

Cloud Computing: Sicherheit und Datenschutz

Michael Winkelmann

Universität Potsdam, Institut für Informatik
Arbeitspapier für die Alcatel-Lucent Stiftung, 22.11.2010

Übersicht

1 Einführung	2
1.1 Verwandte Begriffe	4
1.2 Cloud-Nutzer und Anbieter	6
1.3 Vor- und Nachteile	8
2 Cloud Computing und Sicherheit	10
2.1 Sicherheitsrisiken	10
2.2 Angriffsarten	12
2.2.1 Aktive und passive Angriffe	12
2.2.2 Externe Angriffe.....	12
2.2.3 Seitenkanalattacken	13
2.2.4 Man-in-the-middle-Angriff	13
2.2.5 Cross-Site-Request Forgery	13
2.2.6 DoS- und DDoS-Attacken.....	13
2.2.7 Interne Angriffe.....	14
2.3 Schutzmaßnahmen	14
2.4 Vertragliche Regelungen und Sicherheitsstandards	15
2.4.1 ISO/IEC 27001:2005	16
2.4.2 Statement on Auditing Standard 70 Type II Report.....	16
3 Cloud Computing und Datenschutz	17
3.1 Rechtsfragen.....	17
3.1.1 Vereinbarkeit mit dem Datenschutzgesetz	18
3.1.2 Drittzugriff	20
3.1.3 Vertragliche Regelungen zwischen Nutzer und Anbieter	21
3.1.4 Außereuropäische Clouds	22
3.2 Digitale Identitätsverwaltung	22
3.2.1 Heutige Situation.....	23
3.2.2 Identitätsdiebstahl und -missbrauch	23
3.2.3 Anforderungen an zukünftige Systeme	24
3.2.4 Protokolle	25
3.2.5 Infrastruktur für benutzer-orientiertes Identitätsmanagement.....	28
4 Diskussion und Ausblick	29
5 Referenzen	32

1 Einführung

Cloud Computing ist ein Modell, welches Anwendern über das Internet einzelne Dienste, wie Rechnen, Speichern oder Vernetzen zur Verfügung stellt und bei dem die dafür benötigten Ressourcen von einem Anbieter extern bereitgestellt und verwaltet werden.

Diese Server sind untereinander vernetzt und agieren als einzige „Wolke“ (engl.: Cloud) von Ressourcen.

Das Hauptziel des Cloud-Computings ist es, informationstechnische Dienstleistungen flexibel und skalierbar nutzen zu können. Dieses Konzept ist von der Idee geprägt, Informationen, Dienste und Rechenleistung ähnlich der Vorsorgung mit Wasser und Strom aus einem entfernten Netz zu beziehen.

Durch flächendeckend verfügbare Breitbandanschlüsse und ausgereifte Technologien ist Cloud Computing in den letzten Jahren wahrscheinlich zum bedeutendsten Schlagwort in der IT-Branche geworden. Durch die Nutzung von Cloud Computing brächte für Unternehmen und Endkunden viele Vorteile mit sich.

Im Zusammenhang mit der Etablierung von Cloud Computing im Endkundenbereich ergeben sich allerdings noch viele sicherheitstechnische und datenschutzrechtliche Fragen, die in diesem Artikel näher analysiert werden sollen.

Das Internetzeitalter ist in einer neuen Phase angekommen. Dank zuverlässigerer, erschwinglicherer und allgegenwärtiger Breitbandanschlüsse ist das Internet kein Kommunikationsnetzwerk mehr: Das Internet wird dabei zu einem gigantischen, vernetzten, virtuellen Supercomputer.

Viele ähnliche Begriffe wurden und werden verwendet um diese Entwicklung zu beschreiben: *Web 2.0, Web Services, Grid Computing* und *Cloud Computing*. Jeder dieser Begriffe beschreibt eine grundlegende Änderung in der Art und Weise wie Daten behandelt und verarbeitet werden.

Der Begriff *Cloud Computing* steht hierbei für ein neues Rechenparadigma; der Datenverarbeitung in der Wolke. Derzeit gibt es in der IT-Branche kaum ein öfter benutztes Hype-Wort. Das US-Analystenhaus Gartner schätzte die Erlöse im Jahr 2009 weltweit auf mehr als 56 Milliarden Dollar, was einem Wachstum von etwa 21 Prozent entspricht [11].

Der Name stammt daher, dass schematische Netzwerk-Darstellungen wie das Internet gewöhnlich mit einem Wolkenumriss symbolisiert werden. Die Wolkendarstellung verdeutlicht, dass es unmöglich ist, in eine Wolke hineinzusehen oder zu wissen, welche Vorgänge in ihr ablaufen. Diese Server sind untereinander vernetzt und agieren als einzige „Wolke“ (engl.: *Cloud*) von Ressourcen. Im Fall der Internet-Wolke genügt es, zu wissen, dass sie existiert und Rechner mit ihr verbunden werden können. Zu wissen, was sich darin abspielt, ist für das Funktionieren nicht notwendig.

Das Hauptziel des Cloud-Computings ist es, informationstechnische Dienstleistungen flexibel und skalierbar nutzen zu können. Dieses Konzept ist von der Idee geprägt, Informationen, Dienste und Rechenleistung ähnlich der Vorsorgung mit Wasser und Strom aus einem entfernten Netz zu beziehen. Im Idealfall soll es dem Nutzer egal sein können, ob gerade der eigene oder ein weit entfernter Computer eine Aufgabe löst. Teilweise werden ganze Verfahren in die Cloud verlagert. Teilweise geht es auch nur darum, Bedarfsspitzen abzudecken, mit denen die eigene IT-Infrastruktur überfordert ist.

Die Internetbenutzer sind in der Lage, die Cloud als eine Sammlung von Servern, Speichersystemen und Geräte zu benutzen, um Software, Daten und Rechenleistung über mehrere Standorte im Netzwerk hinweg zu verteilen. Cloud Computing ist also ein Rechen- und Architekturparadigma, das Anwendern über das Internet einzelne Dienste, wie Rechnen, Speichern oder Vernetzen zur Verfügung stellt und bei dem die dafür benötigten Ressourcen von einem Anbieter extern bereitgestellt und verwaltet werden.

Das Konzept ähnelt dem Anwendungsmodell früherer Großrechner und existiert schon lange vor Windows, MacOS und Linux. Bei einem solchen Mainframe diente ein sehr einfach aufgebautes Terminal dazu, Zugriff auf die Ressourcen des Großrechners zu ermöglichen. Erforderlich waren

sowohl ein schneller (und daher kostspieliger) Großrechner als auch die entsprechende Netzwerkinfrastruktur. Die PCs und Heimrechner von IBM kamen hingegen ohne diese Komponenten aus, denn sie vereinigten sämtliche Funktionen in einem einzigen Gerät und machten somit das Konzept des Mainframes obsolet [1].

Mit der flächendeckenden Verfügbarkeit von Breitband- und mobilen Internetzugängen und der erhöhten Funktionalität des Internets wird so die Rolle des PCs in den Hintergrund gedrängt. Beim Cloud-Computing-Konzept ist der PC nun wieder das Terminal, welches den Zugriff auf die in der Cloud zur Verfügung gestellten Dienste ermöglicht.

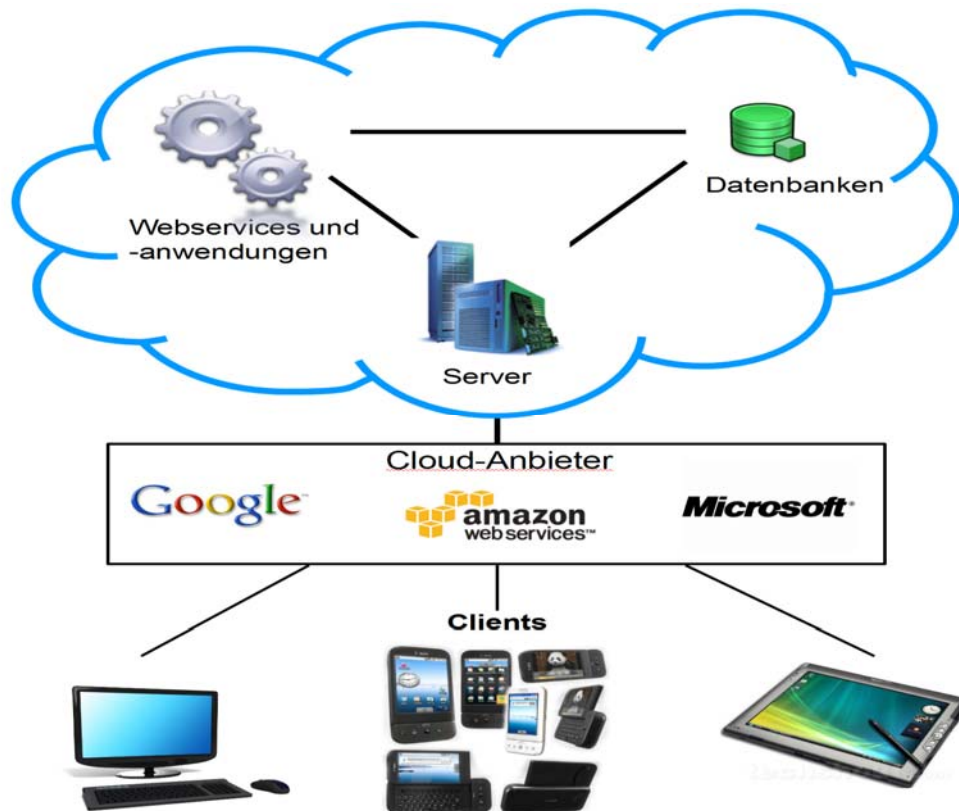


Abbildung 1: Das Cloud-Konzept; Verhältnis zwischen Clients und Anbieter.

Aus der Benutzersicht lässt sich die Evolution von Consumer Computing in drei Phasen einteilen [7]:

1. Der *Stand-alone PC* mit dem Betriebssystem, den Anwendungen und den Daten, die alle auf einer einzigen, leicht absicherbaren Maschine gespeichert sind.
2. Das *Web*, in dem die meiste Software immer noch auf dem PC installiert ist, aber immer mehr Daten nur im Netz gefunden werden können.
3. Die *Wolke*, in dem die Benutzer ausschließlich auf im Internet verfügbare Software und Daten setzen.

Die Übergänge dieser drei Phasen sind dabei fließend. Die meisten Tätigkeiten, die wir am Computer erledigen, sind immer noch in Phase 1 oder 2 angesiedelt. Zurzeit lässt sich ein langsamer Übergang in Phase 3 beobachten und es beginnen immer mehr Menschen, die Vorteile der Cloud zu nutzen.

Viele Benutzer haben bereits Erfahrungen mit Cloud Computing gemacht ohne es wahrzunehmen oder die dahinterliegende Technologie zu verstehen. So sind die meisten Benutzer mit einem Textverarbeitungsprogramm wie Microsoft Word vertraut. Das Programm wird auf dem Computer gestartet und erstellte Dokumente werden auf der Festplatte des Computers gespeichert.

Im Gegensatz dazu erlaubt es Cloud Computing, die komplette Aufgabe über das Internet auszuführen, wodurch sie nicht mehr an einen bestimmten Computer gebunden ist. Über das Internet kann der Benutzer ebenfalls eine entsprechende, auf einem Server installierte Textverarbeitungssoftware, z.B. Google Documents, starten und erstellte Textdokumente werden dann auf den Servern des Providers gespeichert.

Analysiert man das Cloud-Computing-Konzept genauer, lassen sich fünf wesentliche Merkmale ableiten [16]:

1. **Nutzung von Ressource nach Bedarf.** Ein Kunde erwirbt dabei automatisch die benötigten Rechenkapazitäten und Netzwerkspeicher und ohne den Provider zu kontaktieren. Die Abrechnung erfolgt ebenfalls automatisch.
2. **Verfügbarkeit.** Wenn eine Breitbandnetzverbindung besteht, können die angebotenen Cloud-Dienste von nahezu allen Endgeräten genutzt werden.
3. **Abstrahierte Ressourcennutzung.** Die verfügbaren Ressourcen eines Anbieters werden gebündelt, um so für viele Benutzer gleichzeitig verfügbar zu sein. Der Benutzer hat meist keine Kontrolle und kein Wissen darüber, woher die Ressourcen stammen.
4. **Skalierbarkeit und Belastbarkeit.** Die Ressourcen können beliebig skaliert und an die entsprechende aktuelle Auslastung angepasst werden. Für den Benutzer scheint es, als seien die Ressourcen unbegrenzt.
5. **Automatische Optimierung.** Cloud-Systeme kontrollieren und optimieren den Bedarf an Ressourcen automatisch. Dies geschieht durch die Überwachung verschiedener Parameter wie aktuell verfügbarer Bandbreite, Anzahl der aktiven Benutzerkonten oder verfügbarem Speicher.

1.1 Verwandte Begriffe

Die zuvor aufgezählten Merkmale unterscheiden das Cloud-Computing von anderen verwandten Begriffen. Diese Begriffe wie Grid Computing und Virtualisierung sind jedoch auch als Basistechnologien und Voraussetzung für Cloud Computing zu betrachten.

Beispielsweise war der Begriff Grid Computing wenige Jahre zuvor ein ähnliches Hypeword und wurde mindestens genauso umfangreich beworben. Dies hat zahlreiche Diskussionen über die Abgrenzung zwischen Grid und Cloud Computing angeregt. Zwischen beiden Konzepten existiert aber ein wesentlicher Unterschied: Bei Grid Computing geht es um die gemeinschaftliche Nutzung der gemeinsamen Ressourcen und es gibt keine zentrale Steuerung. Im Gegensatz dazu existieren beim Cloud Computing ein Anbieter von Ressourcen und ein Nutzer. Die Steuerung der Ressourcen erfolgt zentral.

Das Cloud-Konzept ist ebenfalls nicht zu verwechseln mit Peer-to-Peer-Netzwerken. Der Unterschied zwischen beiden Ansätzen liegt hier bei den unterschiedlichen Zielsetzungen. In Peer-to-Peer-Netzwerken geht es darum, Rechenlast auf möglichst viele Rechner zu verteilen und den Server zu entlasten. Beim Cloud Computing hingegen geht es nicht um Verteilung, sondern um das Auslagern von Rechenlasten. Anstatt eigene Rechner-, Server- oder Softwareressourcen zu nutzen oder die Last im Netzwerk zu verteilen, werden die Ressourcen von Cloud-Anbietern genutzt.

Cloud-Computing ähnelt dem klassischen Outsourcing von IT-Ressourcen, bei dem Arbeits- und Geschäftsprozesse einer Organisation zu externen Dienstleistern ausgelagert werden. Im Gegensatz zum Outsourcing ist das Auslagern von Ressourcen durch Cloud Computing innerhalb kürzester Zeiträume beliebig skalierbar, wodurch Cloud-Dienste schneller an den tatsächlichen Bedarf angepasst werden können. Außerdem können die Ressourcen über mehrere Standorte hinweg dynamisch verteilt

werden. Dadurch, dass die Steuerung der Cloud-Dienste meist über eine Webschnittstelle erfolgt, kann der Benutzer die Dienste gezielt an seine Bedürfnisse anpassen [32].

