Information Standards (OASIS)

Die Organization for the Advancement of Structured Information Standards (OASIS) hat ein Technical Committee (TC), welches sich den Sicherheitsstandards des Cloud Computing zuwendet. Das Identity in the Cloud TC entwickelt hauptsächlich Richtlinien für das

Identitätsmanagement des Cloud Computing. Dazu werden Anwendungsfälle aufgestellt, um vorhandene Sicherheitslücken des Identitätsmanagements aufzudecken. Zusätzlich entwickelt das TC Anwendungsfälle für die Bereiche Beschaffung und Verwaltung.

4.3.7 TM Forum

Das TM Forum ist führender Industrie-Verein für Umsetzungen im IT-Dienstleistungssektor. Dabei beschafft das Forum mit Hilfe von Initiativen benötigte Standards.

Die relevante Initiative für Cloud-Standards ist die Cloud Service Initiative (CSI). Diese Initiative hat bereits ein Dokument über IaaS Anforderungen herausgebracht, in dem klar definierte Anforderungen, sowohl für Betreiber als auch für die technische Umsetzung, eines solchen Dienstes beschrieben sind.

Genaue Details zur Umsetzung liegen nicht vor, da das erwähnte Dokument nur TM Forum-Mitgliedern zugänglich ist. An dieser Stelle soll jedoch ein Zitat über den Umfang dieses Dokuments gegeben werden.

> *„This document is a milestone in the realization of Cloud Services. The approach that the ECLC took to write down the needs of the enterprises that can then be used as the basis for how services are defined, ordered, and monitored has the power to enhance collaboration between enterprises and suppliers of external compute IaaS. The key strength of a standardization of interfaces is a win-win-situation for all involved.“*
>
> `Sean Kelley, Deutsche Bank and Chair of TM Forum's ECLC`

4.3.8 Internet Engineering Task Force (IETF)

Die Internet Engineering Task Force (IETF) ist eine große internationale Gemeinschaft von Netzwerkentwicklern, Betreibern, Händlern und Forschern. Mitglieder der IETF sind am Fortschritt des Internets interessiert. Als Organisationsstruktur bestehen Arbeitsgruppen zu verschiedenen Bereichen. Eine konkrete Arbeitsgruppe für die Standardfindung in Cloud Computing gibt es derzeit nicht, aber dennoch gehen aus dem Bereich Internet einige Ausarbeitungen bezüglich der Cloud hervor.

Diese individuellen Ausarbeitungen sind dabei von unterschiedlicher Form, sodass nur ein Teil auf den Prozess der Standardisierung abzielt. Der andere Teil besteht aus reinem Informationsmaterial, wie Umfrageergebnissen.

4.3.9 International Telecommunications Union (ITU)

Die International Telecommunications Union (ITU) ist die führende Agentur der Vereinten Nationen für informations- und kommunikationstechnische Probleme. Die Union operiert

weltweit mit insgesamt 192 Mitgliederstaaten und mehr als 700 weiteren Mitglieder aus dem IT-Bereich. Intern ist die ITU in vier Sektoren untergliedert. Der erste Sektor ist die Radiokommunikation, der zweite ist Standardisierung, der dritte ist Entwicklung und der vierte ist die ITU Telecom, welche eine Messeveranstaltung ist.

Aus dem Sektor Standardisierung geht die Focus Group Cloud (FG Cloud) hervor, welche seit 2010 besteht, deren Ziele im Folgenden aufgelistet sind:

- Feststellung von potentiellen Einflüssen auf die Entwicklung von Standards
- Ermittlung von Bedarf an zukünftigen Forschungsgegenständen für feste und mobile Netzwerke
- Herausstellung der Komponenten, die am meisten von einer Standardisierung profitieren würden
- Analyse von Fortschrittsraten von Cloud Computing-Attributen um angemessene Zeitpunkte für einen Standard zu finden

Wie bereits zu erkennen ist, legt sich die FG Cloud auf keinen genauen Bereich des Cloud Computing fest. So umfasst das Gebiet der Forschungsgruppe Sicherheit, Anforderungsanalyse, Infrastruktur und Ressourcenmanagement. Die Gruppe hat bereits einen Entwurf online gestellt, der leider nur Mitgliedern zugänglich ist.

4.3.10 European Telecommunications Standards Institute (ETSI)

Das European Telecommunications Standards Institute (ETSI) ist das offiziell anerkannte Institut für Standardisierung im IT-Bereich der Europäischen Union. Es ist nicht kommerziell und hat über 700 Mitglieder.

Bisher gibt es lediglich eine Veröffentlichung unter dem Namen „Initial analysis of standardization requirements for Cloud services“, diese ist jedoch sehr abstrakt und knapp. Von daher wird nicht näher auf diese Veröffentlichung eingegangen.

4.3.11 Object Management Group (OMG)

Die Object Management Group (OMG) ist eine unkommerzielle, internationale und offene Gruppe, welche der Standardfindung in der Computerbranche dient.

Bisher initiierte die OMG ein technisches Treffen im Dezember 2009, an dem ein Großteil der wichtigen Standardisierungsgruppen teilnahmen. Dieses Treffen ist Teil des Cloud Interoperability Roadmap Process (CIRP), welcher in Zukunft die Richtung der Standardisierung im Bereich IaaS vorgeben soll. Ziel dieses Treffens war es einen gemeinschaftlichen Plan für die Verbesserung der Kompatibilität zu erstellen. Der Hintergrund ist, dass sich

die Funktionalität der Schnittstellen für IaaS bei einigen Entwürfen überschneidet und nur in spezifischen Details unterscheidet. So sollte mit dem Treffen ein grober Konsens getroffen werden.

4.4 Standards im Bereich Sicherheit

Der Faktor Sicherheit ist für jeden Nutzer von Cloud-Diensten von Bedeutung. Die aktuelle Lage ist dabei noch relativ undurchschaubar, denn es gibt keine Einigung auf feste Sicherheitsrichtlinien. Dabei muss man jedoch die verschiedenen Anwendungsfälle der Cloud-Dienste betrachten. Nicht jeder Dienst ist potentiell mit gleich schwerwiegenden Sicherheitsrisiken behaftet.

Wir unterscheiden dabei folgende drei Modelle. Zum ersten IaaS, welches die niedrigste Ebene ist, auf der Schnittstellen vereinbart werden müssen, auf denen höhere Ebenen aufbauen. Hier herrscht am meisten Flexibilität für eine eigene Implementierung, da nur die Hardwareebene durch einen Cloud-Anbieter realisiert wird. Dadurch ist hierbei der Kunde zum größten Teil für die Sicherheit mitverantwortlich.

Die zweite Ebene ist Platform as a Service (PaaS). Diese Ebene ist im höheren Maße erweiterbar als IaaS, denn auf die Software kann der Kunde direkt zugreifen. Das bedeutet, dem Kunden wird hier die Möglichkeit gegeben eigene Sicherheitsschichten zu implementieren.

Die letzte Ebene ist SaaS. Es handelt sich hierbei um das am meisten eingeschränkte Modell, da es eine detaillierte Implementierung seitens des Anbieters zur Verfügung stellt, die einem bestimmten Zweck dienen soll. Wir sprechen bei diesem Modell auch von der höchsten Integrationsstufe. Nun liegt die Verantwortung für die Sicherheit in diesem Modell auf der Seite des Anbieters.

Die drei verschieden Stufen der Implementierung sagen aus, dass es unterschiedliche Anforderungen an die Sicherheit gibt. Grundsätzlich werden Sicherheitslücken mit dem Grad der Implementierung vererbt.

Es stellt sich die Frage, welche Bedingungen ein Sicherheitsstandard für die verschiedenen Anwendungsfälle erfüllen muss.

Es ist offensichtlich, dass mit Einführung von Cloud-Diensten ein erhöhter Bedarf an Sicherheit verlangt wird. Ein Unternehmen welches sich dazu entscheidet Zweige in die Cloud auszulagern, wird wissen wollen, welche Sicherheitsvorkehrungen auf Anbieterseite getroffen wurden. An dieser Stelle muss man noch die privaten Clouds von den öffentlichen Clouds unterscheiden. Sobald Daten in ein Netzwerk öffentlicher Clouds gegeben werden, kann der Kunde nicht mehr nachvollziehen wo seine Daten gespeichert werden. Mit anderen Worten, der Kunde muss seinem Cloud-Anbieter in erster Linie vertrauen. Der Anbieter wird verschiedene Hürden zu überwinden haben, bis er als nachweislich sicher gilt.

4.4.1 Datenintegrität

Dort wo Daten eines Kunden liegen, da liegen auch Daten eines anderen Kunden. Der Anbieter muss sicherstellen, dass verschiedene Daten ausreichend voneinander getrennt werden. Grundsätzlich müssen gespeicherte Daten ausreichend verschlüsselt sein.

4.4.2 Datenverfügbarkeit

Ein weiterer Punkt um Sicherheit zu gewährleisten ist das Wiederherstellungsverfahren des Anbieters. Im schlimmsten Fall gehen dem Anbieter Datensätze komplett verloren. Er muss dann in der Lage sein sofort Ersatz in Form einer Sicherheitskopie bereitzustellen. Wir könnten uns ein solches Szenario jedoch auch ohne den direkten Ausfall eines Dienstes vorstellen und zwar genau dann wenn der Cloud-Anbieter an sich nicht mehr stabil ist. Die Gründe sind vielfältig. Ein Anbieter könnte finanzielle Schwierigkeiten bekommen oder von einem größeren Anbieter übernommen werden. Wie bleibt dennoch garantiert, dass die bis dahin gespeicherten Daten dem Kunden verfügbar bleiben?

4.4.3 Identität und Zugangsmanagement

Sobald die Daten einer Firma nicht mehr auf eigenen Servern liegen, fehlen Informationen über deren Verwaltung. Der Zugang zu netzwerkspezifischen Daten wie Log-Dateien wird dadurch erschwert. Wir nehmen an, dass eine Firma auch Ermittlungen bezüglich ihrer eigenen Daten anstellen und forensische Daten sammeln will. Ein Beispiel für ein vorhandenes Problem ist die im DNS-Speicher verbleibende IP eines Kunden, nachdem er eine neue IP zugeteilt bekommen hat. Es wäre einem Angreifer möglich die alte IP zu erlangen und damit Zugang zu fremden Daten zu bekommen.