Ein weiterer im Kontext auftauchender Begriff ist Service-orientierte Architektur (SOA). SOA ist im Wesentlichen eine einheitliche Abbildung von Geschäftsprozessen, mit der organisationsübergreifend Prozesse abgewickelt werden können. SOA wird meist in Form von Webservices angewendet, mit denen Daten zwischen unabhängigen Organisationen ausgetauscht werden können [2]. Diese Webservices bilden die Schnittmenge zwischen Cloud Computing und SOA.

Im Zusammenhang mit Cloud Computing fällt immer wieder der Begriff *Virtualisierung*. Virtualisierung ist das Betreiben eines „virtuellen Computers“ auf einer meist fremden Hardware durch eine logische Trennung eines Programms vom Betriebssystem des genutzten Rechners. Virtualisierung ist Bestandteil vieler Sicherheitskonzepte von Cloud-Systemen, wie z.B. Amazons Elastic Compute Cloud [23].

Beim Cloud-Computing werden die angebotenen Dienste in den drei Ebenen *Software-as-a-Service* (SaaS), *Platform-as-a-Service* (PaaS), *Infrastructure-as-a-Service* (IaaS) bereitgestellt [16]. Alle drei Schichten haben gemeinsam, dass die Abrechnung nach Bedarf erfolgen kann und sie beliebig skalierbar sind.

Bei der untersten Schicht, der *Infrastructure as a Service* (kurz: IaaS) wird sämtliche Infrastruktur wie zum Beispiel Archivierungs- oder Backup-Systeme zur Verfügung gestellt. Darunter fallen auch komplette Betriebssysteme oder Firmenintranets.

Der große Vorteil gegenüber traditionellen Datacentern ist die Skalierbarkeit und die Möglichkeit, Daten repliziert zu halten, um Verluste und Verfügbarkeitsprobleme weitestgehend zu vermeiden. Einer der ersten großen Anbieter von IaaS war Amazon mit dem 2008 eingeführten Konzept *Amazon Elastic Compute Cloud*. Mit der Windows Azure Platform ist auch Microsoft in das Cloud-Computing-Geschäft eingestiegen.

Die mittlere Schicht wird als *Platform as a Service* (oder kurz: PaaS) bezeichnet. Auf dieser Cloud-Plattform werden IT-Entwicklungen errichtet und gehostet. Auch die Bereitstellung von Software-Systemen wie Datenbanken, Programmierumgebungen oder Application Servern gehören zur PaaS. Beispiel für PaaS-Anbieter sind die Google App Engine, die Microsoft Azure Service und Force.com.

Die oberste Ebene heißt *Software as a Service* (kurz: SaaS). Hier wird die Software bei einem Dienstleister entwickelt und betrieben. Der Benutzer benötigt dann nur noch einen Account für den Zugriff auf die bereitgestellte Software. Die Abrechnung erfolgt nach Bedarf, daher steht der Begriff SaaS oft stellvertretend für Mietsoftware. Der Vorteil dieses Konzepts besteht darin, dass die angebotene Software plattformunabhängig und keine Installation nötig ist. Beispiele für SaaS sind Google Docs, Microsoft Live Services für Privatpersonen und Google Apps for Business sowie Microsoft Online Services für Konzerne und größere Unternehmen.

Bei den Nutzungsarten kann man zwischen *Private Clouds* und *Public Clouds* unterscheiden. Private Clouds sind vernetzte Rechner, die von Firmen oder Privatpersonen betrieben werden und deren Ressourcen nicht öffentlich zugänglich sind. Als Private Clouds gelten auch Rechnernetze von rechtlich zueinander in einem engen Verhältnis stehenden Stellen, z.B. Stellen der öffentlichen Verwaltung oder eines Unternehmenskonzerns.

Bei Public Clouds wird die Rechenleistung von Dritten im Sinne des geltenden Datenschutzrechtes angeboten. Anbieter von Public Clouds sind die ganz großen globalen IT-Unternehmen, wie beispielsweise Amazon, Google, Microsoft oder IBM. Diese verarbeiten die Daten auf weltweit verteilten Servern bzw. Serverfarmen, die einem oder auch unterschiedlichen Anbietern gehören [12]. Bei solchen Public-Clouds ist das Datenschutzproblem der Cloud besonders ausgeprägt, denn hier muss der Benutzer für die Inanspruchnahme der Cloud-Dienste seine Daten an Dritte aushändigen.

Hybride Clouds sind eine Mischung von Private- und Public Clouds, also eine Nutzung sowohl von eigenen als auch fremden Ressourcen. Eine Besonderheit stellen die Community Clouds dar, bei

denen eine Cloud-Infrastruktur gemeinsam genutzt wird, wobei gemeinsame Anforderungen, z.B. an die Sicherheit und an den Datenschutz kollektiv vereinbart und festgelegt werden können.

1.2 Cloud-Nutzer und Anbieter

Beim Cloud-Computing kann man zwischen drei verschiedenen Rollen unterscheiden: Cloud-Nutzer, Cloud-Anbieter und Ressourcen-Anbieter. Der Cloud-Nutzer nimmt die Rechenleistung von Cloud-Diensten in Anspruch. Der Cloud-Anbieter stellt diese Dienste dem Cloud-Nutzer zur Verfügung. Die Ressourcen-Anbieter stellen dem Cloud-Anbieter für die Cloud-Datenverarbeitung ihre Hard- oder Software bereit, damit diese zusammengefasst dem Nutzer angeboten werden können.

Einer der ersten großen Anbieter war Amazon mit dem 2008 eingeführten Konzept *Amazon Elastic Compute Cloud* (kurz: *EC2*). Auch andere größere Unternehmen wie Microsoft oder Google haben diesen Markt ebenfalls für sich entdeckt und werden um ihren Anteil an potentiellen Gewinnen kämpfen. Der Markt für Cloud-Dienstleistungen ist vorhanden und er wird zweifelsohne noch wachsen. Außerdem existiert eine Vielzahl von Hosting-Unternehmen, die ihre virtuellen Server kleinen Unternehmen oder Privatpersonen preisgünstig anbieten.

Die großen IT-Dienstleister wie Amazon, Microsoft oder Google stellen Cloud-Dienste auf allen drei Ebenen bereit, die sich auch durch unterschiedliche Sicherheitskonzepte unterscheiden.

Die Amazon EC2 ist ein Dienst auf der IaaS. Man kann EC2 als eine Art virtuellen Host betrachten. Sie erlaubt es Benutzern, virtuelle Computer zu mieten und darauf Anwendungen laufen zu lassen. Jeder virtuelle Computer wird dabei als Instanz bezeichnet. Bei der Erstellung einer EC2-Instanz erhält der Rechner sowohl eine öffentliche, von außen erreichbare IP sowie eine private IP zur Kommunikation innerhalb der EC2-Cloud. Nach der Definition der entsprechenden Sicherheitsregeln kann auf den Rechner beispielsweise über Remotedesktop von jedem Standort der Welt zugegriffen werden. Für eine Gewährleistung von Sicherheit hat Amazon eine Vielzahl von Mechanismen eingebaut.

Die Amazon Virtual Private Cloud (kurz: Amazon VPC) ist ebenfalls ein kommerzieller Cloud-Computing-Dienst. Er stellt eine virtuelle, private, nach außen hin abgeschottete Cloud als Brücke zur bereits vorhandenen Infrastruktur eines Unternehmens und der Amazon Elastic Compute Cloud zur Verfügung. Der Zugriff auf die Amazon Elastic Compute Cloud erfolgt über isolierte AWS-Rechenressourcen, die über eine abgesicherte VPN-Verbindung laufen. Mit dieser Technik ist es möglich, einen Teil oder die gesamte IT-Infrastruktur eines Unternehmens auf die Cloud auszulagern.

Die App Engine von Google ist ein Dienst auf PaaS-Ebene. Er erlaubt es, Web-Applikationen in einer skalierbaren Cloud-Umgebung zu entwickeln und zu hosten. Sie arbeitet auf der PaaS-Ebene.

Für die Sicherheit sorgt bei der Google App Engine der Secure Data Connector (SDC). Hiermit kann der Anwendungsentwickler Regeln festlegen, auf welche Ressourcen die Benutzer der Anwendung zugreifen dürfen. Diese Regeln werden den Google Apps übermittelt, so dass bestimmte Benutzer auch auf Ressourcen zugreifen können, die hinter der Firewall des Unternehmens liegen. Ähnlich wie beim Amazon VPC ist es somit möglich, die Cloud mit bereits bestehenden Ressourcen zu verbinden.

Googles Informationspolitik zum Thema Sicherheit ist äußerst spärlich. Im Security White Paper [25] wird zwar geschrieben, dass das System gegen alles geschützt ist, aber gegen welche Attacken genau und mit welchen Mechanismen, das verrät Google nicht.

Ebenso wie Google App Engine ist die Windows Azure auf der PaaS-Ebene angesiedelt. Windows Azure Platform ist Microsofts Cloud-Computing-Plattform, in der Unternehmen web-basierte Dienste entwickeln, verbreiten und verwalten können.

Cloud-Anbieter stellen Anwendungen und Datenbanken zur Verfügung, die in der Cloud genutzt werden können. Die Anwendungen und die dazugehörigen Daten werden dann in der Azure-Cloud gehostet. Die Azure-Cloud hat verschiedene Sicherheitstechniken eingebaut. Ein wichtiger Aspekt zur Absicherung der Daten ist das Überprüfen der Identitäten der Zugreifenden. Für diesen Zweck hat

Microsoft den .NET Access Control Service eingebaut, der mit Hilfe von Webservices versucht, gemeinsame Identitäten integriert [24].

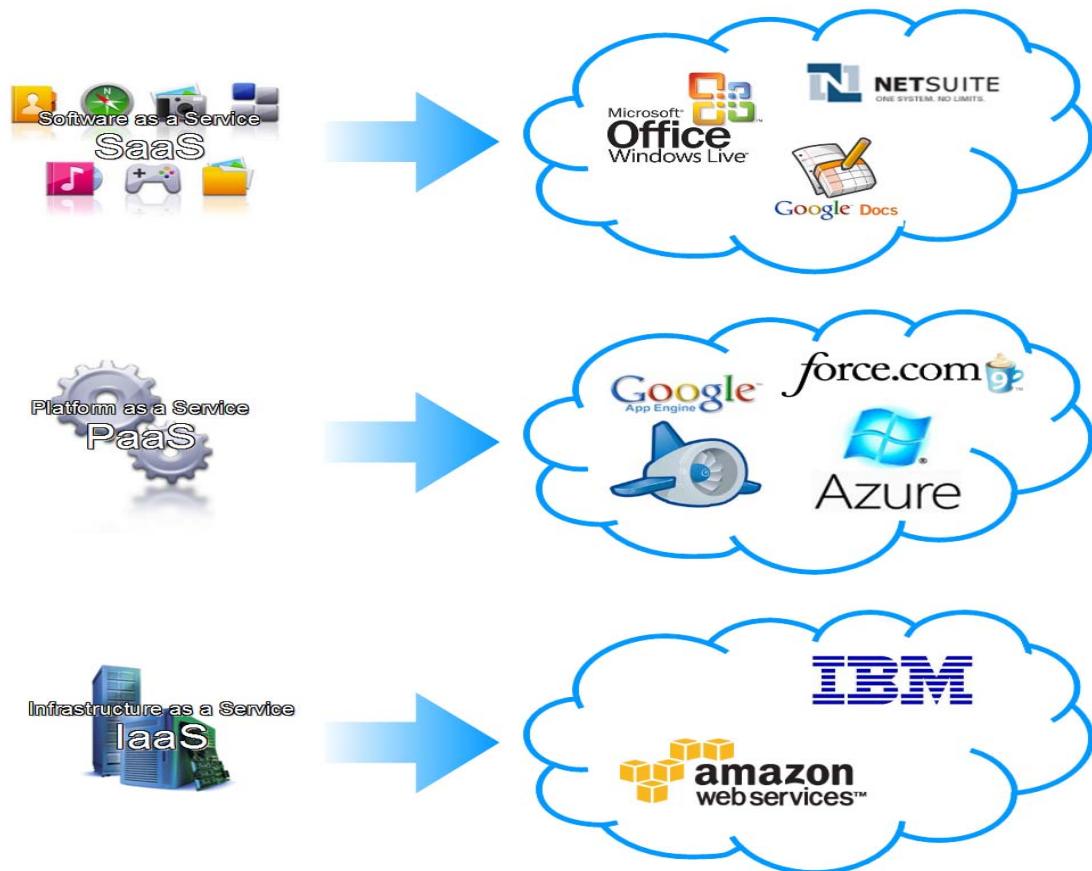


Abbildung 2: Die drei Service-Ebenen vom Cloud Computing und ausgewählte Anbieter.

Auf SaaS-Ebene bieten Google und Microsoft mit Google Docs und Office365 zudem auch in der Cloud laufende Bürosoftware an.

Während große, international agierende IT-Firmen wie Amazon, Microsoft oder Google Cloud Computing für Standardanwendungen wie z. B. E-Mail, Bürosoftware oder Speicherplatz im Netz bereits anbieten, sind viele kleinere IT-Dienstleister, mittelständische und öffentliche Einrichtungen in Sachen Cloud-Computing noch eher zurückhaltend. Das ist zum einen durch die nicht ausreichende Standardisierung als auch durch die hohe Komplexität und dem Entwicklungsstand der Technik geschuldet. Wird dem Mittelstand der Zugang zu modernen Cloud-Technologien eröffnet, ergäbe sich ein großes Potenzial für den Wirtschaftsstandort Deutschland, prognostiziert das BMWi [33].

Für die Cloud-Anbieter wird die Hardware-Beschaffung bald eine der größten Herausforderungen darstellen [2]: Steigt die Nachfrage nach Cloud-Diensten, werden auch mehr Server benötigt werden. Entsprechende Serverzentren müssen sich in geographischer Nähe zu den Kunden befinden, da die Übermittlungszeit von der Entfernung zwischen Kunde und Server abhängig ist. Es existieren beispielsweise seit kurzem zwei Anbieter von Online-Gaming, die solche Echtzeit-Verbindungen voraussetzen: Gaikai und OnLive. Bei solchen Anwendungen sind bereits Verzögerungen von 50 ms inakzeptabel, weil sonst die Echtzeitfähigkeit der Spiele verloren geht [21].

Haben sich Cloud-Dienste erst einmal bei Privatkunden etabliert, werden die Provider gezwungen sein, erheblich mehr Hardware zuzukaufen. Innerhalb der nächsten zehn Jahre werden wohl in jeder Stadt Serverzentren entstehen, von denen sich einige voraussichtlich in Mehrzweckgebäuden mit mehr als 100 Bewohnern befinden werden [11].

Zur Zeit sind Geschäftskunden die Hauptzielgruppe der meisten Anbieter. Es zeigt sich aber, dass immer mehr Privatpersonen Cloud-Dienste nutzen.

Erst mit der flächendeckenden Akzeptanz und Nutzung von Cloud-Dienste unter Privatpersonen wird das Cloud-Konzept von Erfolg gekrönt sein. Denn momentan gibt es auf Anwenderseite immer noch Zweifel an der Zuverlässigkeit, Sicherheit und den ökonomischen Vorteilen von Cloud Computing.

Welche Macht die Cloud-Anbieter haben, welche Verantwortung sie tragen, zeigt sich besonders in den Momenten, in denen die Informationen auf der Cloud plötzlich nicht mehr zugänglich sind oder nicht mehr auffindbar sind.

Beispielsweise waren Mail-Accounts von Google im vergangenen September mehrere Stunden nicht mehr erreichbar. In einem anderen Fall waren für einige T-Mobile-Kunden in den USA, die das Sidekick-Smartphone nutzten, ihre Kalendereinträge, Telefonnummern und Fotos scheinbar für immer verschwunden, tauchten aber nach ein paar Tagen plötzlich wieder auf [11].

1.3 Vor- und Nachteile

Sicherlich liegt die Motivation für den Einsatz von Cloud Computing primär in ökonomischen Interessen begründet. Dazu zählen zum einen Kostensenkungen und verringerte Kapitalbindung, weil weniger in neue Hardware und stattdessen in operative Betriebskosten (z.B. Personalkosten) investiert wird. Aber auch der verbesserte Zugriff auf die öffentlich zugänglichen Unternehmensdaten und eine höhere Geschwindigkeit bei der Umsetzung von Geschäftsprozessen spielen eine Rolle.

Denn durch die bessere Verteilung von Lasten auf vorhandenen Systemen kann Cloud Computing erhebliche Kostenvorteile in der Datenverarbeitung ermöglichen. Einzelne Server müssen nicht mehr übertrieben leistungsfähig sein, weil sich alle verfügbaren Systeme an allen anstehenden Aufgaben gemeinsam beteiligen.

Aber ist gibt noch weitere Vorteile:

- **Unbegrenzte Flexibilität:** Mit dem Zugriff auf Millionen von unterschiedlichen Teilen von Software und Datenbanken und der Fähigkeit diese zu angepassten Diensten zu kombinieren, sind die Benutzer besser als je zu vor in der Lage, die Antworten auf ihre Fragen zu finden, ihre Gedanken zu teilen und das Internet gemeinsam zu erleben.
- **Bessere Zuverlässigkeit und Sicherheit:** Die Benutzer müssen sich keine Sorgen mehr über Festplattencrashes oder gestohlene Laptops machen.
- **Verbesserte Beteiligung:** Durch die Möglichkeit, Informationen und Anwendungen online zur Verfügung zu stellen, bietet die Cloud den Benutzern neue Wege gemeinsam zu arbeiten.
- **Portierbarkeit:** Die Benutzer können von überall auf ihre Daten zugreifen, wenn eine Internetverbindung besteht.
- **Digitale Rechteverwaltung:** Mit Cloud-Computing würden DRM-Dateien einen zweiten Frühling erleben, da Content-Produzenten den Kunden Filme, Spiele und Musik auf direktem Weg anbieten können. Die angebotenen Inhalte werden rein für das Abspielen innerhalb des Cloud-Computing-Systems konzipiert und die Erstellung von unautorisierten Kopien derartiger Film- und Musikdateien wird erheblich mehr Zeit und Geld kosten. Letztlich kann somit die Anzahl illegaler Kopien reduziert und der Gewinn der Produzenten gesteigert werden.
- **Automatische Updates:** Der Benutzer muss seine Software nicht mehr manuell auf dem neusten Stand halten. Mit in der Cloud laufenden Anwendung kann dies automatisch geschehen, so dass das Arbeiten mit dem Heimcomputer billiger, sicherer und zuverlässiger wird.
- **Wettbewerbsvorteile:** Mit Cloud Computing können auch mittelständische Unternehmen Technologien nutzen, die bislang großen Unternehmen vorbehalten waren. Durch die Auslagerung der Infrastruktur können sich die Unternehmen so auf ihr eigentliches Kerngeschäft konzentrieren. Die erwarteten Effektivitätsvorteile und die Qualitätsverbesserungen können die Wettbewerbsfähigkeit der gesamten Wirtschaft erhöhen.

Ungeklärt ist, ob sich durch Cloud Computing der Energieverbrauch reduziert. Das BMWi schätzt, dass dadurch den Einsatz von Cloud Computing der Energieverbrauch langfristig gesehen sinkt [33]. Der Chef vom US-Venture-Unternehmen Spencer Trask, Bill Clifford, prognostiziert hingegen, dass

der Energieverbrauch durch Cloud Computing durch „Ghost-Server“ drastisch ansteigen wird [10]. Auch Greenpeace warnt vor einer drastischen Erhöhung des Anstiegs an Treibhausgasen [34].

So verheißungsvoll das Konzept auch klingen mag, so gibt es besonders sicherheitstechnisch viele Probleme zu bewältigen. Kaum ein Tag vergeht ohne Meldung über abgefangene oder verlorengangene Daten, denn das Hauptproblem beim Cloud Computing ist, dass der Kunde dem Cloud-Anbieter sämtliche für die Dienste benötigten Daten zur Verfügung stellen muss und nicht nur einen ausgewählten Anteil. Doch enthalten eben diese Daten meist auch Geschäftsgeheimnisse oder private Informationen, die Rückschlüsse auf die Identität des Nutzers zulassen.

Zu welchem Unternehmen hat aber man soviel Vertrauen, dass man vollen Zugriff nur nicht auf seine E-Mail-Nachrichten, sondern auch auf sämtliche Passwörter, Bankkontoinformationen und private Dokumente gewähren würde? Selbst wenn das Vertrauen in ein bestimmtes Unternehmen vorhanden wäre, fehlt schlicht eine Garantie dafür, dass die Daten nicht in falsche Hände geraten.

Daraus ergibt sich ein grundlegendes Datenschutzproblem in der Cloud. Die Preisgabe von Geschäftsgeheimnissen kann zu Rufschädigungen und finanziellen Einbußen beim betroffenen Unternehmen führen. Und ein Datenverlust hätte weitreichende Folgen. Durch die Veröffentlichung personenbezogener Daten entsteht ein Konflikt mit dem Bundesdatenschutzgesetz, denn bei personenbezogenen Daten ist nach deutscher Gesetzgebung das Datenschutzrecht anwendbar, wenn anhand der vorhandenen Daten eine eindeutige Identifizierbarkeit einer lebenden Person möglich ist.

Ein weiteres Problem bei der Nutzung öffentlicher Ressourcen ist nach wie vor die Abschottung des Datentransfers über Internet-Leitungen. Aber nicht nur der Transport, sondern auch die Verarbeitung und Speicherung der persönlichen oder Firmendaten muss verlässlich abgeschottet sein. Zwar existieren Ansätze zur Verteilung von Daten auf unterschiedliche Ressourcen ohne Möglichkeit, Rückschlüsse auf die Produktionsdaten zu ziehen, jedoch bestehen auch hier immer noch berechtigte Bedenken.

Und so ist wie bei vielen neuen Technologien auch beim Cloud Computing die Gesetzeslage größtenteils unklar [8]. Denn meist werden die benötigten Gesetze erst entworfen und verabschiedet, nachdem solche neuen Technologien entworfen wurden und sich auf dem Markt etabliert haben. Dies ist auch bei Cloud Computing der Fall. Ein entsprechender Dienstleister kann nicht genau sagen, welcher Teil einer Datei sich gerade wo befindet. Allerdings könnten sich die genutzten Ressourcen außerhalb des eigenen Rechtsraumes befinden, was im Widerspruch zum Bundesdatenschutzgesetz steht.¹

Die Sicherheits- und Datenschutzproblematiken von Cloud-Computing sollen nun in den folgenden Abschnitten näher beschrieben werden.

¹ siehe BDSG §9 und §11

2 Cloud Computing und Sicherheit

Bereits Anfang 2006 schrieb der Sicherheitsexperte Bruce Schneier über die Sicherheitsproblematik in der Cloud [28]. Im weiteren Verlauf wurden so zahlreiche Diskussionen über die Art und Weise angeregt, wie man ein sinnvolles Sicherheitskonzept umsetzen könnte.

Schon allein die bisher vorliegenden Informationen und Erkenntnis sollten suggerieren, dass die Umsetzung eher eine Notwendigkeit denn eine Option ist. Aus welchem Grund haben sich beispielsweise die Hersteller von Antiviren-Software mehrere Jahre Zeit gelassen, bevor sie mit der Implementierung entsprechender Technologien in ihre Produkte begannen? [13]

2.1 Sicherheitsrisiken

Infrastruktur-Dienste aus der Wolke können zum Sammelbecken krimineller Projekte wie beispielsweise Botnetze oder Trojaner werden. Im Artikel [22] im Paper [18] der Cloud Security Alliance (CSA), ein Zusammenschluss von Firmen, werden die sieben gravierendsten Sicherheit beim Cloud Computing herausgestellt:

1. Die Registrierung ist zu einfach.

Für die Nutzung und Bezahlung einiger Cloud-Dienste reicht lediglich die Eingabe einer Kreditkartennummer aus. Zum Teil sind die Registrierungsvorgänge so einfach gehalten, dass zwar eine völlige Anonymität der Nutzer, aber dadurch eben auch Identitätsdiebstahl oder -missbrauch einfach möglich sind. Hier sind Authentifizierungssysteme wie OpenID gefragt. Dies betrifft die SaaS-Ebene.

2. Die Schnittstellen sind zu unsicher.

Damit Kunden Cloud-Dienste nutzen und anbinden können, legen die Cloud-Anbieter ihre Schnittstellen offen. Zwar versprechen die Anbieter das Einhalten von Sicherheitsstandards, jedoch ist dies keine Verpflichtung. Dadurch können sich Benutzer also nie hundertprozentig sicher sein, ob ihre Daten verschlüsselt und entsprechend eines bestimmten standardisierten Sicherheitsniveaus übertragen werden. Solche unsicheren Schnittstellen sind eine Folge der zum Teil zu einfachen Registrierung für Cloud-Dienste. Die Schnittstellen befinden sich in der PaaS- und IaaS-Ebene.

3. Kriminelle Mitarbeiter.

Zwar stellen kriminelle Mitarbeiter für jedes Unternehmen eine Gefahr dar, aber beim Cloud Computing bekommt dieses Problem eine neue Dimension. Der Kunde vertraut dem Anbieter seine Daten an, während gleichzeitig nicht geklärt ist, welche Anforderungen und Richtlinien für den Umgang mit den Kundendaten der Anbieter an seine Mitarbeiter stellt. Beispielsweise könnte ein Mitarbeiter Root-Rechte besitzen und so uneingeschränkten Zugriff auf Kundendaten haben. Hier ist auf allen Ebenen Sicherheit zu gewährleisten, besonders jedoch auf der IaaS-Ebene.

4. Unsichere Infrastruktur.

Viele Cloud-Rechenzentren weisen keine Infrastruktur auf, bei dem die Daten und Anwendungen strikt voneinander getrennt sind. Auch sind die Komponenten, auf denen die Dienste basieren, nicht dafür ausgelegt, die Speicherbereiche, die von mehreren Kunden genutzt werden, klar voneinander abzugrenzen.

5. Diebstahl von Zugangsdaten.

Durch den Diebstahl von Zugangsdaten kann ein Angreifer auf Daten und Vorgänge eines Unternehmens zugreifen und so Daten manipulieren, heimlich verfolgen oder Kunden auf kriminelle Webseiten locken. Hier muss die Sicherheit auf der IaaS-Ebene gewährleistet sein.

6. Mängel bei der Verschlüsselung.

Ungenügende Sicherheitskontrollen und ein inkonsequenter Einsatz von Kryptographie machen Cloud Computing zu einem Risiko. Dadurch kann es zu Datenmissbrauch und Datenverlusten kommen. In falsche Hände geratene Daten können nicht nur das Vertrauen von Kunden, Geschäftspartnern und Mitarbeitern gefährden, sondern vor allem auch finanzielle Folgen haben. Verschlüsselung ist in allen drei Ebenen von Bedeutung.

7. Intransparente Sicherheitslage.

Die Kunden eines Cloud-Dienstleisters können zwar einfach und ausgiebig dessen Angebote und Funktionen erfahren, jedoch wenig über die internen Vorkehrungen, insbesondere zum Thema Sicherheit. Wer Zugang zum Anbieter besitzt oder welche Informationen bei Sicherheitsvorfällen veröffentlicht werden, sei meist nicht geklärt.

Neben diesen sieben Sicherheitsrisiken gibt es aber noch eine Reihe weiterer. Zum einen stellt die Marktkonkurrenz eine Gefahrenquelle dar. Diese ist an den Kundendaten und Geschäftsabläufen der Mitbewerber interessiert.

Desweiteren häufen sich Fälle von Industriespionage durch Geheimdienste, wie beispielsweise in China. Zwanzig Prozent aller deutschen Unternehmen berichteten über Fälle von Industriespionage. Für die deutschen Unternehmen entstehen so jährlich 50 Milliarden Euro Verlust [29].

Ein weiteres Problem besteht darin, dass den Geheimdiensten wie dem BND oder dem CIA unter dem Deckmantel der Terrorbekämpfung Zugriff auf die in der Cloud gespeicherten Daten gewährt werden kann und darf. Die Polizeibehörden sind nicht zu einer Auskunft über eventuelle Präventivzugriffe verpflichtet.

Auch offene Standards können ein Sicherheitsrisiko darstellen. Offene Standards werden benötigt, um die Fülle an Umgebungs- und Anwendungsszenarios zu unterstützen, in denen das Cloud Computing für die Ermöglichung der Interoperabilität eine kritische Rolle spielt. Mit der Einführung von Standards wird allerdings wohl auch die Aufmerksamkeit von Malware-Autoren und Hackern geweckt werden [9]. Dieses Phänomen hat sich schon im Zuge der Standardisierung von PCs, auf denen mit überwiegender Mehrheit das Windows-Betriebssystem installiert ist, bereits eindrucksvoll bewahrheitet.

Sobald Cloud-Computing eine ausreichende Verbreitung hat, wird es mit großer Wahrscheinlichkeit auch genau auf diese Systeme spezialisierte Hacker geben. Auch hier wird es deren Ziel sein, Daten zu stehlen oder zu manipulieren – immer unter dem Hintergrund des finanziellen Vorteils. Zudem wird es weiterhin die Art Betrüger geben, die an der Technik an sich kein besonderes Interesse zeigt.

Allerdings ist eine Standardisierung auch notwendig, um ein Marktmonopol eines Anbieters zu verhindern und so eine möglichst anbieterunabhängige Cloud-Infrastruktur zu schaffen.