Die CSA untergliedert das Thema Identität und Zugangsmanagement in die Bereiche Identitätsbeschaffung, Authentifizierung, Föderation, Zugangskontrolle und Identity as a Service (IDaaS).

4.4.3.1 Identitätsbeschaffung

Dieser Bereich beschäftigt sich mit der Zuteilung und Wiederfreigabe von Cloud-Diensten für verschiedene Benutzergruppen. Grundsätzlich muss ein Benutzer sich sicher identifizieren können, dazu würde es sich anbieten bereits vorhandene Standards zu nutzen, die für den Bereich der Benutzerverwaltung ausgelegt sind. Ein etablierter Industriestandard für eine solche Verwaltung wäre die Service Provisioning Markup Language (SPML). Es soll weiter möglich sein verschiedene Benutzergruppen zu führen, die jeweils unterschiedlich privilegiert sind. Der Benutzer braucht also einen Dienst, welcher in der Lage ist ihn eindeutig zu identifizieren. Entweder wird ein solcher Dienst durch den Cloud-Anbieter gestellt, oder aber der Benutzer hat bereits einen externen Dienst, der diese Aufgabe übernehmen kann. Auch der Kommunikationsweg zwischen Benutzer und Anbieter sollte

möglichst jeder Zeit gesichert sein. Hierzu würde sich eine einfache SSL Verschlüsselung anbieten.

Es ist für Benutzer empfehlenswert sich an Standardumsetzungen zu halten, statt einen Anbieter zu wählen, der ein auf sich zugeschnittenes System der Identitätsbeschaffung ausführt.

4.4.3.2 Authentifizierung

Dies ist der Prozess der über die Gültigkeit einer Berechtigungsanfrage entscheidet.

Dieser Prozess muss sich bei einer Standardfindung unter folgenden Aspekten bewähren. Die Aspekte sind zum Beispiel ausreichender Schutz von Benutzerpasswörtern, unterschiedliche Passwörter für verschiedene Cloud-Dienste, Schutz vor primitiven Angriffen wie Brute Force und Phishing. Alle diese Anforderungen sind für Internetdienste üblich. Ein konkreter Vorschlag für eine sichere Authentifizierung wäre die Nutzung von Virtual Private Network (VPN).

4.4.3.3 Föderation

Föderative Fähigkeiten werden für interne Kommunikation von Cloud-Diensten benötigt. Die Notwendigkeit dafür entsteht durch die vernetzte Struktur. Der Cloud-Anbieter kann mit dieser Fähigkeit beispielsweise mit einem externen Identitätsbeschaffungsdienst kommunizieren und Details über den Benutzer austauschen. Weiterhin kann damit erreicht werden, dass ein Benutzer sich nur einmal authentifizieren muss, obwohl sein Cloud-Dienst über weitere Cloud-Strukturen verfügt, die von ihm isoliert sein können. Dieses Prinzip ist bekannt unter dem Namen Single Sign-On (SSO).

Es gibt mehrere Möglichkeiten für föderative Standards.

Für die öffentliche Cloud-Variante werden Standards wie Security Assertion Markup Language (SAML) und Web Services-Federation (WS-Federation) genutzt. Für die private Cloud-Variante kann ein VPN genutzt werden um ein SSO zu nutzen.

4.4.3.4 Zugangskontrolle

Es wird mehrere Nutzermuster geben, die bedient werden müssen. Jedes Nutzerprofil wird Attribute beinhalten, welche Variationen von Nutzerrechten ermöglichen.

Wir unterscheiden grundsätzlich zwischen privaten und dienstlichen Nutzern.

Der private Nutzer hat seine Rechte und Einschränkungen direkt im Blick und soll in der Lage sein, diese selbstständig anpassen zu können.

Der dienstliche Nutzer bekommt seine Rechte über seine Firma zugeteilt, welche sich um die Nutzerverwaltung kümmern muss.

Die Herausforderung wird sein, die Zugänge trotz verschiedener Quellen des Nutzermanagements richtig einzuordnen.

4.4.3.5 Identity as a Service

IDaaS könnte als externer Dienst für die Verwaltung von Identitäten den gesamten Funktionsbereich der Identitätsverwaltung abdecken. Dazu gehört das Lebenszyklus-Management und die Funktionalität der einmaligen Anmeldung.

Es wird, wie bei der Zugangskontrolle bereits beschrieben, zu diversen Problemen durch unterschiedliche Quellen kommen.

Entweder der Nutzer ist Mitarbeiter einer Firma, Kunde einer Firma oder nutzt einen Cloud-Dienst privat.

Im ersten Fall muss bei der Umsetzung von IDaaS über die Sicherheit und den Datenschutz von Daten über Angestellte nachgedacht werden. Die öffentliche Zugänglichkeit des Dienstes bereitet nicht weniger Risiken. Der Zugriff auf firmeninterne Strukturen muss geschützt bleiben. Alle Sicherheitsvorkehrungen einer Firma, die nun Cloud-Dienste nutzen möchte, müssen weiterhin umgesetzt werden.

Für Firmenkunden muss ein zuverlässiger Umgang mit ihren Daten gewährleistet sein. Des Weiteren müssen nötige Informationen verfügbar sein, wenn ein Kunde einen bestimmten Dienst nutzen möchte.

Privaten Nutzern soll es ermöglicht werden sich mit bereits existierenden Zugangsdaten zu authentifizieren. So kann ein Dienst wie OpenID als Schnittstelle für die Authentifizierung und den Austausch relevanter Informationen genutzt werden.

Zusammenfassend ist zu sagen, dass existierende Methoden des Identitätsmanagement beibehalten werden sollten und ein zusätzliches Augenmerk auf die Bereiche Datenschutz und Datenintegrität gelegt werden muss.

4.4.4 SLA

Ein Service-Level-Agreement (SLA) ist ein Vertrag zwischen einem Benutzer und einem Anbieter, in welchem festgehalten wird, was der Benutzer vom Anbieter verlangen kann. Auch Cloud-Dienste werden solche SLA brauchen, wenn es um den Kern einer Dienstleistung geht. Der Kern eines Cloud-Dienstes besteht aus den folgenden fünf Sektoren:

- Beschaffung
- Bemessung und Abrechnung
- Sicherheit
- Qualität

- Identität

Ein SLA für Cloud-Dienste müsste erst noch zusammengestellt werden, von daher stellt sich auch hier die Frage nach Standards. Leitgedanke für meine weitere Betrachtung soll der Aspekt Sicherheit sein.

Dem Kunden eines Cloud-Dienstes muss ersichtlich sein, mit welchen Mitteln für seine Sicherheit im Umgang mit dem angebotenen Dienst gesorgt wird. Unter Ausschluss verschiedener Risiken soll dem Kunden ein Dienst transparenter gemacht werden.

Es folgen nun einige Anhaltspunkte für den Ausschluss unterschiedlichster Risiken.

Ein Kunde, der zum Beispiel vertrauliche Daten in die Hände von einem Cloud-Anbieter übergibt, will wissen wo seine Daten gespeichert werden, wer darauf verwaltend zugreifen kann und welche zusätzlichen Metadaten angelegt werden. Gerade die Frage nach dem Ort der Speicherung muss aus rechtlichen Gründen eindeutig geklärt sein.

Als nächstes möchte der Kunde wissen, welche Sicherheitsmechanismen der Anbieter anwendet. Am besten wäre es, wenn Zertifikate bereitstehen würden, die ein ausgiebiges Testen seitens des Anbieter bestätigen würden. In jedem Fall muss für ausreichenden Schutz in Form einer Verschlüsselung gesorgt werden. Zudem müssen Daten unterschiedlicher Kunden strikt voneinander isoliert sein. Nicht nur die Daten soll ein Kunde geschützt wissen, sondern auch die Struktur des Cloud-Dienstes. So wird von Interesse sein, wie es um die Netzwerksicherheit des Anbieters steht. Im besten Falle wird es ein separates Team von Sicherheitsexperten eines Security Operation Centers geben, die ein Netzwerk überwachen.

Ein Punkt, der in jedem Fall im SLA abgehandelt werden muss, ist die Datenkonsistenz, für den Fall, dass ein Dienst die Daten eines Kunden wiederherstellen muss. Gründe dafür gibt es sicherlich mehrfach. Dem Kunden muss also eine Versicherung für den Erhalt seiner Daten gegeben werden.

Abschließend ist zu sagen, dass der Kunde zum Teil selbst verantwortlich für die Sicherheit seiner Daten ist, denn er muss sich über die genannten Punkte informieren und anhand dieser Kriterien einen geeigneten Anbieter wählen. Wenn möglich sollte ein Anbieter gewählt werden, der regelmäßig von einer unabhängigen Einrichtung auf seine Sicherheit geprüft wird.

4.5 Fazit

Aus dieser Erarbeitung soll die Wichtigkeit für Standards in diesem relativ neuen Bereich der IT-Branche hervor gehen. Verdeutlicht wurde dies anhand des nachteiligen Effekt des „Vendor Lock-In“, der Masse an Organisationen, welche sich intensiv bemühen Richtlinien zu erarbeiten, und mithilfe der noch nicht vollständig geklärten Probleme im Bereich Sicherheit.

Das Ziel der zukünftigen Cloud-Landschaft sollte es sein, die Umsetzung angebotener Dienste durch Standards zu festigen. Dies würde den Sektor in vielerlei Hinsicht bereichern. Es ist ein Ausdruck der Weiterentwicklung und vor allem der Ausgereiftheit. Zudem wird vieles für den Nutzer übersichtlicher und transparenter werden.

Die Organisationen, die Standards beisteuern, sind nicht primär profitorientiert, sondern an einem gemeinschaftlichen Prozess der Standardisierung interessiert, der vielen Anbietern und Nutzern zugute kommen wird. Beste Beispiele hierfür sind der CIRP, der OMG, welcher einen gemeinsamen Weg vieler Standardisierungsorganisationen bewirken soll, oder aber die Zusammenarbeit von dem SNIA und dem OGF, aus welcher eine konkrete Umsetzung zweier untereinander kompatibler Schnittstellen entsteht.

Wie bereits durch die Gewichtung in dieser Erarbeitung kenntlich gemacht, lässt der Bereich der Sicherheit noch viele Fragen offen. Um großen Unternehmen eine Transformation in Richtung Cloud schmackhaft zu machen, muss nach meiner Meinung noch einiges für die Gewährleistung zufriedenstellender Sicherheit klarer werden. Auch die Service-Level-Agreements für Cloud-Dienste hängen stark mit der Sicherheit zusammen, sind aber, wie im Abschnitt über SLA verdeutlicht, zur Zeit nicht zufriedenstellend beziehungsweise nicht vorhanden.

Aus meiner Sicht ist die relativ neue Branche des Cloud Computing sehr mächtig und zukunftsweisend. Die Entwicklung von Standards ist mit dieser Einschätzung eng verknüpft, denn sie wirkt förderlich. Während meiner Auseinandersetzung mit meiner Arbeit bin ich zu der Ansicht gelangt, dass es relativ viele Organisationen gibt, die an Cloud-Standards teilhaben möchten. Dabei können die Bereiche der Standardfindung sehr verschieden sein, wodurch sie jeweils unterschiedlich stark abgedeckt werden. Für einige Bereiche gibt es zur Zeit noch nicht genügend konkrete Ansätze.

Literaturverzeichnis

[1] Brandel, Mary. *The Trouble with Cloud: Vendor Lock-in*, http://www.cio.com/article/488478/The_Trouble_with_Cloud_Vendor_Lock_in?page=1&taxonomyId=3112, Stand: 22.02.2011.

[2] Cloud Security Alliance. http://www.cloudsecurityalliance.org, Stand: 22.02.2011.

[3] Cloud Standards Wiki. http://www.cloud-standards.org, Stand: 22.02.2011.

[4] CSA. *Guidance for Identity & Access Management V2.1*, http://www.cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf, Stand: 22.02.2011.

[5] Distributed Management Task Force. http://www.dmtf.org, Stand: 22.02.2011.

[6] DMTF. *Interoperable Clouds*, http://www.dmtf.org/sites/default/files/standards/documents/DSP-IS0101_1.0.0.pdf, Stand: 22.02.2011.

[7] European Telecommunications Standards Institute. http://www.etsi.org, Stand: 22.02.2011.

[8] International Telecommunications Union. http://www.itu.int, Stand: 22.02.2011.

[9] Internet Engineering Task Force. http://www.ietf.org, Stand: 22.02.2011.

[10] Kandukuri, B. Reddy; Paturi, V. Ramakrishna; Dr. Rakshit, Atanu. *Cloud Security Issues*, http://dx.doi.org/10.1109/SCC.2009.84, Stand: 22.02.2011.

[11] Mather, Tim; Kumaraswamy, Subra; Latif, Shahed. *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*, 1. Auflage, O'Reilly Media, 2009.

[12] McKay, Dimitri. *Cloud Service SLA Survival Tips - What should you be asking your cloud provider?*, http://www.securityweek.com/cloud-service-sla-security-tips-what-should-you-be-asking-your-provider, Stand: 22.02.2011.

[13] Object Management Group. http://www.omg.org, Stand: 22.02.2011.

[14] OCCI Working Group. *Open Cloud Computing Interface*, http://www.gridforum.org/Public_Comment_Docs/Documents/2010-01/occi-core.pdf, Stand: 22.02.2011.

[15] OGF und SNIA. *Cloud Storage for Cloud Computing*, http://www.snia.org/cloud/CloudStorageForCloudComputing.pdf, Stand: 22.02.2011.

[16] Open Cloud Consortium. http://www.opencloudconsortium.org, Stand: 22.02.2011.

[17] Open Grid Forum. http://www.ogf.org, Stand: 22.02.2011.

[18] Organization for the Advancement of Structured Information Standards. http://www.oasis-open.org, Stand: 22.02.2011.

[19] SNIA. *Cloud Data Management Interface*, http://www.snia.org/tech_activities/standards/curr_standards/cdmi/CDMI_SNIA_Architecture_v1.0.pdf, Stand: 22.02.2011.

[20] Storage Networking Industry Association. http://www.snia.org, Stand: 22.02.2011.

[21] TM Forum. http://www.tmforum.org, Stand: 22.02.2011.

Kapitel 5

Rechtliche Rahmenbedingungen des Cloud Computing

Achim Fischbach

Im Abschnitt „Rechtliche Rahmenbedingungen des Cloud Computing“ werden die juristischen Regelungen, denen Cloud Computing unterworfen ist, dargestellt. Auf Grund fehlender internationaler und nationaler Bestimmungen diesbezüglich ist es erforderlich, hier die verschiedensten Gesetze, die die Ausgestaltung und Nutzung des Cloud Computing betreffen könnten, zu überprüfen. Ein wichtiger Aspekt ist die Festlegung, welches Gesetz bei der Nutzung einer Cloud überhaupt Anwendung findet. Desweiteren muss der Datenschutz betrachtet werden, um Fragen bezüglich der Sicherheit der in der Cloud gelagerten Informationen zu beantworten. Um den Nutzern einer Cloud eine gewisse Sicherheit bei der Auswahl der Anbieter zu geben, können Zertifizierungen berücksichtigt werden, welche gegen Ende des Abschnittes erläutert werden. Zuletzt erfolgt ein Ausblick, wie sich die gesetzlichen Regelungen in Bereich des Cloud Computing entwickeln könnten.

Inhaltsverzeichnis

5.1 Einleitung

Dieses Kapitel behandelt die rechtlichen Rahmenbedingungen des Cloud Computing. Da vom Gesetzgeber noch keine entsprechende Rechtsprechung vorliegt, gilt es, hier sorgfältig die verschiedenen beeinflussenden Gesetze zu beachten und die rechtlichen Grenzen, denen das Cloud Computing in Deutschland unterliegt, auszuloten. Diese sind gerade im Bezug auf Ländergrenzen überschreitende IT-Strukturen ein nicht zu unterschätzendes Problem. Hier stellt sich dann spätestens die Frage, welches spezielle Recht anzuwenden ist, ob z.B. das Recht des Landes desjenigen, der die Daten hoch lädt, das Recht des Landes, in dem die Daten gespeichert sind oder des Landes, in dem sich der Sitz des anbietenden Unternehmens befindet. Komplizierter kann es noch werden, wenn der Anbieter selbst nicht über die Ressourcen verfügt, sondern über einen Dritten Kapazitäten mietet. Durch mangelnde international gültige Rechtsnormen muss von Fall zu Fall geprüft werden, welches Recht anzuwenden ist. Nichtsdestotrotz kann auch vieles durch eine ausführliche Ausgestaltung des Vertrages zwischen Nutzer und Anbieter der Leistungen abgedeckt werden.

Zum einen haben wir hierbei die diversen Datenschutzgesetze wie das Bundesdatenschutzgesetz oder die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr der europäischen Gemeinschaft. Alleine diese Gesetze müssen schon eine Vielzahl von Gesichtspunkten bezüglich Cloud Computing abdecken, da Firmen und Privatpersonen ihre Daten in die Cloud verlagern können, dabei jedoch keineswegs immer sicher ist, wo diese sich aufhalten, ob alle Daten an einem oder mehreren Orten liegen und wer darauf Zugriff hat. Dies kann zu einer fehlenden Kontrollierbarkeit über die eigenen Daten führen, die auf fremden Servern liegen. Ebenso müssen die Datenintegrität und die Absicherung des Zugriffs sichergestellt sein.

Es gibt jedoch noch weit mehr gesetzliche Regelungen, die das Arbeiten mit einer Cloud beeinträchtigen, wie etwa Verbraucherschutzgesetze, das Strafgesetzbuch, die Abgabenordnung, das Bürgerliche Gesetzbuch (hierbei insbesondere im Bezug auf Miet-, Pacht- und Werkverträge), das Urheberrecht, das Handelsgesetzbuch und weitere.

Diese Regelungen beziehen sich jedoch nicht nur auf klassische Clouds, sondern ebenso auf andere persönliche Daten, die man im World Wide Web hoch lädt, wie persönliche Bilder bei Facebook oder Videos bei YouTube, wobei der Nutzer hier selten einen Einfluss auf die Verwendung seiner Daten oder die technische Ausgestaltung nehmen kann, da diese, wenn überhaupt, über die AGB definiert sind.

Eine gewisse Sicherheit kann man durch Betrachtung von Zertifikaten in Frage kommender Cloud-Anbieter gewinnen. Im Vordergrund stehen hier etwa ISO/IEC 27001 oder SAS 70. Hierbei muss dennoch darauf geachtet werden, wer die Auditierung durchgenommen hat und ob die Zertifizierungen dem gewünschten Maß an die Datensicherheit entsprechen, da die Zertifikate meist nur ein Mindestmaß abdecken.

5.2 Welches Recht gilt?

Einer der wesentlichsten Punkte, wenn man sich mit den rechtlichen Rahmenbedingungen von Cloud Computing beschäftigt, ist die Frage, welches Recht überhaupt Anwendung findet. Gilt das Recht des Landes, aus dem der Nutzer stammt, oder das, in dem der Anbieter seinen Sitz hat? Oder gilt das Recht von der Nation, in der die Daten lagern oder aus der die Cloud-Ressourcen stammen, wenn diese separat vom Anbieter sind?

Oft sind Clouds grenzüberschreitend, sowohl was die Kunden, die Ressourcen als auch die Daten betrifft. Um dennoch eine gesetzliche Regelung garantieren zu können, muss sich, teils vertraglich durch die verschiedenen Parteien, auf das geltende Recht eines Landes geeinigt werden. Im Allgemeinen können die Vertragspartner frei wählen und sich somit das für beide am attraktivsten wirkende Recht aussuchen, um sich eine größtmögliche Rechtssicherheit zu geben. Innerhalb der Europäischen Union wurden diesbezüglich schon Richtlinien bezüglich des Datenschutzes o.ä. vorgegeben, damit sich zumindest in diesem Gebiet Cloud-Nutzer und -Anbieter einer gewissen Rechtssicherheit erfreuen können.