Deshalb ist eine Standardisierung der Schnittstellen und Formate auch erforderlich, um Portabilität gewährleisten zu können. Aber diese Standards müssen auch so spezifiziert werden, dass gleichzeitig ein akzeptables Sicherheitsniveau (beispielsweise nach ISO 27001, vgl. Abschnitt 2.4.1) gegeben ist.

Das Sicherheitsrisiko ist deshalb so groß, weil über die Cloud völlig neue Angriffsmöglichkeiten von Cyberkriminellen eröffnet werden. Diese können die schwächste Sicherheitsstelle der Cloud nutzen, um in diese einzudringen. Da die Cloud- und Ressourcenanbieter kein eigenes Interesse an der Datenverarbeitung, sondern nur an deren Vergütung haben, ist es Kriminellen leicht möglich, unerkannt in die Rolle des Nutzenden zu schlüpfen, um die Datenverarbeitung auszuspionieren und zu sabotieren.

Auch beim alljährlichen Hacker-Treff *Security Nightmares* herrschte Einigkeit darüber, dass es sicherheitstechnisch in Sachen Cloud Computing noch einige Hindernisse zu überwinden gibt [15]. *Scanning*, *Cracking* und *Botnet Command and Control* seien nach wie vor Gefahren in der Cloud. Außerdem gebe es bereits Ansätze zum Umgehen des Hypervisors und zum Slice Hopping, also dem Springen von Maschine zu Maschine. Angreifer können so gleich hunderte von Maschinen unter ihre Kontrolle bringen und so auf Nutzerdaten zugreifen. Außerdem seien die Standardeinstellungen zur Sicherheit in der Cloud häufig zu niedrig eingestellt. Dadurch werden verschiedenartige Angriffe auf die Cloud begünstigt.

2.2 Angriffsarten

Angriffe auf Webanwendungen sind keine Seltenheit und auch Cloud-Computing-Systeme sind nicht davor geschützt. Neben passiven und aktiven Angriffen auf Cloud-Computing-Systeme kann man Gefahren zusätzlich zwischen internen und externen Bedrohungen unterscheiden [19].

Es gibt eine Vielzahl von Angriffsarten, von denen an dieser Stelle nur ein paar ausgewählte beschrieben werden sollen.

2.2.1 Aktive und passive Angriffe

Passive Angriffe zeichnen sich dadurch aus, dass der Angreifer ohne Eingriff in das System Informationen erlangt. Ein Beispiel hierfür ist das Mithören bzw. Mitschneiden von Informationen über das Netzwerk. Da der Angreifer nicht aktiv in das IT-System eingreift, sondern nur passiv zuhört, ist es sehr schwer einen solchen Angriff zu erkennen. Das Mitschneiden von WLAN-Daten bei Google-Street-View könnte man so als einen passiven Angriff deuten.

Um diese Arten von Angriffen zu verhindern, müssen die übertragenen Daten verschlüsselt werden und weitere Maßnahmen (z.B. keine Übertragung wichtiger Daten an den Cloud-Anbieter oder Ersetzen wichtiger Daten durch Platzhalter) eingesetzt werden, die das Mithören erschweren. Passive Angriffe bedrohen die Schutzziele Vertraulichkeit und Authentizität [19].

Bei aktiven Angriffen tritt der Angreifer selbst in Erscheinung indem er z.B. Daten modifiziert oder löscht oder Sicherheitslücken bzw. die Verfügbarkeit von Diensten oder auch beteiligten Diensten sabotiert. Diese Angriffe können auffallen und Spuren hinterlassen, so dass eine Erkennung des Angriffs und vielleicht sogar des Angreifers möglich ist. Außerdem können aktive Angriffe als Vorbereitung für passive Angriffe eingesetzt werden, indem der Datenstrom z.B. so umgelenkt wird, dass der Angreifer daraufhin passiv mithören kann. Die Schutzziele Verfügbarkeit, Integrität und Authentizität sind durch aktive Angriffe bedroht.

2.2.2 Externe Angriffe

Bei einem externen Angriff wird das Cloud-System von außen angegriffen. Unter den externen Angreifern existieren drei verschiedene Typen, die ihre Angriffe mit unterschiedlichen Intentionen und Erfahrungsebenen vollführen: die *Hacker*, die *Cracker* und die *Script-Kiddies*.

Unter der Bezeichnung *Hacker* werden Technikenthusiasten verstanden, die umfangreiche computertechnische Grundlagenkenntnisse besitzen und im Falle der Computersicherheit zusätzlich sicherheitstechnische Kenntnisse haben. Hacker sehen ihre Herausforderung in der Überwindung von Sicherheitsmechanismen, um Schwachstellen zu erkennen. Durch die Umgehung der Sicherheitsmechanismen können somit Zugriffe auf Netzwerke, Virtuelle Maschinen, gesicherte Komponenten oder fremde Dateien erlangt werden.

Hacker greifen ihre Ziele nicht an, sondern begnügen sich mit der Überwindung der Sicherheitsmechanismen, um deren Schwachstellen aufzuzeigen, trotzdem ist nicht zu vergessen, dass auch Hacker sich im rechtlich illegalen Bereich bewegen, wenngleich sie der Hacker-Ethik unterworfen sind.

Cracker können das gleiche Fähigkeitsniveau wie Hacker erreichen, jedoch geht es ihnen beim Angriff auf ein IT-System nicht darum Schwachstellen im System aufzuweisen, sondern sich aufgrund von meist kommerziellen Interessen heraus einen Vorteil zu verschaffen oder Chaos zu stiften. Vorteile kann er sich zum Beispiel verschaffen, wenn er sich Zugriff auf Cloud-Ressourcen oder Cloud-Services ermöglicht, ohne deren Verbrauch bezahlen zu müssen. Durch Angriffe auf Webserver und Mitlesen oder Veränderung von Daten versucht der Cracker dem Cloud-Computing-System Schaden zuzufügen.

Der dritte Typ sind die *Script-Kiddies*, diese sind im Vergleich zu Hackern und Crackern unerfahren und können die wenigsten Kenntnisse von Computern und deren Sicherheitsmechanismen vorweisen. Meist führen sie ihre Angriffe rein zufällig und unter Verwendung von Skripten oder gebrauchsfertigen Softwareprogrammen durch, deren Funktionsweise sie nicht kennen und über deren Folgen sie sich nicht im Klaren sind.

2.2.3 Seitenkanalattacken

Eine Seitenkanalattache ist eine kryptoanalytische Methode, die die physikalische Implementierung eines Kryptosystems in einem Gerät oder in einer Software ausnutzt. Es wird dabei nicht das kryptographische Verfahren selbst, sondern nur eine bestimmte Implementierung angegriffen.

Das Prinzip beruht auf der Beobachtung eines kryptographischen Gerätes bei der Ausführung der kryptologischen Algorithmen sowie dem Finden von Korrelationen zwischen den beobachteten Daten und dem abhängigen manipuliertem Schlüssel. Diese charakteristische Information kann durch die Analyse der Laufzeit des Algorithmus, den Energieverbrauch des Prozessors während der Berechnungen oder der elektromagnetischen Ausstrahlung gewonnen werden. Der kryptologische Algorithmus erhält vom Angreifer festgelegte Daten aus denen dieser sich dann den Schlüssel rekonstruieren kann.

2.2.4 Man-in-the-middle-Angriff

Beim Man-in-the-middle-Angriff (MITM-Angriff) steht der Angreifer im Netzwerk zwischen beiden Kommunikationspartnern und hat dabei vollständige Kontrolle über den Datenverkehr zwischen den Netzwerkteilnehmern und kann nach Belieben Informationen einsehen und sogar manipulieren. Der Angreifer kann den Kommunikationspartnern das jeweilige Gegenüber vortäuschen, ohne dass sie es merken.

2.2.5 Cross-Site-Request Forgery

Bei einem *Cross-Site Request Forgery* (auf Deutsch etwa Seiten-übergreifende Aufruf-Manipulation, kurz CSRF) verändert der Angreifer unberechtigt Daten in einer Webanwendung. Hierzu wird aus dem Webbrowser des Opfers, das ein berechtigter Benutzer der Webanwendung ist, ohne dessen Wissen und Einverständnis ein kompromittierter HTTP-Request an die Webanwendung abgesetzt. Der Angreifer wählt den Request so, dass bei dessen Aufruf die Webanwendung die vom Angreifer gewünschte Aktion ausführt.

Im Gegensatz zu anderen Angriffsarten auf Webanwendungen findet dieser Angriff ausschließlich im Webbrowser des Opfers statt.

Der Angreifer ist an der Interaktion mit der Webanwendung weder aktiv (wie zum Beispiel bei einem MITM-Angriff) noch passiv (wie zum Beispiel beim Belauschen der Datenübertragung) beteiligt. Darum eignet sich dieser Angriff unmittelbar auch nur zum Manipulieren von Daten in der Webanwendung, jedoch nicht zum Aus- oder Mitlesen von Daten.

2.2.6 DoS- und DDoS-Attacken

DoS- und DDoS-Attacken sind die mit am häufigsten durchgeführten Attacken. Dabei versucht der Angreifer durch möglichst große Zahl von Anfragen die Dienste des Servers zu belasten, so dass diese nicht mehr ausgeführt werden können. Daher stammt auch der Name DoS (engl. Denial of Service).

Beim DDoS (engl. Distributed Denial of Service) wird die Attacke von einem Rechnernetzwerk, beispielsweise einem Botnetz ausgeführt, um so möglichst viele Anfragen ausführen zu können. Als Schutzmaßnahmen können einfache Sperrlisten, Firewalls oder Bandbreiten- und Trafficbeschränkungen dienen. Auch können die Attacken durch ausgeklügelte Lastverteilungssysteme und Virtualisierung abgeschwächt werden.

2.2.7 Interne Angriffe

Daten in der Cloud entziehen sich der direkten Kontrolle des eigentlichen Besitzers, so dass die beschriebenen Arten von Angriffen ein ernstzunehmendes Sicherheitsrisiko darstellen, dem mit den entsprechenden Technologien begegnet werden muss. Die Benutzer müssen sich auch im Klaren darüber sein, dass Angriffe nicht nur von außerhalb stattfinden, sondern auch intern in einem Cloud-Computing-System stattfinden können.

Zu den internen Angreifern gehören neben den (temporären oder externen) Mitarbeitern, Dienstleistern, Kooperationspartner oder Praktikanten auch die Kunden des Cloud-Computing-Anbieters.

Mitarbeiter können verschiedene Motivationen haben, einen Cloud-Computing-Anbieter oder dessen Kunden zu schädigen, wie beispielsweise wegen Verärgerung, Unzufriedenheit oder Kündigung. Aber auch durch Fremdmotivation, wie zum Beispiel durch Erpressung oder Bestechung von außerhalb kann ein Mitarbeiter zum internen Angreifer werden.

Die Schädigung des Cloud-Computing-Providers durch Mitarbeiter kann durch diverse Maßnahmen herbeigeführt werden. Beispiele hierfür sind die Modifikation oder das Herunterfahren von virtuellen Maschinen, Herunterfahren von Hosts, Löschung von Daten, Dekonnektierung wichtiger Netzelemente oder die Manipulation von Konfigurationsdateien.

2.3 Schutzmaßnahmen

Zum Schutz vor passiven und aktiven Angriffen sollten regelmäßige Untersuchungen des Systems durchgeführt werden. Neben automatisierten Tests empfiehlt es sich, auch manuelle Überprüfungen der Sicherheit eines Cloud-Computing-Systems durchzuführen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert in seinen Mindestanforderungen für Cloud Computing, dass der Cloud-Anbieter sicherstellen muss, dass „*sein Personal vertrauenswürdig, geschult und auf definierte Regeln verpflichtet ist*“ [32].

Für die Erkennung von aktiven Angriffen ist ein Security Monitoring sowohl auf Anbieter- als auch auf Kundenseite durchzuführen. Dazu zählen auch regelmäßig anzufertigende Sicherheitsberichte und regelmäßige Penetrationstests. Für die Durchführung können Technologien wie Firewalls, Honeypots, IDS oder IPS eingesetzt werden.

Durch Verschlüsselung lassen sich viele Angriffe vermeiden. Beispielsweise lassen sich MITM-Angriffe durch Verschlüsselung der Datenpakete verhindern, wobei allerdings eine gegenseitige Authentifizierung stattfinden muss. Die beiden Kommunikationspartner müssen auf anderem Wege einen gemeinsamen Schlüssel ausgetauscht haben, d. h. sie müssen sich kennen. Sonst kann der Angreifer bei einer ersten SSL- oder SSH-Verbindung beiden Opfern falsche Schlüssel vortäuschen und somit auch den verschlüsselten Datenverkehr mitlesen.

In Cloud-Computing-Systemen ist eine verschlüsselte Übertragung der Daten vom Konsumenten zum Anbieter weit verbreitet und sollte für alle Daten stets verwendet werden. Bestehen die Optionen einer unverschlüsselten und einer verschlüsselten Übertragung von Informationen, so kann beispielsweise durch entsprechende Firewall-Regeln eine SSL-Verbindung über HTTPS erzwungen werden. Der verschlüsselte Kanal endet jedoch meist beim Übergang des öffentlichen in das private Netzwerk des Cloud-Anbieters. Im privaten Netzwerk des Cloud-Anbieters sind die Daten meist unverschlüsselt und

werden häufig unverschlüsselt abgespeichert. Innerhalb der privaten Netzwerke des Anbieters sind ggf. passive Angriffe möglich, so dass der Anbieter Vorkehrungen, z.B. durch Isolierung des Datenverkehrs einzelner Benutzer, treffen sollte.

Zum Schutz vor Angriffen sollte ein Cloud-Computing-Anbieter die Trennung von Funktionen und Rollen, sowie Sicherheitsrichtlinien einhalten. Die Umsetzung des Vier-Augen-Prinzips, bei dem vor jedem Zugriff noch weitere Bestätigungen erforderlich sind, die von einer zweiten Person autorisiert werden müssen, kann ebenfalls hilfreich sein [19].

Zum Schutz vor Angriffen auf die virtuellen Maschinen sollten sichere Umgebungen für virtuelle Maschinen (Hypervisoren, z.B. *Xen*) eingesetzt werden und die Netze durch den Einsatz von VPNs, VLANs und Firewalls sicher getrennt und geschützt werden. Die Trennung der Daten ist ebenfalls ein sehr wichtiger Aspekt, damit Kunden nicht auf Daten ihrer virtuellen Nachbarn zugreifen können.

2.4 Vertragliche Regelungen und Sicherheitsstandards

Sicheres Cloud Computing ist nur möglich, wenn Anwender über die Sicherheitsvorkehrungen des Dienstleisters Kenntnisse besitzen. Kunden sollten nachfragen, ob Subunternehmer beauftragt werden oder wer Zugriff auf die Daten hat. Denn wer auf Cloud Computing setzt, bleibt in der Regel selbst verantwortlich für seine Daten, denn Sicherheitsstandards beim Cloud Computing gibt es bisher kaum [9].