Bei vielen angebotenen Diensten wie Blogs, Google Apps oder Freemail-Diensten besteht jedoch keine Verhandlungsbasis auf Augenhöhe, da der Nutzer nur entweder die Vertragsbedingungen, dies entspricht in der Regel den Allgemeine Geschäftsbedingunen (AGB) nach Richtlinie 93/13/EWG, annehmen oder auf den Dienst verzichten kann. Er hat somit keinen Einfluss auf die technische und rechtliche Ausgestaltung.

Nichtsdestotrotz können nach der Verordnung (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Kurzbezeichnung Rom-I-Verordnung) Verbraucher und Unternehmer das anzuwendende Recht frei wählen, wodurch dem Verbraucher dennoch kein wesentliches Schutzrecht genommen werden darf. Durch das deutsche Recht und dessen hohe Schutzstandards dürfte dem Verbraucher zuzüglich eine hohes Maß an Schutz bezüglich der Rechtswahl zur Verfügung stehen.

Zu berücksichtigen ist hierbei die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, kurz Europäische Datenschutzrichtlinie (EU-DSRL), ergänzt durch die Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation):

Das Datenschutzrecht ist im Allgemeinen an den Ort der Datenverarbeitung geknüpft. Die EU-DSRL besagt jedoch, dass eine grenzüberschreitende Datenverarbeitung innerhalb der Europäischen Union kein rechtliches Hindernis mehr darstellen soll. Artikel 1 EU-DSRL besagt:

> *„(1) Die Mitgliedstaaten gewährleisten nach den Bestimmungen dieser Richtlinie den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten.*
>
> *(2) Die Mitgliedstaaten beschränken oder untersagen nicht den freien Verkehr personenbezogener Daten zwischen Mitgliedstaaten aus Gründen des gemäß Absatz 1 gewährleisteten Schutzes.“*

Um einer Rechtebeschneidung durch Überschreitung nationaler Grenzen ("Race to the bottom") zuvorzukommen, behandelt Artikel 4 EU-DSRL das anwendbare einzelstaatliche Recht:

> *„(1) Jeder Mitgliedstaat wendet die Vorschriften, die er zur Umsetzung dieser Richtlinie erläßt, auf alle Verarbeitungen personenbezogener Daten an,*
>
> *a) die im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaats besitzt. Wenn der Verantwortliche eine Niederlassung im Hoheitsgebiet mehrerer Mitgliedstaaten besitzt, ergreift er die notwendigen Maßnahmen, damit jede dieser Niederlassungen die im jeweils anwendbaren einzelstaatlichen Recht festgelegten Verpflichtungen einhält;*
>
> *b) die von einem für die Verarbeitung Verantwortlichen ausgeführt werden, der nicht in seinem Hoheitsgebiet, aber an einem Ort niedergelassen ist, an dem das einzelstaatliche Recht dieses Mitgliedstaats gemäß dem internationalen öffentlichen Recht Anwendung findet;*
>
> *c) die von einem für die Verarbeitung Verantwortlichen ausgeführt werden, der nicht im Gebiet der Gemeinschaft niedergelassen ist und zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind, es sei denn, daß diese Mittel nur zum Zweck der Durchfuhr durch das Gebiet der Europäischen Gemeinschaft verwendet werden.“*

Sollte sich eine Daten verarbeitende Stelle außerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraumes (EWR) befinden, so kann einem im Inland ansässigen Vertreter gegenüber nach § 1 Abs. 5 Bundesdatenschutzgesetz (BDSG) das anwendbare nationale Datenschutzrecht geltend gemacht werden:

> *„[...]Dieses Gesetz findet Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Soweit die verantwortliche Stelle nach diesem Gesetz zu nennen ist, sind auch Angaben über im Inland ansässige Vertreter zu machen.[...]“*

Es ist allerdings nicht immer gegeben, dass bei grenzüberschreitendem Cloud Computing überhaupt rechtliche Regelungen zum Datenschutz bestehen. Da sogar die Möglichkeit besteht, dass sich Cloud-Ressourcen außerhalb eines nationalen Gebietes befinden (Hochsee), gibt es gar keinen gesetzlichen Persönlichkeitsschutz.

5.3 Datenschutz

Ein wichtiger Punkt bei der Betrachtung der rechtlichen Rahmenbedingungen des Cloud Computing ist die Vertraulichkeit der Datenverarbeitung. Diese betrifft nicht nur personenbezogene Daten, sondern auch sämtliche Daten, die ein hohes Maß an Vertraulichkeit und Integrität erfordern, wie beispielsweise Betriebs- und Geschäftsgeheimnisse, Unterlagen von Behörden, Forschungsdaten oder anderweitig geschützte Daten. Im Hinblick auf die datenschutzrechtliche Verarbeitung muss auch der Schutz der Daten von Kunden, Beschäftigten, Lieferanten, Geschäftspartnern etc. sichergestellt sein. Hierbei ist der Schutz vor unerlaubten Zugriffen von immenser Wichtigkeit.

Das Datenschutzrecht behandelt nur personenbezogene Daten gemäß § 3 Abs. 1 BDSG:

> *„Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).“*

Neben diesem muss in Bezug auf Nutzungsdaten das Arbeitnehmerschutzrecht beachtet werden.

5.3.1 Anonymisierung und Pseudonymisierung

Bei einer genügenden Anonymisierung personenbezogener Daten nach § 3 Abs. 6 BDSG findet das Datenschutzrecht keine Anwendung. Hierbei ist jedoch höchste Vorsicht walten zu lassen, da diese Daten durch Verarbeitung in der Cloud reidentifizierbar werden können, da andere Cloud-Nutzer bzw. die Anbieter der Cloud-Dienste und -Ressourcen über zusätzliches Wissen verfügen. Da es sich heute mit nicht allzu hohem Aufwand bewerkstelligen lässt, durch Verknüpfungen im Netz nicht eindeutig identifizierbare Daten zu verbinden und einer konkreten Person zuzuordnen, wird dies auch innerhalb einer Cloud prinzipiell möglich sein. Dadurch werden auch getrennte, für sich nicht zuordenbare Datensätze unsicher und können somit nicht mehr Datenschutzrichtlinien erfüllen. Durch die elektronische Auswertbarkeit und die Integration in ein größeres Netzwerk ergibt sich eine höhere Wahrscheinlichkeit, dass die Daten zur Identifizierung durch Unbefugte genutzt werden können. Eine Möglichkeit, das Schutzniveau zu erhöhen und eine Zuordnung der Daten zu erschweren, ist eine Pseudonomysierung nach § 3 Abs. 6 BDSG, d.h. „ein Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.“

5.3.2 Verantwortlichkeit

Die Verantwortlichkeit in der Cloud ist durch das BDSG und durch die EU-DSRL bestimmt. Das BDSG bestimmt in § 3 Abs. 7:

> *„Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.“*

Die EU-DSRL unterscheidet sich hier leicht und erklärt in Art. 2 d) Für sie bezeichnet der Ausdruck:

> *„ „für die Verarbeitung Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. [...]“*

Verantwortlich ist hiernach in der Regel der Cloud-Nutzer, da sich die Verantwortlichkeit nicht auf den dem Nutzer zur Verfügung stehenden Einflussbereich beschränkt, sondern auch die Auftragsdatenverarbeitung mit einschließt.

Sollte es zu Datenschutzverstößen kommen, ist der Cloud-Nutzer nach § 42a BDSG dazu verpflichtet, den Betroffenen und die zuständige Aufsichtsbehörde darüber aktiv zu informieren. Des Weiteren muss die „Benachrichtigung des Betroffenen [...] unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird.“ Hierin enthalten sein muss eine Beschreibung der Art der unrechtmäßigen Kenntniserlangung und eine Empfehlung für Maßnahmen zur Minderung möglicher nachteiliger Folgen.

5.3.2.1 Auftragsdatenverarbeitung

Durch die Auftragsdatenverarbeitung wird der Cloud-Nutzer auch verantwortlich für die Einhaltung der Datenschutzregelungen, d.h. er kann z.B. bei unrechtmäßigem Gebrauch von Daten auch zu Schadenersatz nach dem BDSG verklagt werden. Dies wird in § 11 Abs. 1 BDSG verdeutlicht:

> *„Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.“*

Nach Art. 17 Abs. 2 EU-DSRL sehen die Mitgliedsstaaten vor, dass

> *„der für die Verarbeitung Verantwortliche im Fall einer Verarbeitung in seinem Auftrag einen Auftragsverarbeiter auszuwählen hat, der hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen ausreichende Gewähr bietet; der für die Verarbeitung Verantwortliche überzeugt sich von der Einhaltung dieser Maßnahmen.“*

Dies wird in Deutschland durch § 11 BDSG geregelt. Auftragsdatenverarbeitung liegt nicht vor, wenn der Empfänger ein Dritter gemäß § 3 Abs. 8 BDSG ist:

> *„[...]Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle.[...]“*

In diesem Fall trifft § 11 BDSG nicht zu. Jedoch müssen die rechtlichen Bedingungen an eine Datenübertragung (§ 3 Abs. 4 Nr. 4 BDSG) erfüllt sein.

Die Auftragsdatenverarbeitung (im übrigen auch die Funktionsübertragung) ist noch an bestimmte Anforderungen geknüpft, welche am 01. Januar 2009 in § 11 Abs. 2 BDSG konkretisiert wurden. Im Vertrag, der zwischen Cloud-Nutzer und -Anbieter vereinbart wird, müssen der Gegenstand und die Dauer des Auftrags, der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen, die nach § 9 BDSG zu treffenden technischen und organisatorischen Maßnahmen, die Berichtigung, Löschung und Sperrung von Daten, die nach Abs. 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen, die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen, die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers, mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen, der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält sowie die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags festgelegt sein.

Da es sich bei Cloud Computing um eine Auftragsdatenverarbeitung nach § 11 BDSG handelt, ist der Auftraggeber, also der Kunde, für die Vertraulichkeit und die Integrität der Daten verantwortlich. Da er aber in der Regel bei der Nutzung von Cloud Computing weder vollständig über die Art und Weise der Datenverarbeitung noch über den Aufenthaltsort und die Gestaltung der Speicherung der Daten bestimmen kann, kann der Nutzer dieser Verantwortung kaum gerecht werden. Hierzu müsste dem Nutzer eine allumfassende Transparenz und eine Wahlmöglichkeit über die Ausgestaltung dieser Bedingungen zur Verfügung gestellt werden. Der Aufwand für die Überprüfung der Maßnahmen des Auftragnehmers wären allerdings sehr hoch, was die Nutzung einer Cloud, unter dem Gesichtspunkt der Kosten- und Zeiteinsparung durch Outsourcing, sehr unattraktiv machen würde. Dies lässt sich nur dadurch umgehen, dass sich entweder der Auftragnehmer vertraglich an eine entsprechende Vorgehensweise bindet oder die Kontrolle an eine unabhängige Stelle übertragen wird. Dies wäre durch Zertifizierungen möglich (weiteres dazu später).

5.3.2.2 Funktionsübertragung

Von der Auftragsdatenverarbeitung zu unterscheiden ist die Funktionsübertragung. Bei der Funktionsübertragung wird eine Aufgabe komplett mit allen Verantwortlichkeiten an

einen Auftragnehmer abgegeben, inklusive der Verantwortung für den Schutz der personenbezogenen Daten. Dies können beim Cloud Computing die Cloud- und Ressourcen-Anbieter jedoch nicht gewährleisten, da sie in der Regel mit der Datenverarbeitung an sich nichts zu tun haben. Dennoch ist der Cloud-Nutzer dazu verpflichtet, die Anforderungen an die Übermittlung bei allen Daten sicherzustellen. Nach § 28 Abs. 1 BDSG sind die folgenden Bedingungen notwendig:

> *„Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig*
>
> *1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,*
>
> *2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder*
>
> *3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.*
>
> *Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.“*

Dies führt dazu, dass der Übermittlung in die Cloud ein vertragliches oder anderweitig berechtigtes Interesse zugrunde liegen muss und sie erforderlich ist. Durch eine vertragliche Beziehung zwischen Cloud-Nutzer und dem Betroffenen kann diese sich auch auf die Cloud-Verarbeitung erstrecken. Andernfalls muss die Übermittlung in die Cloud „erforderlich“ sein (§ 28 Abs. 1 S. 1 Nr. 1 BDSG). Dadurch ist jedoch schwer zu begründen, dass die Cloud-Nutzung außerhalb der EU oder des EWR notwendig ist. Ebenso muss sichergestellt werden, dass die schutzwürdigen Interessen des Betroffenen gesichert werden (§ 28 Abs. 1 S. 1 Nr. 2 BDSG). Diese Sicherung kann, wie in § 11 BDSG vorgesehen, ausgestaltet werden, bildet jedoch nur die Grundlage zur Wahrung der Interessen des Betroffenen und genügt nicht zum Ausgleich der Aufgabe der rechtlichen Verantwortlichkeit im Falle einer Funktionsübertragung. Um einen sicheren Umgang mit den schutzwürdigen Interessen des Betroffenen zu gewährleisten, muss die Ausgestaltung des Vertrages zwischen Cloud-Nutzer und -Anbieter diese Anforderungen zur Genüge berücksichtigen. Des Weiteren müssen die Anforderungen für Datenübermittlungen ins Drittausland, d.h. in ein Land außerhalb des EU/EWR-Raumes, gemäß §§ 4b und 4c BDSG erfüllt sein. Hier wird ein „angemessenes Datenschutzniveau“ gefordert, welches durch die EU-Kommission beispielsweise für die Schweiz, Kanada und Argentinien festgelegt wurde. Die Feststellung hat jedoch nicht die Folge, dass dortige Stellen als Auftragnehmer gemäß § 11 BDSG behandelt werden können. Eine Datenweitergabe muss somit als Übermittlung gekennzeichnet werden.

5.3.3 Zugriffsmöglichkeiten Dritter

Dadurch, dass die Daten durch den Cloud- oder Ressourcen-Anbieter in anderen Staaten gelagert werden, kann die Möglichkeit bestehen, dass Dritte, also weder der Cloud-Nutzer noch der Cloud- oder Ressourcen-Anbieter, ob legal oder illegal, auf die Daten zugreifen können.

Legal wäre dies durch staatliche oder halbstaatliche Behörden möglich, wie etwa der Polizei, der Justiz, des Militärs, der Geheimdienste oder der Finanzbehörden. Hierdurch könnten sicherheitsempfindliche Daten über Personen oder Unternehmen abgerufen werden, die zur Industriespionage, Überwachung, strafrechtlichen Verfolgung oder zur Verfolgung auf Grund von ethischen, religiösen, politischen, sexuellen, wirtschaftlichen oder sonstigen Erwägungen genutzt werden könnten. Finanzbehörden hätten eventuell die Möglichkeit, Bankdaten zu Überprüfungen bezüglich Steuerbetrug und Steuerhinterziehung heranzuziehen, Einwanderungsbehörden könnten Daten über Immigranten abfragen. Aber auch ohne einen rechtlich begründbaren Zugriff durch diese oder andere Institutionen könnte bei einem erlaubten Zugriff durch weitere oder durch ein völliges Fehlen oder eine unzureichende Gestaltung von Datenschutzbestimmungen der mögliche Zugriff auf Daten in der Cloud legal sein.

Des Weiteren besteht die Möglichkeit, dass Dritte unberechtigt und damit illegal auf die Daten in der Cloud zugreifen können. Durch die Verlagerung der Daten in die Cloud wird dem Cloud-Nutzer nahezu jegliche Möglichkeit genommen, für die Sicherheit seiner Daten zu sorgen. Dadurch muss die Datensicherheit, inklusive der Vertraulichkeit, der Integrität, der Transparenz und der Verfügbarkeit für die Nutzer und der Unverknüpfbarkeit (zur Herstellung eines Zusammenhangs) innerhalb des Vertrages zwischen Cloud-Nutzer und -Anbieter geklärt werden. Durch die Cloud werden neue Möglichkeiten des illegalen Zugriffs durch unberechtigte Dritte ermöglicht, beispielsweise dadurch, dass sich ein Dritter als Nutzer ausgibt, der berechtigten Zugang zu den Daten hätte (Man-in-the-middle-Angriff). Bedingt durch die Ursache, dass der Cloud- und Ressourcen-Anbieter in der Regel nichts mit der Datenverarbeitung zu tun hat, könnte eine Überprüfung dieses Sachverhalts schwierig werden. Der unberechtigte Zugriff könnte somit zur Spionage oder Sabotage der Daten genutzt werden.

Diese Zugriffsmöglichkeiten können durch verschiedene Möglichkeiten abgewehrt werden. Zum einen kann durch die zuvor besprochene Pseudonymisierung (§ 3 Abs. 6 BDSG) eine Auswertung der Daten verhindert werden, wenn keine Möglichkeit besteht die Zuordnungen aufzudecken. Ebenso ist es möglich, die Datensätze zu verschlüsseln, solange keine Entschlüsselungsmöglichkeiten bestehen. Dabei muss jedoch bedacht werden, dass es in diversen Staaten rechtliche Regelungen gibt, die die Cloud- und Ressourcen-Anbieter dazu zwingen könnten, die Zuordnungen (Pseudonymisierung) oder Schlüssel (Verschlüsselung) an die am Zugriff interessierten Behörden auszuhändigen, oder sogar sämtliche Schutzvorkehrungen zu unterlassen. Des Weiteren besteht natürlich auch die Möglichkeit, dass Behörden auf legaler Grundlage die technischen Schutzvorkehrungen überwinden dürfen. Die gesetzliche Verpflichtung zu technischen und organisatorischen Maßnahmen zur Verhinderung von unberechtigten Zugriffen (gemäß § 9 BDSG und Art. 17 Abs. 1 EU-DSRL) besteht jedoch nur im EU/EWR-Raum, und selbst hier gibt es beträchtliche Unterschiede in der Umsetzung. Vertraglich können ungesetzliche Zugriffe Dritter auf die Daten in der

Cloud zwischen dem Cloud-Nutzer und -Anbieter geregelt werden; gegen legale Zugriffsrechte ist dies jedoch nicht möglich. Hier würde lediglich die Möglichkeit bestehen, den Anbieter dazu zu bringen, nur Ressourcen in Staaten zu nutzen, die über eine entsprechende gesetzliche Regelung verfügen, die die Sicherheit der schutzwürdigen Interessen abdeckt.

5.3.4 Technische und organisatorische Maßnahmen

Die zuvor erwähnten technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes werden durch den § 9 BDSG gefordert:

> *„Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.“*

Ähnliches fordert Art. 17 Abs. 1 EU-DSRL.

Bei der Benennung der technischen und organisatorischen Maßnahmen darf es sich jedoch nicht nur um die abstrakte Methode oder das Schutzziel handeln, sondern es müssen das konkret genutzte Sicherungsmittel sowie die Kontrollmaßnahmen, die vom Cloud- gegenüber dem Ressourcen-Anbieter durchgeführt werden müssen, explizit benannt werden gemäß §§ 11 Abs. 2 S. 2 Nr. 3,5 BDSG. Dies führt dazu, dass eine „Verschleierung“ der getroffenen Maßnahmen, wie es heute oft üblich ist, nicht rechtens ist.

5.3.5 Haftung

Zu regeln ist auch die Haftung, die der Cloud- und Ressourcen-Anbieter gegenüber dem Nutzer hat. Durch die Datenverarbeitung in der Cloud können dem Nutzer erhebliche Schäden entstehen, ob im wirtschaftlichen oder im persönlichkeitsrechtlichen Sinn, etwa durch Verlust oder Beschädigung der in die Cloud verlagerten Daten. Die Betroffenen können gegenüber dem Cloud-Nutzer durch folgende Gesetze Schadensersatz beanspruchen:

§ 7 BDSG:

> *„Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.“*

und § 823 Bürgerliches Gesetzbuch (BGB):

> *„(1) Wer vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt, ist dem anderen zum Ersatz des daraus entstehenden Schadens verpflichtet.*
>
> *(2) Die gleiche Verpflichtung trifft denjenigen, welcher gegen ein den Schutz eines anderen bezweckendes Gesetz verstößt. Ist nach dem Inhalt des Gesetzes ein Verstoß gegen dieses auch ohne Verschulden möglich, so tritt die Ersatzpflicht nur im Falle des Verschuldens ein.“*

Bedingt durch diese Regelungen wäre es ratsam, dass die Regelungen bezüglich der Haftung innerhalb des Vertrages zwischen Cloud-Nutzer und -Anbieter bzw. zwischen Cloud- und Ressourcen-Anbieter alle vom Kunden nicht zu vertretenen Schäden abdecken. Zusätzlich sollte geklärt sein, welches konkrete Recht im Schadensfall Anwendung findet. Zu bedenken ist in diesem Zusammenhang auch die Möglichkeit einer Insolvenz des Cloud- oder Ressourcen-Anbieters.