Ein zentraler Aspekt jedes Cloud-Vertrages ist die Sicherheit der Datenverarbeitung. Hierzu gehören Pflege- und Fehlerbeseitigungsmaßnahmen sowie Maßnahmen zur Abwehr von Angriffen und Störungen. Schon aus haftungsrechtlichen Gründen ist es von Bedeutung, dass die Verantwortlichkeit für spezifische Sicherheitsmaßnahmen eindeutig zugewiesen wird. Sicherheitszusagen können über so genannte Security-Service-Level-Agreements (SSLA), die den üblichen allgemeinen Geschäftsbedingungen nicht unähnlich sind, verabredet werden. Auch muss der Anbieter dem Kunden Einlass in die SSLAs gewähren. Tatsächlich aber bleiben die Cloud-Anbieter bei ihren Garantien für Sicherheitsmaßnahmen im wahrsten Sinne des Wortes „wolkig“ [13].

Die Anbieter unterscheiden sich stark in ihren jeweiligen Vorkehrungen. Wer sich über die Sicherheits-Standards der Anbieter von Cloud Computing kundig machen will, auf den wartet eine Menge Arbeit. Was Firmen wie Amazon oder Google über die Sicherheit ihrer Cloud-Angebote von sich aus preisgeben, ist oft dürftig. Wenn es Informationen gibt, sind diese oft zu ungenau. Angaben zu SSLAs und zum Schutz der Privatsphäre machen die Anbieter zwar meist. Allerdings sind gerade die SSLAs zum Teil zu ungenau definiert.

Weiterhin ist auch möglich, dass sich die an einer Cloud beteiligten Unternehmen verbindlichen Unternehmensregeln unterwerfen, wodurch ein angemessenes Schutzniveau vertraglich hergestellt werden soll. Dieses zunächst für internationale Konzerndatenverarbeitung entwickelte rechtliche Instrumentarium lässt sich auch auf die Cloud-Anbieter übertragen. Nach den Empfehlungen der Art.-29-Datenschutzgruppe in der EU muss im Rahmen dieser Unternehmensregeln die Hauptniederlassung oder ein von der Unternehmensgruppe benanntes Gruppenmitglied für die Verstöße aller verbundenen Unternehmen außerhalb der EU entstehen. Solche Regelungen müssen durch die zuständigen Datenschutzaufsichtsbehörden genehmigt werden. Das BSI definiert im Artikel mehrere Basisanforderungen, die an jeden Cloud-Anbieter gestellt und zusätzlich mehrere erweiterte Anforderungskriterien, die für eine hohe Vertraulichkeit und eine Verfügbarkeit von Nöten sind. [32]

Einige Sicherheits-Zertifikate sind allerdings schon weit verbreitet, wie beispielsweise der Statement on Auditing Standard 70 Type II Report und die internationale Norm für Systeme zum Informations-Sicherheits-Management, ISO/IEC 27001.

2.4.1 ISO/IEC 27001:2005

ISO/IEC 27001:2005 ist ein Teil internationaler Standards zur Informationssicherheit. Im Standard werden die Bedingungen für Herstellung, Durchführung, Betrieb, Überwachung, Überprüfung, Aufrechterhaltung und Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems (ISMS) unter Berücksichtigung der Risiken innerhalb der gesamten Organisation spezifiziert. Er dient der Auswahl geeigneter und angemessener Sicherheitskontrollen.

Der Standard ist überall dort von Bedeutung, wo der Schutz vertraulicher Daten gewährleistet sein muss, z.B. im Finanz- und Gesundheitswesen, im öffentlichen Dienst und natürlich auch beim Cloud-Computing.

Voraussetzung für die Vergabe eines ISO27001-Zertifikats ist eine Überprüfung der Geschäftsprozesse des Cloud-Unternehmens durch einen Auditor für ISO 27001-Audits. Der Auditor selbst muss mit dem Bundesamt für Sicherheit in der Informationstechnik kooperieren und von diesem ebenfalls zertifiziert sein.

Im Rahmen des Audits werden von der Institution erstellte Referenzdokumente gesichtet, eine Vor-Ort-Prüfung durchgeführt und ein Auditbericht erstellt. Das Audit wird nach einem im Standard festgelegten Prüfschema durchgeführt. Für die Vergabe eines ISO 27001-Zertifikats muss dieser Auditbericht der Zertifizierungsstelle im BSI zur Überprüfung vorgelegt werden.

Durch eine Zertifizierung erhält ein Cloud-Unternehmen mehrere Vorteile.

Das Unternehmen kann eine Einhaltung der Sicherheitsstandards gewährleisten, ohne seine gesamte Infrastruktur offenlegen zu müssen. Die Kunden des Unternehmens können sich somit sicher sein, dass das Unternehmen die Sicherheitsstandard einhält und die Daten vor Drittzugriff geschützt sind.

Das BSI schreibt ISO 27001 als Basisanforderung für jeden Cloud-Anbieter vor. So müssen die Anbieter ein wirksames ISMS oder IT-Grundschutz nach diesen Richtlinien umsetzen.

2.4.2 Statement on Auditing Standard 70 Type II Report

Der *SAS70-Type-II-Report* ist ein vom American Institute of Certified Public Accountants entwickelter Standard, der die Prüfung der Einhaltung von Sicherheitsstandards eines Cloud-Unternehmens regelt. Der Prüfungsbericht und das Zertifikat werden dabei durch unabhängige Wirtschaftsprüfer erstellt.

Das Ziel des SAS70 ist es, dem Kunden einen sachverständigen und unabhängigen Einblick in ausgewählte Prozesse und Kontrollen des Dienstleistungsunternehmens zu ermöglichen, um damit den eigenen Steuerungs- und Kontrollaufgaben nachkommen zu können. So wird vermieden, dass das Dienstleistungsunternehmen Informationen zum Geschäftsbetrieb offen legen muss, die die Grundlage des eigenen Geschäftsmodells sind. Damit die Interessen beider Seiten berücksichtigt werden, wird für einen SAS70-Report ein unabhängiger Wirtschaftsprüfer eingesetzt, dessen Beauftragung durch das Dienstleistungsunternehmen erfolgt.

Die Ergebnisse der SAS70-Reports werden nur für die Prüfer des Dienstleisters und des die Dienstleistung in Anspruch nehmenden Unternehmens erstellt. Die Nutzung der Berichte gegenüber Dritten, beispielsweise zu Marketingzwecken, unterliegt der Abstimmung zwischen Kunden und Dienstleistungsunternehmen.

Das Hauptproblem beim SAS70-Report ist jedoch, dass das Dienstleistungsunternehmen einen Großteil der zu erfüllenden Aspekte des Standards selbst festlegen kann. Dadurch wird zum einen die Sicherheitslage für einen Kunden intransparent und zum anderen die Sicherheitsrichtlinien auf ein oftmals nicht akzeptables Minimum reduziert. Für einen Kunden, der bei einem SAS70-zertifizierten Unternehmen Dienstleistungen in Anspruch nimmt, ist es somit nicht ersichtlich, in welchem Umfang seine Daten geschützt sind. Im Gegensatz zum ISO/IEC27001 ist das SAS70 somit kein Garant für eine transparente und sichere Informationspolitik des Dienstleistungsunternehmens.

3 Cloud Computing und Datenschutz

Informationelle Selbstbestimmung bezieht sich auf die Fähigkeit von Individuen, Kontrolle über die Verbreitung, die Nutzung und Offenlegung ihrer persönlichen Informationen zu haben. Dies bildet weltweit die Grundlage der modernen Rechtsprechung zum Thema Privatsphäre und Datenschutz [7].

Alle Organisationen, die persönliche Informationen sammeln und benutzen, müssen die Interessen des Einzelnen beachten. Die Organisationen können dies durch Offenheit ihrer Informationsmanagementpraxis und durch das Anbieten von Datenschutzoptionen gewährleisten. Dem steht das blinde Vertrauen der Benutzer gegenüber dem Anbieter entgegen.

Die Benutzer müssen natürlich die Vertraulichkeit ihrer Information auch selbst in die Hand nehmen, aber es gibt auch Technologien, welche die grundlegende Privatsphäre verbessern. Solche Technologien können das Risiko von Datenmissbrauch und versehentliche Offenlegung minimieren.

Unser digitaler Fingerabdruck wird Megabyte für Megabyte in Form von Profilen und Avataren zusammengestellt - virtuelle Repräsentationen von uns, die in vielen zeitgleichen Orten gespeichert sind.

Als Ergebnis der weitreichenden Entwicklung in der Informations- und Kommunikationstechnologie erschaffen, speichern und verbreiten wir Informationen bei nahezu exponentieller Wachstumsrate.

Ein Großteil der Daten lässt Rückschlüsse auf den Urheber zu. Gleichzeitig stehen diese Informationen unter Kontrolle von Dritten. Sie werden benutzt, um uns neue Dienste zur Verfügung zu stellen und uns so neue vollkommen neue Möglichkeiten und Vorteile zu eröffnen, die sich unsere Eltern und Großeltern kaum hätten erträumen lassen.

Zur gleichen Zeit ergeben sich dadurch aber auch Risiken und Gefahren dieses digitalen Überflusses.

Was wird Privatsphäre bedeuten, und wie wird sie bestehen und Erfolg haben als ein grundlegendes und einklagbares Menschenrecht, als grundlegendes Leitbild in einer Welt, in der das Individuum immer weniger direkt präsent im Zentrum der Datentransaktionen steht?

Wie werden die Benutzer Kontrolle über ihre persönlichen Daten erlernen, wenn die Daten in der Wolke gespeichert und verwaltet werden, sich also eigentlich außerhalb ihres eigenen Einflussbereichs befinden?

Weil sich Cloud Computing auch im Privatkundenbereich immer größerer Beliebtheit erfreut, ist es daher auch nötig, die Rahmenbedingungen des Datenschutzes abzuleiten und zu benennen und so ein Leitbild zu definieren.

3.1 Rechtsfragen

Das zentrale Problem des Cloud Computing ist die Gewährleistung der Integrität und Vertraulichkeit der Datenverarbeitung des Cloud-Nutzers. Dies gilt nicht nur für die Verarbeitung personenbezogener, sondern sämtlicher Daten, bei denen es auf Vertraulichkeit und Integrität ankommt. Dazu zählen sowohl Betriebs- und Geschäftsgeheimnisse, als auch Forschungsdaten und anderweitige immateriell-rechtlich geschützte Daten. Letztendlich geht um das Verhindern unberechtigter und schädigender Zugriffe Dritter.

Die meisten existierenden Gesetze haben ihre Ursprünge in den Richtlinien der OECD (Organisation für ökonomische Zusammenarbeit und Entwicklung). Diese fordern beispielsweise, dass bereits existierende und personenbezogene Daten für einen bestimmten Zweck gesammelt werden sollten und dass diese Datensammlung geschützt werden muss [12].

Rechtlich erfolgt die Bereitstellung und Nutzung von Clouds im Rahmen eines Schuldvertrags, aus dem sich viele juristischen Fragestellungen (z.B. Haftung, Gewährleistungsansprüche, Urheberrecht)

ergeben können. Diese juristische Problematik genauer zu analysieren, würde allerdings den Rahmen dieser Übersicht sprengen. Cloud-Verträge lassen sich rechtlich nicht eindeutig zuordnen, sondern sind eine Mischung aus Mietvertrag, einer Leihe und eines Dienst- und/oder eines Werkvertrages (Schulung, Pflege, Schnittstellenanpassung) [3].

Die Archivierung von Daten in grenzüberschreitenden Clouds ist bezüglich steuerlich relevanter Dokumente von Bedeutung, denn diese sind grundsätzlich im Inland zu führen und aufzubewahren². Auf Antrag kann die zuständige Finanzbehörde bewilligen³, dass die Dokumente in einem EU-Mitgliedstaat archiviert werden. Die ausländische Finanzbehörde muss zustimmen, und die deutsche Finanzbehörde muss auf die Dokumente zugreifen können. Nach § 148 AO dürfen steuerrechtliche Unterlagen außerhalb des EU-Raumes nach Bewilligung der Finanzbehörde nur aufbewahrt werden, wenn durch die Aufbewahrung im Inland für den Steuerpflichtigen Nachteile und Härten entstehen und die Besteuerung nicht beeinträchtigt wird. Nach dem Handelsrecht müssen Buchungsbelege und Handelsbriefe im Inland aufbewahrt werden. Es besteht eine gesetzliche Aufbewahrungsfrist von 6 bzw. 10 Jahren.⁴

Außerdem richten sich einige Cloud-Angebote direkt an die Verbraucherinnen und Verbraucher (z.B. Google Apps), so dass das nationale und das internationale Verbraucherrecht zu beachten ist. Für die Ermittlung von Straftaten und Ordnungswidrigkeiten stellt die Speicherung von Daten in der Cloud dann ein Problem dar, wenn durch die Art und den Ort der Datenverarbeitung ein Zugriff für die Ermittlungs- und Sanktionsbehörden nicht möglich ist.

Wegen der Vielzahl der mit Cloud-Datenverarbeitungen verbundenen rechtlichen Fragen, die bisher keiner gesetzlichen Regelung zugeführt worden sind, kommt einem Gesetzesentwurf eine zentrale Bedeutung zu.

3.1.1 Vereinbarkeit mit dem Datenschutzgesetz

Aus Datenschutzsicht ist Cloud Computing nur relevant, wenn personenbezogene Daten verarbeitet und die verarbeiteten Einzeldaten einem Menschen, dem Betroffenen, zugeordnet werden können. Betroffene können zum einen Mitarbeiter des verantwortlichen Unternehmens sein, die bei der Cloud-Nutzung beschäftigt werden und deren Daten in diesem Zusammenhang verarbeitet werden. Regelmäßig verarbeitet werden zudem personenbezogene Daten als Gegenstand der Cloud-Dienste, z.B. die Angaben zu Kundinnen und Kunden, zu Lieferanten und sonstigen Geschäftspartnern oder von Personen, die mit dem Cloud-Nutzer in keinem spezifischen Verhältnis stehen.

Keine Anwendbarkeit des Datenschutzrechtes ist bei hinreichender Anonymisierung personenbezogener Daten gegeben. Als anonymisiert angesehene Daten⁵ können durch ihre Verarbeitung in der Cloud reidentifizierbar werden, wenn andere Cloud-Nutzer oder die Cloud- bzw. Ressourcen-Anbieter über Zusatzwissen verfügen, durch das eine Reidentifizierung ermöglicht wird.

Durch Pseudonymisierung, also das Ersetzen der Identifikationsmerkmale einer natürlichen Person durch ein anderes Merkmal⁶, wird die Anwendbarkeit des Datenschutzrechtes nicht ausgeschlossen. Jedoch kann durch diese Methode eine Identifizierung der Betroffenen derart erschwert werden, dass ein Schutzniveau erreicht wird, das eine Datenverarbeitung zulässig macht.