5.4 Weitere gesetzliche Regelungen

5.4.1 Aktiengesetz

Durch § 91 Aktiengesetz (AktG) wird, ebenso wie z.B. durch § 9 BDSG, vorgeschrieben, dass Aktiengesellschaften, aber auch GmbHs, u.a. für entsprechende IT-Sicherheit zu sorgen haben:

> *„(1) Der Vorstand hat dafür zu sorgen, daß die erforderlichen Handelsbücher geführt werden.*
>
> *(2) Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.“*

Vorstand und/oder Geschäftsführung einer solchen Gesellschaft können haftbar gemacht werden beim Entstehen eines für die Gesellschaft erheblichen Schadens, beispielsweise durch einen Ausfall des Zugriffs der durch SaaS angebotenen Software. Hierdurch sollte bei der Ausgestaltung der Verträge mit dem Kunden gewissenhaft vorgegangen werden. Es können verschieden Schwerpunkte gelegt werden, etwa auf die Verfügbarkeit der Programme oder auf die Sicherheit der Daten.

5.4.2 Abgabenordnung

Eine besondere Herausforderung können Aufbewahrungspflichten für Daten, insbesondere steuerlich relevante, führen. Dies kann insbesondere dann ein Problem darstellen, wenn die Daten im Ausland gelagert werden. Hinzu kommt, dass sichergestellt werden muss, dass die Daten jederzeit zur Verfügung stehen, wobei dabei auch eine mögliche Inkompatibilität mit alten Daten oder eine Veränderung derselbigen ausgeschlossen werden muss. Man muss sich zusätzlich absichern, bedenkt man, dass die Möglichkeit besteht, dass der Cloud-Anbieter seine Dienste einstellt oder diese ungenügend durchführt. § 146 Abgabenordnung (AO) besagt hierzu:

> *„(2) Bücher und die sonst erforderlichen Aufzeichnungen sind im Geltungsbereich dieses Gesetzes zu führen und aufzubewahren. [...] (2a) Abweichend von Absatz 2 Satz 1 kann die zuständige Finanzbehörde auf schriftlichen Antrag des Steuerpflichtigen bewilligen, dass elektronische Bücher und sonstige erforderliche elektronische Aufzeichnungen oder Teile davon außerhalb des Geltungsbereichs dieses Gesetzes geführt und aufbewahrt werden können. Voraussetzung ist, dass*
>
> *1. der Steuerpflichtige der zuständigen Finanzbehörde den Standort des Datenverarbeitungssystems und bei Beauftragung eines Dritten dessen Namen und Anschrift mitteilt,*
>
> *2. [...]*

3. der Datenzugriff nach § 147 Absatz 6 in vollem Umfang möglich ist und

4. die Besteuerung hierdurch nicht beeinträchtigt wird.

Werden der Finanzbehörde Umstände bekannt, die zu einer Beeinträchtigung der Besteuerung führen, hat sie die Bewilligung zu widerrufen und die unverzügliche Rückverlagerung der elektronischen Bücher und sonstigen erforderlichen elektronischen Aufzeichnungen in den Geltungsbereich dieses Gesetzes zu verlangen. Eine Änderung der unter Satz 2 Nummer 1 benannten Umstände ist der zuständigen Finanzbehörde unverzüglich mitzuteilen.“

Ausnahmen wie im Absatz 2a erwähnt können in der Regel nur in einem Mitgliedstaat des EU/EWR-Raumes beantragt werden. Dazu muss jedoch die ausländische Finanzbehörde zustimmen, ebenso müssen die deutschen Finanzbehörden auf die Daten zugreifen können.

Nach § 148 AO können hierzu aber auch Ausnahmen genehmigt werden:

„Die Finanzbehörden können für einzelne Fälle oder für bestimmte Gruppen von Fällen Erleichterungen bewilligen, wenn die Einhaltung der durch die Steuergesetze begründeten Buchführungs-, Aufzeichnungs- und Aufbewahrungspflichten Härten mit sich bringt und die Besteuerung durch die Erleichterung nicht beeinträchtigt wird. [...]“

5.4.3 Handelsgesetzbuch

Nach dem Handelsgesetz besteht die Pflicht, Buchungsbelege, Handelsbriefe u.ä. im Inland aufzubewahren, und dies nach § 257 Abs. 4 Handelsgesetzbuch (HGB) mit einer Aufbewahrungszeit von sechs beziehungsweise zehn Jahren. Durch Abs. 3 wird bestimmt, dass die unter diesen Paragraphen fallenden Daten „während der Dauer der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können.“

Dies könnte zu tiefgreifenden Problemen – wie bei der Abgabenordnung bereits besprochen – führen.

5.4.4 Miet-, Werk- und Pachtvertrag

Dienstleistungen anderer Anbieter wie z.B. Applikationen (Anwendungssoftware, in der Regel ein SaaS oder Application Service Provider (ASP)-Modell) oder Webhosting, die in der Cloud zur Verfügung gestellt werden, können durch einen Miet-, Werk- oder Pachtvertrag angeboten werden. Um Wirksamkeit zu besitzen, muss der Vertrag in Schriftform festgehalten werden.

Das Bundesgerichtshof (BGH) hat am 04.03.2010 in einem Urteil zur rechtlichen Einordnung eines „Internet-System-Vertrags“, der die Erstellung und Betreuung einer Internetpräsentation (Website) des Kunden sowie die Gewährleistung der Abrufbarkeit dieser

Website im Internet für einen festgelegten Zeitraum (Aktenzeichen: III ZR 79/09) beschlossen, dass ASP-Anwendungen unter das Mietrecht fallen. Laut dem BGH ist der Hauptzweck dieses Vertrages die Nutzung fremder Software, die meist einer großen Anzahl von Kunden zur Verfügung gestellt wird. Dadurch sei die in der Regel entgeltliche Gebrauchsüberlassung der Schwerpunkt des Vertrags, wodurch er dann unter das Mietrecht (§§ 535 ff. BGB) falle. Die mietrechtlichen Regelungen genügen jedoch in den meisten Fällen zur Ausgestaltung der Verträge nicht, wodurch eine vertragliche Gestaltung von Service-Level-Agreements (SLA) nötig wird. SLA, zu Deutsch Dienstgütevereinbarung, bezeichnet eine Vereinbarung zwischen Kunde und Dienstleister für wiederkehrende Dienstleistungen. Beabsichtigt wird dadurch, dass der Kunde über Kontrollmöglichkeiten verfügt, indem zugesicherte Leistungseigenschaften wie beispielsweise Leistungsumfang, Reaktionszeit und Schnelligkeit der Bearbeitung exakt beschrieben werden. Die Dienstgüte steht hierbei im Vordergrund, da sie die vereinbarte Leistungsqualität beschreibt.

Beim Webhosting, also die Bereitstellung von Webspace und die Unterbringung von Websites auf einem Webserver eines Internet Service Providers, wird vertreten, dass es sich hierbei nicht um einen solchen Mietvertrag, sondern vielmehr um einen Werkvertrag gemäß §§ 631 ff. BGB handelt. Im Vordergrund des Webhosting steht die Leistung, also die Speicherung der Website des Kunden und die Aufrufbarkeit derselbigen im Internet. Im Sinne des Kunden ist die dauerhafte Verfügbarkeit der Inhalte mit der höchsten Priorität zu betrachten. Wie die Umsetzung der Leistung durch den Hosting-Provider oder den Cloud-Anbieter bewerkstelligt wird spielt hierbei keine Rolle. Die Speicherung der Inhalte ist nur die technische Umsetzung, Inhalt des Werkvertrages ist jedoch nur die Verfügbarkeit an sich.

Denkbar wäre des Weiteren auch eine Ausgestaltung der Vereinbarung als Pachtvertrag gemäß §§ 581-597 BGB.

5.4.5 Strafrecht

Hier gilt es zu bedenken, inwiefern Ärzte, Psychologen und Versicherungen Kundendaten in Clouds speichern dürfen, da dies möglicherweise unter § 203 Strafgesetzbuch (StGB) fallen könnte:

> *„(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart[...]“*

Auch betroffen wären viele öffentliche Verwaltungen, wie etwa Amtsträger, für den öffentlichen Dienst besonders Verpflichtete oder Mitglieder diverser Gesetzgebungsorgane.

Die Speicherung von Daten in der Cloud muss insbesondere bei Ermittlungen von Straftaten und Ordnungswidrigkeiten den Zugriff für die Ermittlungs- und Sanktionsbehörden sicherstellen.

Da Datenschutzverstöße auch Straftatbestände erfüllen können, sind strafrechtliche Ermittlungen nach der Strafprozessordnung (StPO) möglich. Selbst der durch die Auslagerung der Daten möglichen Ermittlungserschwernis wurde durch § 110 Abs. 3 StPO teilweise entgegen gewirkt:

> *„getrennte Speichermedien, soweit auf sie von dem Speichermedium aus zugegriffen werden kann, erstreckt werden, wenn andernfalls der Verlust der gesuchten Daten zu besorgen ist. Daten, die für die Untersuchung von Bedeutung sein können, dürfen gesichert werden; § 98 Abs. 2 gilt entsprechend.“*

Dennoch dürften die gesetzlichen Ermittlungsmöglichkeiten außerhalb des deutschen Zugriffsbereichs nach deutschem Recht sehr eingeschränkt sein, da die Kontrolle des Datenschutzes durch die Aufsichtsbehörden auf das jeweilige Landesterritorium beschränkt ist. Innerhalb des EU/EWR-Raumes ist es zwar noch möglich, durch eine Amtshilfe der Aufsichtsbehörden Ermittlungen über Ländergrenzen hinweg durchzuführen, doch spätestens bei Kontrollen (§38 Abs. 1 S. 1 BDSG und Art. 28 Abs. 3 EU-DSRL) in Drittländern wird dies durch den hohen bürokratischen Aufwand praktisch unmöglich. Hierdurch besteht die Gefahr, dass verantwortliche Cloud-Nutzer oder -Anbieter gezielt mit Clouds arbeiten, um sich Datenschutzkontrollen zu entziehen, insbesondere, wenn die Datenverarbeitung in Drittländern stattfindet.