Soweit kein objektiver, sondern ein relativer Begriff der Personenbeziehbarkeit vertreten wird, kann sich also die Qualität der Datenverarbeitung durch Cloud-Anwendungen ändern. Da es aber heute keines unverhältnismäßig großen Aufwandes an Zeit, Kosten und Arbeitskraft mehr bedarf, um durch

² Nach § 146 Abs. 2 HGB

³ nach dem 01.01.2009 eingefügten § 146 Abs. 2a AO

⁴ nach § 257 Abs. 4 HGB

⁵ vgl. § 3 Abs. 6 BDSG

⁶ § 3 Abs. 6a BDSG

komplexe Verknüpfungen in Netzen nicht eindeutig identifizierende Daten einer bestimmbar Person zuzuordnen, ändert allein der Umstand einer Verarbeitung in einer Cloud an der Anwendbarkeit des Datenschutzrechtes nichts. Eine Personenbeziehbarkeit ist bei Einzeldatensätzen zu Personen regelmäßig anzunehmen. Gerade die elektronische Auswertbarkeit und die Integration in ein möglicherweise weltweites Netzwerk erhöht die Wahrscheinlichkeit des Vorliegens von Zusatzwissen, das eine Identifizierung der Betroffenen ermöglicht.

Clouds sind tendenziell grenzüberschreitend. Daraus ergibt sich ein weiteres Problem bei der Vereinbarkeit mit dem Datenschutzrecht ist, weil es keine technischen Gründe zur Berücksichtigung territorialer Grenzen gibt. Dies gilt jedoch nicht für das Datenschutzrecht, denn dieses ist immer an den Ort der Datenverarbeitung gebunden.

Mit der Europäischen Datenschutzrichtlinie (EU-DSRL) gibt es innerhalb des europäischen Binnenmarktes erstmals eine gesetzliche Grundlage für eine grenzüberschreitende Datenverarbeitung. Durch die Überschreitung der nationalen Grenzen soll es nicht zu einer Einschränkung der Rechte der Betroffenen und der Minimierung der Schutzstandards kommen. Beim grenzüberschreitenden Cloud-Computing ist allerdings trotzdem nicht gewährleistet, dass in den von der konkreten Anwendung betroffenen Staaten überhaupt Regelungen zum Datenschutz und zum Datenschutz bestehen. Das Datenschutzzentrum Schleswig-Holstein [12] schreibt dazu:

Gemäß Artikel 4 Abs. 1 a), b) EU-DSRL kommt es für die Anwendbarkeit einzelstaatlichen Rechts darauf an, in welchem Mitgliedstaat die Daten verarbeitende Niederlassung ihren Sitz hat. Hat die Daten verarbeitende Stelle keine Niederlassung im EU/EWR-Raum, so kann nach § 1 Abs. 5 S. 3 BDSG ein im Inland ansässiger Vertreter benannt werden, dem gegenüber das anwendbare nationale Datenschutzrecht geltend gemacht werden kann.

In einer Cloud droht die Verantwortung für die konkrete Verarbeitung und für eventuelle Persönlichkeitsverletzungen hinter den grenzüberschreitenden Wolken verloren zu gehen. Für die datenschutzrechtliche Bewertung von Cloud-Anwendungen ist daher eine präzise Klärung der Verantwortlichkeiten von zentraler Bedeutung. Verantwortlich ist, wer „über die Zwecke und Mittel der Verarbeitung entscheidet“.⁷ Dies ist beim Cloud Computing der Cloud-Nutzer, der sich zur Nutzung entschließt und die Daten in die Cloud eingibt. Allerdings gibt es seitens des Cloud-Anbieters keine einheitlichen Verträge und keine verbindlichen Standards, so dass jeder Anbieter unterschiedliche Verträge und Garantien definieren kann und der Cloud-Nutzer so einer Flut an Bedingungen und Vertragsklauseln gegenüber steht. Wie schon zuvor erwähnt, müssen deshalb solche Cloud-Verträge und Sicherheitsstandards vereinheitlicht werden.

Die Verantwortung wird nicht auf den eigenen tatsächlichen Machtbereich beschränkt, sondern auch auf die Auftragsdatenverarbeitung erstreckt.⁸ In § 11 Absatz 1 S. 1 BDSG wird bekräftigt, dass bei der Auftragsdatenverarbeitung der Auftraggeber für die Einhaltung der Vorschriften über den Datenschutz verantwortlich ist. Dies bedeutet: Durch die Beauftragung und Einschaltung Dritter kann sich ein Cloud-Dienstleister seiner Verantwortung nicht entziehen.

Bei einer Begehung von Datenschutzverstößen in der Cloud außerhalb des deutschen Territoriums werden die gesetzlichen und faktischen Ermittlungsmöglichkeiten nach deutschem Recht regelmäßig fehlen. Rechtlich ist die Datenschutzkontrolle der Aufsichtsbehörden in den Bundesländern auf das jeweilige Landesterritorium beschränkt. Innerhalb der EU bzw. dem EWR kann eine gegenseitige Amtshilfe der Aufsichtsbehörden erfolgen, die bisher allerdings wegen des damit verbundenen bürokratischen Aufwandes nur im Einzelfall auch tatsächlich durchgeführt wird. Unbegründete Kontrollen, wie sie sowohl im BDSG als auch in den EU-Datenschutzrichtlinien vorgesehen sind, sind als koordinierte oder gemeinsame Kontrollen in Clouds mit Drittlandsbezug praktisch nicht möglich.

⁷ nach Art. 2 c) S. 1 EU-DSRL

⁸ nach § 3 Absatz 7 BDSG

Dies führt dazu, dass Cloud-Anbieter, die sich Datenschutzkontrollen entziehen wollen, gezielt Clouds nutzen können. Dies gilt insbesondere für Verarbeitungen außerhalb der EU, da hier jede Kontrolle von der vertraglichen Einräumung von Kontrollrechten durch die Cloud- und Ressourcenanbieter abhängt, die vom Cloud-Nutzer durchgesetzt werden müsste, der in der Regel selbst kein Interesse an der Datenschutzkontrolle hat.

3.1.2 Drittzugriff

Durch die Verlagerung des Ortes der Datenverarbeitung in einen anderen Staat ergibt sich, dass Dritte, die keine Cloud-Anbieter sind, in diesem Staat möglicherweise tatsächlich und möglicherweise auch auf rechtlicher Basis Zugriff auf diese Daten nehmen. Dies gilt vorrangig für die Behörden der inneren Sicherheit, also Polizei, sonstige Strafverfolgungsbehörden, nationale Geheimdienste oder Finanzbehörden. So gehört es beispielsweise zu den rechtlichen Aufgaben und Befugnissen vieler nationaler Geheimdienste, für die heimischen Interessen Wirtschaftsspionage zu betreiben. Dies kann in keinem Fall im Interesse des Cloud-Nutzers sein und sollte auch nicht in dem der Cloud-Anbieter liegen, lässt sich aber rechtlich nicht und faktisch nur schwer verhindern.

Neben den klassischen Sicherheitsbehörden sind Finanzbehörden an Cloud-Daten interessiert, mit denen sie z.B. über den Zugriff auf Bankdaten Erkenntnisse zur Steuerhinterziehung und zum Steuerbetrug zu erlangen versuchen. Die Cloud kann eine weitere Informationsquelle beispielsweise für Aufenthalts-, Asyl- und Einwanderungsbehörden sein, bei denen Erkenntnisse aus dem Heimatstaat von hoher Relevanz sind.

Es ist nicht auszuschließen, dass das nationale Recht, etwa wegen eines völligen Fehlens von Datenschutzrestriktionen, sogar den Zugriff durch private Dritte erlaubt. Je niedriger das Datenschutzniveau in dem Staat ist, in dem die tatsächliche Datenverarbeitung stattfindet, desto größer ist die Gefährdung der Betroffeneninteressen durch die Cloud-Datenverarbeitung.

Besonders problematisch wird es beim tatsächlichen und dem rechtlich erlaubten Zugriff, wenn eine Datenverarbeitung in einem Staat erfolgt, in dem Datenschutz rechtlich keine Bedeutung hat, sondern in dem zusätzlich bewusst und gezielt Menschenrechte ignoriert und in denen Menschen politisch, wirtschaftlich, ethnisch oder aus anderen Gründen verfolgt werden. So können staatliche Zugriffe auf Cloud-Rechner durch staatliche oder halbstaatliche Einrichtungen in Diktaturen wie z.B. dem Iran oder China Informationen offenbaren, die zur Grundlage von weiterer Überwachung, Verfolgung, Verhaftung, bis hin zur Tötung benutzt werden können.

Der legale Zugriff auf Cloud-Daten kann unter Umständen durch technische Vorkehrungen wie Pseudonymisierung, Verschlüsselung oder durch sichere Virtualisierung verhindert werden. Das BSI fordert, dass die Cloud-Anbieter offen legen müssen, an welchen Standorten die Daten und Anwendungen gespeichert werden und wie der Zugriff durch Dritte geregelt ist [32]. Allerdings stellt dies lediglich eine Forderung und noch keine gesetzliche Regelung dar.

Außerdem muss man berücksichtigen, dass in vielen Staaten rechtliche Regelungen existieren, mit denen die Cloud-Anbieter unter Androhung staatlicher Sanktionen verpflichtet werden können, Schutzvorkehrungen gegen unberechtigten Zugriff entweder völlig zu unterlassen oder auf behördliche Aufforderung aufzuheben. So gibt es insbesondere im Sicherheitsbereich in fast allen Staaten behördliche Befugnisse, technische Sicherungsvorkehrungen zu überwinden.

Je nach den vorgesehenen und umgesetzten Sicherungsvorkehrungen besteht zudem ein Angriffsrisiko durch unberechtigte Dritte auf die von Cloud-Nutzern verarbeiteten Daten. Soll der Cloud-Anbieter alle Sicherungsvorkehrungen und -bestimmungen selbst treffen, so verliert er beim Cloud Computing regelmäßig völlig die Herrschaft über sie. Und das, obwohl Datensicherheit fast immer ein Bestandteil des Serviceangebots ist. Denkbar sind Beeinträchtigungen sämtlicher Schutzziele technisch-organisatorischer Datensicherheitsmaßnahmen, also der Integrität, Verfügbarkeit, Vertraulichkeit, der Transparenz für die Berechtigten oder der Unverknüpfbarkeit der verarbeiteten Daten.

Unberechtigte Zugriffe können durch technisch-organisatorische Maßnahmen, wie sie in im Bundesdatenschutzgesetz obligatorisch vorgesehen sind, eingeschränkt oder gar vermieden werden. Zu beachten ist aber, dass die gesetzliche Verpflichtung zu derartigen Vorkehrungen nur bei Cloud-Anbietern im EU-Raum besteht. Dessen ungeachtet bestehen auch hier oft große Umsetzungsdefizite [12]. Während jedoch gegen legale Zugriffsrechte auf Cloud-Daten keine vertraglichen Absprachen zwischen Nutzer und Cloud-Anbieter helfen, können gegen ungesetzliche Zugriffe vertraglich umfassende und wirksame Sicherungsmaßnahmen verabredet werden.

3.1.3 Vertragliche Regelungen zwischen Nutzer und Anbieter

Cloud Computing ist aus technischer Sicht klassische Auftragsdatenverarbeitung.⁹ Der Auftraggeber, also der Cloud-Nutzer, soll vollständig über die Art und Weise der Datenverarbeitung bestimmen. Die Cloud-Anbieter erfüllen reine Hilfs- und Unterstützungsfunktionen und sind völlig von den Vorgaben der verantwortlichen Stelle abhängig. Der Auftraggeber bleibt für die Sicherstellung der Vertraulichkeit und Integrität der Daten verantwortlich. Dieser Verantwortung kann er auf der Basis der etablierten Cloud-Strukturen im Allgemeinen nicht gerecht werden, bei denen Dienste angeboten werden, zu denen die Dienstleister gegenüber dem Cloud-Nutzer keine Auskunft zur Art und zum Ort der Verarbeitung und zu den Sicherungsmaßnahmen geben können. Dem gegenüber ist eine datenschutzgerechte Datenverarbeitung in der Cloud vorstellbar, wenn dem Cloud-Nutzer als verantwortliche Stelle umfassende Transparenz über diese Rahmenbedingungen und Wahlmöglichkeiten gewährt werden.

Die Anforderungen an eine Funktionsübertragung sind weitergehend. Die Datenschutzgesetze gehen davon aus, dass der Übermittlungsempfänger von Daten selbst für die weitere Verarbeitung verantwortlich ist. Dies können aber beim Cloud Computing die Cloud-Anbieter nicht gewährleisten, da diese von der konkreten Datenverarbeitung im Idealfall nichts bewusst mitbekommen und mitbekommen sollen. Die rechtlichen Mindestanforderungen für jede Cloud-Anwendung ist die Beachtung der Regelungen zur Auftragsdatenverarbeitung. Dies gilt selbst im Fall einer Funktionsübertragung, da durch den Umstand, dass eine Verarbeitung außerhalb der EU erfolgt, das Datenschutzniveau für die Betroffenen nicht abgesenkt werden darf.

Im Auftrag müssen die Voraussetzungen und Verfahren bei unerwarteten bzw. unzulässigen Verarbeitungen festgelegt werden, das heißt bei welchen Vorfällen eine Information des Nutzers unaufgefordert erfolgen muss. Wegen des standardisierten Vorgehens ist bei Cloud-Anwendungen das Erteilen von Weisungen des Nutzers meist nicht umsetzbar. Dies muss kompensiert werden durch Optionsangebote, die dem Nutzer die Auswahl bestimmter Ressourcen, Orte und Sicherheitsniveaus erlaubt. Dies ist in jedem Fall nötig, wenn an die konkrete Verarbeitung zusätzliche rechtliche Anforderungen gestellt werden, so wie dies z.B. bei besonderen Datenkategorien nach¹⁰, bei Daten von Finanzdienstleistern¹¹, bei Sozialgeheimnissen¹² oder bei besonderen Berufs- und Dienstgeheimnissen der Fall ist. Bei der Verarbeitung von sensitiven Daten können diesen Kennungen beigefügt werden.

Regelungsbedürftig ist die Haftung der Cloud- und Ressourcen-Anbieter gegenüber den Nutzern. Durch die Verarbeitung in der Cloud können sowohl direkt Schäden für den Nutzer entstehen wie auch persönlichkeitsrechtliche Schäden der von der Datenverarbeitung Betroffenen, die diese gegenüber dem Nutzer geltend machen können¹³. Die Haftungsregelung des Cloud-Vertrages sollte sicherstellen, dass alle vom Nutzer nicht zu vertretende Schäden vom Cloud-Anbieter übernommen werden.