5.4.6 Urheberrecht

Beim Urheberrecht stellt sich die Frage, wer die in der Cloud gespeicherten Daten gegebenenfalls unrechtlich nutzen und vervielfältigen kann. Von Seiten des Nutzers, der die Dienste nur über spezielle Anwendungen oder über seinen Browser nutzt, gibt es dabei wenig Bedenken, da er davon ausgehen kann, die durch die Cloud zur Verfügung gestellten Dienste auch nutzen zu dürfen. Der Kunde hat selbst keinen Einfluss auf die Technik in der Cloud, wodurch unrechtmäßige Vervielfältigung automatisch unterbunden wird. Um die Lizenzen hierfür dürften sich in der Regel die Dienstanbieter selbst kümmern. Welches Urheberrecht letztendlich Anwendung findet entspricht den selben Umständen wie zuvor beim Datenschutz.

Eine andere Frage stellt sich bei Lizenzverträgen zwischen den Cloud-Anbietern und den Anbietern der durch die Cloud angebotenen Applikationen:

Der Cloud-Anbieter muss sich die Rechte, die Applikationen öffentlich zur Verfügung zu stellen, übertragen lassen. „Öffentlich“ schließt in diesem Falle auch die Verfügbarkeit für einzelne Kunden, z.B. in einer privaten Cloud, ein, da auch eine höhere Zahl von miteinander nicht verbundenen Nutzern eine „Öffentlichkeit“ darstellt.

In Deutschland ist hierbei das Urheberrechtsgesetz (UrhG) zu beachten.

5.5 Zertifizierung

Damit der Kunde von einem gewissen Maß an rechtlichen und technischen Sicherheit- und Compliance-Anforderungen bei der Auswahl von Cloud-Anbietern ausgehen kann, besteht die Möglichkeit, sich an Zertifikaten zu orientieren. Mit Compliance sind die gesetzlichen, unternehmensinternen und vertraglichen Regelungen des IT-Bereichs in einem Unternehmen gemeint. Dies beinhaltet u.a. Informationssicherheit, Verfügbarkeit, Datenaufbewahrung und Datenschutz. Im Bereich des Cloud Computing sind hierbei vor allem die beiden Zertifikate ISO/IEC 27001 sowie das Zertifikat SAS 70 von Belang. Dennoch sollte man stets selbst noch einmal die Angaben und die Inhalte des Vertrages eines Unternehmens kontrollieren, da solche Zertifikate auch als Marketing-Instrumente genutzt werden. Die Zertifikate bieten in der Regel nur ein Mindestmaß an Qualitätsanforderungen. Um sicherzugehen, sollte immer auch der Auditor, also der Prüfer, sowie Inhalt des Audit-Berichts und das zugrundeliegende Managementsystem überprüft werden, abhängig von der benötigten Datensicherheit.

Unabhängig von den im Weiteren genauer erklärten Zertifikaten können Datenschutzaudits und Datenschutzzertifizierungen gemäß § 9a BDSG erwägt werden. Es gibt hierzu zwar kein, wie in § 9a BDSG vorgesehenes, „Auditgesetz“, dennoch werden Zertifizierungen, die sich am Bundesdatenschutzgesetz ausrichten, von privaten Unternehmen angeboten. Hier gilt es, wie bei den anderen Zertifikaten auch, das Renommee des Auditors zu bewerten, da es keine öffentlich akkreditieren Zertifizierungsstellen gibt.

5.5.1 ISO/IEC 27001

Die internationale Norm ISO/IEC 27001 (IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen) beschreibt die Anforderungen an ein Unternehmen oder eine Organisation bezüglich Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung der möglichen Risiken. In Deutschland wurde diese Norm als DIN-Norm DIN ISO/IEC 27001 umgesetzt, welche vom DIN NIA-01-27 IT-Sicherheitsverfahren betreut wird. Hervorgegangen ist die ISO/IEC 27001 aus dem British Standard BS 7799, welcher dadurch keine Gültigkeit mehr besitzt, und wurde erstmals am 15. Oktober 2005 veröffentlicht. Laut Wikipedia ist die ISO/IEC 27001:2005 für folgende Bereiche anwendbar:

- Zur Formulierung von Anforderungen und Zielsetzungen zur Informationssicherheit
- Zum kosteneffizienten Management von Sicherheitsrisiken
- Zur Sicherstellung der Konformität mit Gesetzen und Regulatorien
- Als Prozessrahmen für die Implementierung und das Management von Maßnahmen zur Sicherstellung von spezifischen Zielen zur Informationssicherheit
- Zur Definition von neuen Informationssicherheits-Managementprozessen

- Zur Identifikation und Definition von bestehenden Informationssicherheits-Managementprozessen
- Zur Definition von Informationssicherheits-Managementtätigkeiten
- Zum Gebrauch durch interne und externe Auditoren zur Feststellung des Umsetzungsgrades von Richtlinien und Standards

ISO 27001-Zertifikate können auf verschiedenen Managementsystemen aufgebaut sein, so beispielsweise auf Basis des IT-Grundschutz-Katalogs des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI). Das BSI-Grundschutz-Zertifikat baut auf dem ISO 27001 auf, geht jedoch auf Grund zusätzlich geprüfter technischer Aspekte weiter als das reine ISO 27001-Zertifikat. Die ISO 27001-Zertifizierungen bieten dennoch keinen zwingenden Rückschluss auf die Erfüllung der Anforderungen an den Datenschutz bei der Datenverarbeitung gemäß § 9 BDSG. Ein Großteil der technischen und organisatorischen Anforderungen hiernach werden zwar erfüllt, dennoch bleiben einige Aspekte offen, wie etwa Trennungsgebot, Auftragskontrolle und Eingabekontrolle.

5.5.2 SAS 70

Statement on Auditing Standards No. 70: Service Organizations, kurz SAS 70, ist ein Zertifikat des Auditing Standards Board des American Institute of Certified Public Accountants (AICPA) und wird von Wirtschaftsprüfungsgesellschaften angewendet. Die Zertifizierung überprüft das interne Kontrollsystem eines Unternehmens und den ordnungsgemäßen Betrieb von ausgelagerten Service Prozessen wie beispielsweise ASP. Hierbei gibt es zwei Typen: Der SAS 70 Typ I beurteilt das interne Kontrollsystem des Service-Anbieters, wohingegen im SAS 70 Typ II dessen Effektivität geprüft wird. Obwohl SAS 70 keinen Maßnahmen- bzw. Prüfungskatalog kennt, werden die SAS 70-Prüfberichte vom amerikanischen Public Company Accounting Oversight Board (PCAOB), das die ordnungsgemäße Umsetzung vom Sarbanes Oxley Act (SOX), eines amerikanischen Bundesgesetzes, das die Verlässlichkeit der Berichterstattung von Unternehmen verbessern soll, überprüft, akzeptiert. Ähnlich zum SOX gibt es in der Europäischen Union die Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006, umgangssprachlich auch 8. EU-Richtlinie oder EuroSox genannt, welche in Deutschland mit dem Berufsaufsichtsreformgesetz (BARefG) umgesetzt wurde. Nichtsdestotrotz wird zur SAS 70-Zertifizierung weiter der amerikanische SOX herangezogen. Dennoch gibt es in anderen Ländern Standards, die mit SAS 70 vergleichbar sind. Hier sind im deutschsprachigen Raum der IDW PS951 in Deutschland, der IWP-PE14 in Österreich und der GzA18 PS402 in der Schweiz, welche inklusive der darauf basierenden Zertifizierungen prinzipiell äquivalent sind. Gleichwohl ist in internationalen Unternehmen, vor allem wenn sie unter das SOX fallen, auch auf Grund der englischen Berichtssprache und der internationalen Akzeptanz des SAS 70-Standards, dieser zu empfehlen.

5.6 Ausblick

Wie gezeigt wurde, besteht im Bereich der rechtlichen Regelungen beim Cloud Computing ein sehr großes Spektrum, das beachtet werden muss, sollte man empfindliche Daten oder deren Verarbeitung in die Cloud übertragen. Dies gestaltet sich insbesondere dadurch als schwierig, dass vom Gesetzgeber, sowohl von der Europäischen Union als auch vom Deutschen Bundestag oder den Landtagen, keine gesonderte Regelung zum Cloud Computing besteht. Dieses Problem könnte sich, zumindest innerhalb der Europäischen Union, jedoch in Zukunft lösen. Die Enquete-Kommission „Internet und digitale Gesellschaft“ sowie der Unterausschuss „Neue Medien“ des Deutschen Bundestages wird sich im Herbst diesen Jahres mit dem Thema Cloud Computing explizit auseinander setzen. Des Weiteren plant auch die Europäische Kommission den Ausbau der Cloud Computing Services in Europa. Dazu hat die Business Software Alliance (BSA) ein Strategiepapier entworfen. Die EU-Vizepräsidentin Neelie Kroes hat in einer Rede am 27. Januar 2011 in Davos Maßnahmen zur leichteren Einführung von Cloud Computing als sehr wichtig beschrieben. Sie erwartet davon eine Vielzahl neuer Serviceangebote für die EU-Bürger sowie in vielen Branchen ein dadurch gefördertes wirtschaftliches Wachstum. Dazu müssten jedoch zuerst komplexe rechtliche, technische und wirtschaftliche Fragen geklärt werden, die möglicherweise einer positiven Entwicklung des Cloud Computing im Wege stehen könnten. Hierzu forderte sie die Ausarbeitung einer EU-weiten Strategie.

Dadurch, dass noch keine rechtlichen Sicherheits- und Datenschutzrichtlinien explizit für Clouds vorgeschrieben sind, ist davon auszugehen, dass zur Zeit in beträchtlichem Maße Datenschutz- und Persönlichkeitsrechtsverstöße erfolgen, welche durch die indirekte Beteiligung von Cloud-Nutzern und -Anbietern sowie den Ressourcenanbieter an den verschiedenen Funktionen bedingt sind. Hinzu kommt, dass keiner der Betroffenen ein wesentliches Interesse daran haben kann, dass mögliche Verstöße in die Öffentlichkeit getragen werden, da natürlich weder der Cloud-Nutzer möchte, dass seine Daten oder Fehler publik werden, noch die Cloud- und Ressourcenbieter eine Veröffentlichung von Missständen in der angebotenen Technik gutheißen können.

Auf internationaler Ebene hat sich mit der US-dominierten Cloud Security Alliance (CSA) im Jahr 2008 eine Vereinigung gebildet, die sich zum Ziel gesetzt hat, Richtlinien für ein sicheres Cloud Computing zu entwickeln, die Kommunikation zwischen Cloud-Nutzer und -Anbieter zu verbessern, Leitfäden zum Gebrauch zur Verfügung zu stellen und Forschungen zur besten Ausgestaltung der Cloud Computing-Sicherheitsmaßnahmen zu betreiben.

In Europa wurde 2009 der Dachverband EuroCloud Europe von Pierre-José Billotte, Gründer und Vorsitzender des französischen ASP Forums, gegründet, welcher die Interessen der europäischen Cloud Computing-Branche gegenüber der europäischen Politik und Organisationen vertritt und die Koordination von technologischen Partnerschaften und Geschäftsbeziehungen zu anderen Branchenvertretern auf internationaler Ebene und mit der CSA regelt. EuroCloud möchte ebenso für eine einheitliche Herangehensweise innerhalb seines Einflussgebietes sorgen.

In Deutschland hat sich 2010 der Verband EuroCloud Deutschland_eco gegründet, der von vielen Unternehmen aus den verschiedenen Cloud Computing-Bereichen (SaaS, PaaS,

IaaS) mit Partnern aus dem Bereich Recht und Beratung unterstützt wird und sich ähnliche Ziele wie die CSA gesetzt hat. Er repräsentiert die deutsche Cloud Computing-Industrie im paneuropäischen EuroCloud-Netzwerk. Im selben Jahr hat der Verband den Leitfaden „Cloud Computing – Recht, Datenschutz & Compilance“ veröffentlicht, um einen Anhalt zu bestehenden Rechtsfragen zu geben. Der Verband setzt sich laut eigener Beschreibung „für Akzeptanz und bedarfsgerechte Bereitstellung von Cloud Services am deutschen Markt ein“. EuroCloud Deutschland_eco hat sich als Ziel gesetzt, ein SaaS-Gütesiegel einzuführen sowie offene Rechtsfragen zu klären. In Zusammenarbeit mit eco, dem Verband der Internetwirtschaft in Deutschland, wird versucht, eine große Reichweite zu schaffen.

Gleichwohl bleiben, trotz dem hohen Interesse und den immensen Vorteilen sowohl für Cloud-Nutzer als auch -Anbieter, internationale Normen und Auditierungsverfahren bzw. Zertifizierungen bezüglich Datenverarbeitung und Datenschutz in naheliegender Zukunft unwahrscheinlich, da sich die nationalen Regelungen in diesem Bereich, sofern sie überhaupt existieren, stark unterscheiden und noch keine Bestrebungen seitens der Regierungen bekannt sind.

Des Weiteren ist zu vermuten, dass das bestehende deutsche Recht, das Einfluss auf die Nutzung von Cloud Computing hat, noch weiter ergänzt werden wird. Hier wäre es beispielsweise möglich, dass der Deutsche Bundestag ein Arbeitnehmerdatenschutzgesetz verabschiedet. Der Arbeitnehmerdatenschutz ist, trotz seiner großen praktischen Relevanz, noch nicht explizit durch ein eigenes Gesetz behandelt, sondern wird bis jetzt nur durch die allgemeinen Regeln des Bundesdatenschutzgesetzes geregelt. Im Februar 2009 hat das Bundeskabinett auf Vorschlag des damaligen Bundesinnenministers Dr. Wolfgang Schäuble beschlossen, eine Grundsatzregelung zum Datenschutz der Arbeitnehmer in das Bundesdatenschutzgesetz aufzunehmen. Zum 1. September 2009 trat die im § 32 BDSG beschriebene Regelung zur Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses in Kraft. Neben dieser gibt es noch weitere bereichsspezifische Vorschriften, die das informationelle Selbstbestimmungsrecht des Beschäftigten regeln, wie etwa im Telemediengesetz, im Bundesbeamtengesetz, in der Bildschirmarbeitsverordnung, im Betriebsverfassungsgesetz oder in den Personalvertretungsgesetzen. Am 4. September 2009 legte der damalige Bundesarbeitsminister Olaf Scholz den Entwurf für ein „Gesetz zum Datenschutz im Beschäftigungsverhältnis (Beschäftigungsdatenschutzgesetz - BDatG)“ vor, welches die bestehenden Regelungen vereinheitlichen sollte. Die Koalitionsvereinbarung der kurz darauf folgenden Regierungskoalition sah hingegen nur noch eine Erweiterung des BDSGes vor. Am 25. August 2010 wurde der Entwurf des Gesetzes zur Regelung des Beschäftigtendatenschutzes beschlossen. Mittlerweile ist am 15. Dezember 2010 die Bundestags-Drucksache 17/4130 mit einem neuen, überarbeiteten Entwurf eines Beschäftigtendatenschutzgesetzes erschienen.

Bedenkt man jedoch, dass es im Grunde nur amerikanische Unternehmen sind, die im großen Stil Cloud Computing anbieten, stellt sich die Frage, ob es überhaupt möglich ist, deutsches bzw. europäisches Recht in internationalen Regelungen durchzusetzen. Es könnte sein, dass diese Unternehmen, wie etwa Amazon, Microsoft, Google etc., ihre herausragende Marktstellung dazu nutzen, nur ihnen entgegenkommende Bedingungen zu akzeptieren oder sich, sollte dies nicht geschehen, aus den entsprechenden nationalen Märkten zurückzuziehen. Hier besteht deshalb die Chance, dass sich auf nationaler oder

europäischer Ebene eigene Anbieter finden, die diese freien Märkte besetzen. Um konkurrenzfähig zu bleiben und auf Grund ihrer nationalen Herkunft werden diese Anbieter sich an die lokalen gesetzlichen Rahmenbedingungen halten müssen.

Literaturverzeichnis

[1] Dr. Otto Singer. *Aktueller Begriff: Cloud Computing*, Wissenschaftlicher Dienst des Deutschen Bundestages, Berlin 2010.

[2] Thilo Weichert. *Cloud Computing und Datenschutz*, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, https://www.datenschutzzentrum.de, 28.02.2011.

[3] Sebastian Dosch. *Juristische Aspekte des Cloud Computing*, www.it-administrator.de, 28.02.2011.

[4] Carsten Gerlach. *Zertifizierungen für Cloud-Computing-Systeme und SaaS: Datenschutz und Compliance*, www.it-rechts-praxis.de, 28.02.2010.

[5] datenschutz nord GmbH. *Rechtliche Vorgaben und Standards zur IT-Sicherheit und zum Risikomanagement*, www.datenschutz-nord.de, 28.02.2010.

[6] Elke Witmer-Gossner. *BSA entwirft Zehn-Punkte-Plan für Cloud Computing in Europa* , www.searchsoftware.de, 28.02.2011.

[7] EuroCloud Deutschland_eco. www.eurocloud.de, 28.02.2010.

[8] EuroCloud Deutschland_eco. *Cloud Computing — Recht, Datenschutz & Compilance*, Köln 2010.

[9] Michael Winkelmann. *Cloud Computing: Sicherheit und Datenschutz*, Arbeitspapier, Universität Potsdam, Potsdam 2010.

[10] Bundesamt für Sicherheit in der Informationstechnik. *BSI-Mindestsicherheitsanforderungen an Cloud-Anbieter*, Bonn 2010.

[11] Deutsches SAS-70 Portal. www.sas-70.de, 28.02.2010.

[12] Martin Schweinoch. *Damit das Cloud Computing nicht zur Rechtsfalle wird*, www.computerwoche.de, 28.02.2011.

Abkürzungsverzeichnis

AktG	Aktiengesetz.
AO	Abgabenordnung.
ASP	Application Service Provider.
BDSG	Bundesdatenschutzgesetz.
BGH	Bundesgerichtshof.
BSI	Bundesamt für Sicherheit in der Informationstechnik.
CDMI	Cloud Data Management Interface.
CIRP	Cloud Interoperability Roadmap Process.
CMWG	Cloud Management Working Group.
CRUD	Create, Retrieve, Update, Delete.
CSA	Cloud Security Alliance.
CSI	Cloud Service Initiative.
DaaS	Data as a Service.
DMTF	Distributed Management Task Force.
ETSI	European Telecommunications Standards Institute.
FG Cloud	Focus Group Cloud.
HGB	Handelsgesetzbuch.
IaaS	Infrastructure as a Service.
IDaaS	Identity as a Service.
IdP	Identity Provider.
IETF	Internet Engineering Task Force.
ITU	International Telecommunications Union.
LIFF	Liberty Identity Federation Framework.
OASIS	Organization for the Advancement of Structured Information Standards.

OCC	Open Cloud Consortium.
OCCI	Open Cloud Computing Interface.
OGF	Open Grid Forum.
OMG	Object Management Group.
PaaS	Platform as a Service.
REST	Representational State Transfer.
SaaS	Software as a Service.
SAML	Security Assertion Markup Language.
SAML	Security Assertion Markup Language.
SLA	Service-Level-Agreement.
SNIA	Storage Networking Industry Association.
SOAP	Simple Object Access Protocol.
SP	Service Provider.
SPML	Service Provisioning Markup Language.
SSO	Single Sign-On.
StGB	Strafgesetzbuch.
StPO	Strafprozessordnung.
TC	Technical Committee.
URI	Uniform Resource Identifier.
URL	Uniform Resource Locator.
VPN	Virtual Private Network.