⁹ Siehe § 11 BDSG

¹⁰ § 3 Abs. 9 BDSG

¹¹ § 25a KWG

¹² § 80 SGB X

¹³ nach § 7 BDSG oder nach den §§ 823, 847 BGB

Bei einer längerfristigen Cloud-Verarbeitung muss geklärt werden, was mit den gespeicherten Daten passiert, wenn ein Cloud-Anbieter insolvent wird oder von einem anderen Unternehmen übernommen wird. Nach Abschluss der Verarbeitung müssen die verarbeiteten Daten gelöscht werden. Es bedarf noch einer weitergehenden Untersuchung, welche Protokolldaten für welche Zeit aufbewahrt werden müssen und dürfen.

Nicht zuletzt muss im Vertrag gewährleistet werden, dass im Fall einer Datenschutzkontrolle nach § 38 BDSG diese ungehindert durchgeführt werden kann. Im Fall einer Wahrnehmung der Rechte des Nutzers müssen diese uneingeschränkt in Anspruch genommen werden können.

3.1.4 Außereuropäische Clouds

Werden Rechnerstandorte außerhalb der Europäischen Union mit einbezogen, so sind Clouds wegen der damit zwangsläufig erfolgenden Datenübermittlung, für die es keine datenschutzgesetzliche Legitimation gibt, grundsätzlich unzulässig. Dies hat dazu geführt, dass einzelne Cloud-Anbieter wie z.B. Amazon Web Services den Nutzern die Möglichkeit einräumen, eine Datenverarbeitung ausschließlich innerhalb des EU-Raumes durchführen zu lassen.

Ein weitgehend freier Datenverkehr in Nicht-EU-Ländern ist aber eventuell möglich, wenn in den Drittstaaten ein angemessenes, durch die EU-Kommission festgestelltes Datenschutzniveau besteht. Dies ist z.B. bei der Schweiz, Kanada oder Argentinien der Fall. Die Feststellung der Angemessenheit des Datenschutzniveaus in einem außereuropäischen Staat hat jedoch nicht zur Folge, dass Stellen dort rechtlich als Auftragnehmer gemäß § 11 BDSG behandelt werden können.

Die Selbstzertifizierung von US-Unternehmen als „*Safe Harbor*“ genügt nicht den EU-Datenschutzstandards. Zielsetzung des Safe Harbors war es, eine praktikable Lösung für die zwangsläufig zwischen den USA und Europa notwendigen Datenübermittlungen zu schaffen. Keinesfalls kann aber Safe Harbor dazu dienen, die strengeren Datenschutzvorschriften in Europa zu umgehen, so wie dies beim Cloud Computing der Fall wäre.

Diese Maßstäbe dienen lediglich der Schaffung einer tragfähigen Brücke zwischen den strengen europäischen Datenschutzregeln und dem in vielerlei Hinsicht nicht existierenden Datenschutzniveau in den USA. Cloud-Verträge, die sich an „Safe-Harbor“-Maßstäben orientieren, sind daher nicht ausreichend.

US-amerikanische Cloud-Anbieter wie z.B. Google oder Amazon weisen sich häufig mit dem SAS-70-Type-II-Zertifikat aus, dessen Zertifizierung wie zuvor erwähnt durch unabhängige Dritte erfolgen soll. Diese Maßnahme genügt nur teilweise den Anforderungen der Auftragsdatenverarbeitung. Sie berücksichtigt z.B. nicht die materiellen und prozeduralen Betroffeneninteressen bei Übermittlungen.

3.2 Digitale Identitätsverwaltung

In der ersten Phase des Verbraucher-Computings war die Privatsphäre und Sicherheit des Benutzers durch die Beschränkung des physikalischen Zugriffs zu den Stand-alone-Rechnern und Speichermedien gegeben. Die Anforderung für die Benutzeridentität waren sehr minimal, sie bestanden nur aus einer Handvoll von Benutzernamen und Passwörtern für lokale Systeme und Dateizugriff.

In der zweiten Phase müssen die Benutzer sich für jede Internetanwendung, die sie verwenden, neu identifizieren. Meist geschieht dies durch das Ausfüllen von Online-Formularen und durch Angabe persönlicher Informationen (z.B. Name, Anschrift, Kreditkartennummer etc.). Dadurch wird eine Spur persönlicher Informationen hinterlassen, die durch nicht ausreichenden Schutz eventuell ausgenutzt und missbraucht werden könnte.

Im jetzigen, sukzessiven Übergang zur dritten Phase müssen sich die Benutzer nicht mehr für jede Internetanwendung registrieren, sondern sollen durch digitale Identitätsverwaltung so einfach wie möglich auf Cloud-Dienste zugreifen und diese nutzen können.

Trotzdem soll die digitale Identität jedes Nutzers gewahrt bleiben und es darf nicht zu Identitätsfälschung oder -missbrauch kommen. Die Benutzer verwenden einen oder mehrere Authentifikationsdienste und haben so mehr Kontrolle darüber, wer über ihre persönlichen Daten verfügt und wie zu benutzen sind.

Identitätsverwaltung ist grundlegender Bestandteil der Zugangskontrolle in Cloud-Computing-Systemen und muss von jeder Cloud-Plattform unterstützt werden. Das Rechtemanagement muss gewährleisten, dass jede Rolle nur die Daten (auch Metadaten) sehen darf, die für die Nutzung eines Cloud-Dienstes notwendig sind [32].

3.2.1 Heutige Situation

Fast alle Online-Aktivitäten setzen voraus, dass Informationen über die Benutzeridentität ausgetauscht werden. Heutzutage müssen die meisten Benutzer eine Identität einrichten, wenn sie eine neue Webapplikation benutzen wollen. Dies geschieht durch Ausfüllen eines Online-Formulars, in das meist sensible Daten eingegeben werden müssen (Name, Adresse, Kreditkartennummer, Telefonnummer etc.) [7].

So hat ein typischer Internetbenutzer irgendeinen Teil seiner persönlichen Informationen bei vielen verschiedenen Webseiten angegeben. Wenn man Cookies und IP-Adressen als persönliche Informationen dazurechnet, dann hinterlassen die Internetbenutzer persönliche Daten aller von ihnen genutzten Webseiten. Sie hinterlassen „digitale Brotkrümel“ im Cyberspace und sind sich meist nicht im Klaren darüber, wie diese Daten verwendet werden könnten und ob diese geschützt sind. Außerdem liegt der Fokus von vielen neuen Applikationen auf der Beteiligung und der Generierung von Inhalten von Benutzern. Auch dadurch hinterlässt ein Benutzer indirekt eine Identität.

Die Gemeinsamkeit solcher Szenarien besteht darin, dass Cloud-Anbieter mit Nutzern umgehen müssen, die nicht körperlich identifiziert sind, jedoch durch ihre Reputation und anderen Attributen, die ihnen durch Dritte attestiert werden, repräsentiert sind.

Die sich entwickelnde Infrastruktur für die Identitätenverwaltung muss solche gemeinschaftlichen Umgebungen unterstützen. Dadurch werden dezentralisierte und verbündete Vertrauensmodelle möglich, die auf einer begrenzten Anzahl an Identitätsinformationen basieren.

3.2.2 Identitätsdiebstahl und -missbrauch

Identitätsdiebstahl und -missbrauch sind die Krankheiten des Informationszeitalters, zusammen mit neuen Formen von Diskriminierung wie „Cybermobbing“, die durch die nahezu unbegrenzte Verfügbarkeit an Informationen ermöglicht werden. Persönliche Informationen, seien sie biographisch, biologisch, genealogisch, historisch, transaktional oder ortsspezifisch, machen unsere moderne Identität aus. Mit ihnen muss verantwortungsbewusst umgegangen werden. Wenn dies nicht geschieht, ist die Zuversicht in die sich entwickelnde Informationsgesellschaft beschädigt.

Digitales Identitätenmanagement soll solche Probleme wie das Anlegen von Fake-Accounts weitestgehend verhindern. Allerdings kommt es ja auch in der realen Welt durchaus vor, dass sich Personen durch gefälschte Ausweise illegalen Zugang verschaffen. Durch Pseudonymisierung und Anonymität im Internet ist bedeutend schwieriger, herauszufinden, ob eine Person über die entsprechende Zugangsberechtigung verfügt.

Identitätsdiebstahl geht noch einen Schritt weiter als das bloße Anlegen von Fake-Accounts oder gefälschten Ausweisen. Hier werden keine erfundenen Pseudonyme, sondern Namen real existierender Personen verwendet, die von der Verwendung durch Daten meist keine Kenntnis haben. Insbesondere

durch soziale Netzwerke, wie zum Beispiel Facebook oder StudiVZ ist das Anmelden unter dem Namen von Kollegen oder Kommilitonen zu einer problematischen Angelegenheit für die betroffenen Personen geworden. Da meist auch Fotos der Opfer verfügbar sind, können realistische Profile erstellt werden, mit Hilfe derer nun Falschinformationen an Dritte weitergetragen werden können oder aber Informationen von Dritten in gutem Glauben erfragt werden können.

Es mag sein, dass sich unsere grundlegenden Ideen über Identität und Privatsphäre ändern und unsere gemeinschaftlich verfolgten Strategien und die eingesetzten Technologien im Zuge der zunehmenden Vernetzung der Welt anpassen.

Jedoch wird die Cloud flexiblere, benutzerfreundlichere der Benutzerauthentifizierung unterstützen müssen. Ohne besseres Management digitaler Identitäten werden wir nicht nur mit existierenden Problemen wie Identitätsdiebstahl, Spam, Malware, Betrug zu kämpfen haben, wir werden nicht einmal in der Lage sein, einzelnen Benutzern die Migration von ihrem Desktop ins Web sicher zu gewährleisten.

3.2.3 Anforderungen an zukünftige Systeme

Es wird ein flexibles und benutzerorientiertes Identitätsmanagement benötigt. Zum einen flexibel, weil mehrere Identitätsmechanismen und -protokolle unterstützt werden müssen. Hinzu kommen die verschiedenen benutzten Arten von Plattformen, Applikationen und Service-orientierte architekturelle Entwurfsmuster zu Tage.

Zum anderen benutzerorientiert, weil die Benutzer das Zentrum des Identitätenmanagement darstellen. Die Benutzer müssen ermächtigt werden, effektive Kontrollmechanismen auf ihre persönlichen Information anzuwenden. Die Hauptanforderungen für solche Identitätenmanagementsysteme sind folgende [7]:

- sind geräteunabhängig,
- ermöglichen Eine einmalige Anmeldung für tausende von verschiedenen Onlinediensten,
- unterstützen Pseudonyme und mehrere gültigen Identitäten zum Schutz der Privatsphäre,
- sind untereinander kompatibel,
- basieren auf offenen Standards,
- stehen unter OpenSource-Software-Lizenzen
- sind transparent und erweiterbar.

In Zukunft werden die Benutzer ihre persönlichen Informationen nicht jedes Mal von neuem eintragen müssen, wenn sie eine Website besuchen.

Die Benutzeridentität wird auf verschiedene Cloud-Dienste übertragbar sein. Wenn sich ein Benutzer einen guten Ruf erarbeitet, beispielsweise bei einem Onlineauktionshaus, wird er in der Lage sein, diesen Vorteil auch auf anderen Cloud-Angeboten nutzen zu können. Ein Ergebnis davon wäre die größere Auswahl an Onlinediensten, weil die Nutzer nicht mehr an einen Dienst oder Händler gebunden sind. Wie das Problem zu lösen ist, dass reale Personen ihre Nutzerkonten untereinander austauschen können, ist noch ungeklärt.

Ein vollflexibles Identitätenmanagement wäre nicht nur auf Laptops und Desktopcomputer beschränkt, es würde auch auf Handys, PDAs, Spielekonsolen oder eingebetteten Systemen funktionieren. Dieser Ansatz einer digitalen Identität würde das volle Potential der Cloud freisetzen. Es würde es den Benutzern erlauben, eine große Bandbreite an Onlinediensten gleichzeitig zu benutzen und zu kombinieren.

Cloud Computing mit digitalem Identitätenmanagement setzt eine Reihe von Technologien voraus:

- Open Source und proprietäre Software zur Identitätenverwaltung, die auf offenen Standards basiert, die leicht in alle verfügbaren Online-Dienste und Geräte einbezogen werden können (ähnlich wie die OpenSource-Software, die heute den Kern des Internets darstellt).
- Verbündete Identität: Wenn ein Benutzer bei einem Dienst oder einer Institution seine Identität einmal hinterlassen hat, können sie diese Bescheinigungen auch problemlos woanders einsetzen. Dadurch wird auch keine separate Anmeldung für jeden Online-Dienst mehr erforderlich.
- Mehrfache oder unvollständige Identitäten sollten möglich sein, damit Benutzer auf Online-Services zugreifen und mit anderen zusammenarbeiten können ohne ihren wahren Namen oder wahre Identität jedem preisgeben zu müssen.
- Verschiedene Pseudonyme sollen unterschiedliche Stufen von Identifikation und Authentifizierungsstärken unterstützen.
- Datenzentrierte Bestimmungen, die erzeugt werden, sobald ein Benutzer persönliche Informationen oder sensible Daten zur Verfügung stellt, und mit der ein Zertifikat verbunden ist, solange diese Informationen existiert. So wird sichergestellt, dass die Informationen mit den gegebenen Bestimmungen im Einklang stehen.
- Prüfwerkzeuge, die einfach ermitteln können, wie die Daten gespeichert, geschützt und benutzt und ob die Bestimmungen eingehalten wurden.

Wenn diese Identitätsdaten in die Hände von Dritten gelangen, besteht allerdings das Problem, dass diese dadurch unter falschem Namen illegalen Zugriff auf jeden beliebigen Cloud-Dienst haben.

Um das Problem zu minimieren, wäre ein möglicher Lösungsansatz, die Identifikationsdaten so zu verschlüsseln, in so kleine Teile wie möglich zu splitten und auf so vielen Servern wie möglich zu verteilen, so dass dadurch die Gefahr einer Identifikation minimiert wird.

Bildlich gesprochen wäre dies in etwa so, als wären die Daten in Papierform durch einen Reißwolf in kleine Schnipsel zerteilt und an verschiedenen Orten hinterlassen worden. Bei jedem Zugriff muss jeder Schnipsel gefunden und auch wieder zu einem Blatt Papier zusammengesetzt werden, was in der virtuellen Welt natürlich ressourcensparender abläuft als in der Realität. Trotzdem werden für die Verschlüsselung und das Splitten der Dateien natürlich mehr Rechenkapazitäten benötigt. Um Identitätsdiebstahl zu begehen, muss man im Besitz aller Teile der Identitätsdaten sein, denn das Ganze ist hier mehr als die Summe seiner Teile.

3.2.4 Protokolle

Mit der erhöhten Nutzung des Internets für die Geschäftsabwicklung und dem Aufkommen von neuen Online-Interaktionen wie sozialen Netzwerken oder User-generated Content sind für die Aufrechterhaltung des offenen Webs innovative Technologien gefragt, die solche digitalen Fingerabdrücke realisieren. Online-Nutzer müssen ihre vielen Nutzerkonten und Passwörter sicher verwalten, zugleich jedoch ohne die Gefahr überwacht oder ausgespäht zu werden.

Authentifikationsprotokolle sollen in der Cloud einen Single-Sign-On erlauben. Das bedeutet, dass ein Benutzer sich nach einer einmaligen Authentifizierung auf alle Dienste zugreifen und sich nicht für jeden Dienst separat anmelden muss.

Dadurch wird für den Benutzer Zeit gespart und es entsteht ein Sicherheitsgewinn, da das Passwort nur einmal übertragen und nur ein Benutzerkonto betrachtet werden muss. Hat ein Angreifer jedoch von einem Benutzer einmal das Passwort für den Single-Sign-On geknackt, so stehen ihm sofort alle Systeme, auf die dieser Benutzer Zugriff hat, zur Verfügung.

Als Beispiele für offene Identitätsverwaltungssysteme werden im Folgenden die Protokolle OpenID und OAuth näher beschrieben.

OpenID

OpenID ist ein Authentifizierungssystem für Webseiten und andere webbasierte Cloud-Dienste. Das zugrundeliegende Protokoll wurde 2005 entwickelt. OpenID erlaubt es einem Benutzer, der sich bei seinem sogenannten OpenID-Provider einmal mit Benutzername und Kennwort angemeldet hat, sich nur mit Hilfe der sogenannten OpenID (einer URL) ohne Benutzername und Passwort bei allen das System unterstützenden Webseiten und -diensten anzumelden. Heute unterstützen bereits mehr als 10.000 Websites einen solchen OpenID-Login und eine geschätzte Zahl von 350 Millionen OpenID-fähigen URLs existieren zur Zeit.

OpenID wurde von einer Open Community entwickelt. Es ist eine freie benutzerorientierte Technologie zur Umsetzung digitaler Identitäten.

OpenID ist dezentral angelegt und setzt auf ein URL-basiertes Identitätskonzept. Hierbei werden einzelne Personen über eine HTTP-URL identifiziert, die beispielsweise auf ein Profil einer Online-Community oder einem privaten Blog verweist. Zur Identifikation werden heutzutage normalerweise E-Mail-Adressen verwendet, deren Nachteil jedoch darin besteht, dass sich Benutzerinformationen nicht in Echtzeit abrufen lassen.

Für die Anmeldung mit OpenID wird eine OpenID-Identität benötigt, die durch einen OpenID-Provider bereitgestellt wird. Wegen der dezentralen Architektur von OpenID gibt es viele verschiedene OpenID-Provider, denn im Prinzip kann jeder OpenID-Provider werden und einen OpenID-Server betreiben. Webseiten, die OpenID unterstützen, müssen keinen klassischen Login mehr bereitstellen. Dadurch müssen keine Funktionen wie "Passwort vergessen" implementiert werden und aufgrund der nicht mehr zu speichernden Logininformationen entfällt der hierfür notwendige Sicherheitsaufwand auf Seiten des Websitebetreibers.

Für Online-Geschäftsverkehr kann solch ein System geringere Kosten für Passwort- und Account-Management bedeuten. Und es hilft durch das Begrenzen der Menge an persönlichen Informationen (die sie speichern und schützen müssen), die allgegenwärtigen Risiken von Sicherheitslücken zu reduzieren und gleichzeitig erhöht es den Datenverkehr auf den Webseiten, da keine Registrierung für mehr nötig wird, um die Services einer Website nutzen zu können.

Zwar ist OpenID ein großartiges Konzept zur Identitätenverwaltung, sicherheitstechnisch gibt es jedoch einige Bedenken. Zum einen wird das OpenID häufig Opfer von Phishing-Attacken, bei denen die Benutzer auf falsche Login-Seiten gelockt werden und so ihre Login-Daten ungewollt preisgeben [27]. Wird für die Verbindung kein HTTPS verwendet, können CSRF- oder MITM-Attacken (vgl. 2.2.4 und 2.2.5) ausgeführt werden. Für die Sicherheitsmaßnahmen ist jedoch der Betreiber des OpenID-Servers verantwortlich und Nutzer hat keinen Einfluss darauf. Daher sollte es für OpenID entsprechende verpflichtende Sicherheitsrichtlinien geben und für Zugänge zu sensiblen wie Online-Banking-Accounts sollte man es am besten überhaupt nicht verwenden.

Was an OpenID fehlt, ist eine vom Benutzer kontrollierte Preisgabe seiner Informationen. Nicht jeder Dienst benötigt alle Informationen des Benutzers, um zu funktionieren. Der Benutzer muss für jeden Dienst nur die nötigsten Informationen hinterlassen müssen. Dies ist vor allem beim Online-Dating und bei elektronischen Gesundheitsangelegenheiten von entscheidender Bedeutung.

Ein Online-Dating-Service vergleicht Leute anhand ihrer persönlichen Daten und Interessen durch Algorithmen und Heuristiken miteinander und sucht so die für eine Person passendsten Partner aus. Solch ein Algorithmus benötigt möglichst viele persönliche Daten um zu funktionieren, weshalb die Benutzer den Dating-Seiten ein großes Vertrauen entgegenbringen müssen, dass ihre Informationen mit Respekt und nur für die vorgegebenen Zwecke verwendet werden.

Selbst wenn der Benutzer dem Empfangen von Werbemails von Drittanbietern zustimmt, dann möchten sie trotzdem, dass bestimmte Informationen von ihnen nicht an die Drittanbieter weitergegeben werden. Zum Beispiel jemand der übergewichtig ist, würde es sicher nicht unbedingt wollen, dass er Werbemails für Diätprodukte bekommt.

Um die Privatsphäre zu schützen, erlauben es die meisten Dating-Services ihren Kunden, Pseudonyme anstatt ihrer bürgerlichen Namen zu benutzen. So eine Dating-Seite muss auch nicht die richtigen Namen ihrer Kunden kennen, es sei denn das Angebot ist kostenpflichtig.

Heutzutage können die Kunden von Flirtseiten fast zu jedem Persönlichkeitsmerkmal Angaben machen. Mit solch einer kontrollierten Preisgabe von Informationen wäre der Dating-Service in der Lage von Drittanbietern bereitgestellte und überprüfte Merkmale zu akzeptieren, ohne dass die Kunden dem Risiko unterliegen, unfreiwillig ihre wahren Namen preisgeben zu müssen. Allerdings ist hier die Gefahr von einer Angabe falscher Informationen natürlich entsprechend groß.

Zum Beispiel kann ein bescheinigtes Geburtsdatum eine höhere Übereinstimmung im Ranking-Algorithmus geben als ein ungeprüftes. Ein Zertifikat, das ein Kunde nicht auf einer Blacklist steht, wäre für bestimmte Dating-Seiten zwingend. Solch ein Ansatz würde die Gefahr einer falschen Persönlichkeitsdarstellung reduzieren und das gegenseitige Vertrauen erhöhen, ohne dass sich dies negativ auf die Privatsphäre auswirkt.

Ein anderes Beispiel für solche sensiblen personenbezogenen Daten sind medizinische Dienstleistungen und Medikamente. Heute sind die Informationen über verschiedene Standorte wie der Hausarztpraxis, Apotheken, Versicherungsunternehmen und unserem Arbeitgeber verteilt.

Einer der größten Hürden, die die breite Akzeptanz von elektronischen Gesundheitsdaten behindern, ist die Tatsache, dass solche Daten leicht gestohlen oder missbraucht werden könnten und so Menschenleben in Gefahr geraten könnten. Hier muss es absichert sein, dass der bürgerliche Name (und andere identifizierende Informationen) geschützt sind und getrennt von den eigentlichen medizinischen Daten, Versicherungsbescheinigungen und Rezepten gehalten wird.

Es würde einem Patient auch ermöglichen, ein Online-Portal mit einem gebündelten Identitätensystem zu benutzen, das einen schnellen und sicheren Zugriff auf alle Informationen böte, die beim Arzt, der Apotheke oder bei der Versicherung liegen können. Das vielleicht wichtigste ist, dass diese Daten überprüft werden können und bestimmt werden kann, wo persönliche Daten gespeichert werden, wie sich geschützt sind und wer Zugriff auf sie hat.

OAuth

Ebenso wie OpenID ist auch OAuth ein offenes Protokoll, das eine standardisierte, sichere Authorisierung für Desktop-, Web- und mobile Anwendungen ohne Preisgabe der Nutzeridentität erlaubt. Im Jahr 2007 wurde die erste Version veröffentlicht.

Ein Benutzer kann mit Hilfe dieses Protokolls einer Anwendung den Zugriff auf seine Daten erlauben, die von einer anderen Anwendung verwaltet werden, ohne alle Details seiner Zugangsberechtigung zur anderen Anwendung preiszugeben. Der Benutzer kann so Dritte damit beauftragen und dazu autorisieren, sich von ihnen den Gebrauchswert von Anwendungen erhöhen zu lassen. Typischerweise wird dabei die Übermittlung von Passwörtern an Dritte vermieden.

Im Gegensatz zu OpenID benutzt OAuth keine URLs zur Identifikation, sondern die Benutzer vergeben Token, die innerhalb einer bestimmten Zeitspanne oder für einen bestimmten IP-Adressraum gültig sind. Dieser Token bieten dann einen Zugriff auf eine spezifische Webseite oder auf spezifische Ressourcen. Die Token selbst sind durch SSL verschlüsselt [26].

Allerdings existieren noch viele Sicherheitsprobleme, so wurde im April 2009 eine Sicherheitslücke aufgedeckt, die Phishing ermöglicht [30].

3.2.5 Infrastruktur für benutzerorientiertes Identitätsmanagement

Das Ziel einer flexiblen, nutzerorientierten Identitätsmanagementinfrastruktur muss es sein, dem Nutzer gestatten, zu bestimmen, welche Informationen er welchen Personen und unter welchen Bedingungen preisgeben will. Dabei muss auch gewährleistet sein, wie vertrauenswürdig diese Personen sind, wie sie die Information verwenden und welche Konsequenzen die Verwendung dieser Information besitzt. Solche Systeme sollen es dem Benutzer also erlauben, eine kontrollierte Informationspreisgabe zu ermöglichen. In der Standardeinstellung sollten so wenig Informationen wie möglich preisgegeben werden, das heißt nur die für den Zweck notwendigen. Zusätzliche Informationen sollten nur nach Bestätigung sichtbar gemacht werden können.

Die Unternehmen müssen sich klarmachen, dass Identitätsmanagement nicht nur einen Geschäftsprozess darstellt, sondern auch eine Aktivität der Benutzer. Die Benutzer müssen die entsprechenden Werkzeuge erhalten, ihre persönlichen Informationen auf allen Endgeräten verwalten zu können. Das bedeutet, dass eine Infrastruktur für das Identitätenmanagement für viele Arten von Endgeräten, das heißt sowohl auf dem Desktop-PC als auch auf dem Handy, funktionieren muss. Die Infrastruktur muss auch auf allen Endgeräten über eine einheitliche Bedienung verfügen.

Das bedeutet auch, dass das System auf einem klar strukturierten und offenen Framework von klar definierten Regeln basieren muss. Dies beinhaltet Bestimmungen, die dem Benutzer darlegen, welche Informationen angefordert werden und aus welchem Grund dies geschieht (ähnliche wie eine maschinenlesbare und verbesserte Version der heutigen Datenschutzbestimmungen). Es sollte auch eine Art angeheftetes Zertifikat beinhalten, das immer mit der Information verbunden ist und so absichert, dass diese nur in Übereinstimmung mit der Bestimmung genutzt wird. Im letzten Schritt müssen Konzepte zur Realisierung, Standardisierung und Durchsetzung solcher angehefteten Zertifikate entwickelt werden.

Es existiert bereits eine gewisse Anzahl an Identitätsverwaltungssystemen auf verschiedenen Plattformen. Dies ist nur möglich, wenn die Infrastruktur selbst als auch die individuellen Systeme auf offenen, auf allen Plattformen verfügbaren Standards basieren.

Für eine erfolgreiche nutzerorientierte Identitätsverwaltungsinfrastruktur ist es eine Kernfrage, dass die Entwicklung durch eine große und offene Community vorangetrieben wird, die sich über den gesamten Erdball erstreckt. Außerdem sollte eine solche Infrastruktur vollständig mit offenem Quelltext implementiert sein und keine patentierten Techniken verwenden. Durch personenbezogene Daten lassen sich auch immer Rückschlüsse auf die Identität des Nutzers ziehen. Solche Informationen werden durch besondere Bestimmungen in vielen Teilen der Welt reguliert.

Weiterhin kann ein unsachgemäßer Gebrauch personenbezogener Daten zu Identitätsdiebstahl und anderen Sicherheitsverstößen führen. Daher gebührt den persönlichen Informationen ein besonderer Schutz. Dies beinhaltet auch die Unterstützung solcher angehefteten Zertifikate, Datenverschlüsselungen und die Minimierung der Menge an von verschiedenen Anwendungen genutzten persönlichen Informationen.

Systeme für die Identitätenverwaltung sollten auch eine große Anzahl von Sicherheits- und Datenschutzeigenschaften unterstützen, die von Systemen mit Passwort-basierter Anmeldung und niedriger Sicherheit bis zu State-of-the-art Systemen mit attributbasierten Sicherheitszertifikaten (z.B. die Identity-Mixer-Technologie von IBM oder Microsofts U-Prove-Technologie [31]) reichen.

Am Ende müssen die entsprechenden Applikationen in der Lage sein, die Infrastruktur auch zu verwenden. Das setzt voraus, dass die Anwendung eine Schnittstelle plattform- und geräteübergreifend zu dieser Infrastruktur besitzt. Solche Schnittstellen sollten von benutzten Protokollen und Mechanismen unabhängig sein, die für die Übermittlung der persönlichen Informationen dienen. Deshalb wäre beispielsweise eine vereinheitlichte Architektur sinnvoll, die sich aus mehreren verschiedenen Teilen zusammensetzt.

Durch das Unterstützen einer Fülle von Identitätsmanagementsystemen würde eine solche Architektur eine Migration von Anwendungen von den veralteten Systemen zu den sich etablierenden und moderneren nutzerorientierten erlauben. Um eine solche Migration und das Entwickeln von Applikationen von Grund auf zu ermöglichen, müssen entsprechende Werkzeuge und quelltextoffene Referenzsoftware bereitgestellt werden.

4 Diskussion und Ausblick

Bei der Untersuchung der Situation zur Sicherheit und des Datenschutzes in der Cloud fielen vor allem das Fehlen von verbindlichen Sicherheitsrichtlinien sowie das Fehlen eines einheitlichen Datenschutzniveaus auf, wodurch das Cloud Computing sicherheitstechnisch unberechenbar wird. Daher sollten mittelfristig durch den Gesetzgeber solche verbindlichen Sicherheits- und Datenschutzrichtlinien gesetzlich verpflichtend sein, damit ein Cloud-Anbieter seine Dienste auch legal und ohne Nachteil für den Kunden zur Verfügung stellen kann. Ein großes Problem dabei ist, dass die Cloud-Anbieter länderübergreifend agieren und somit auch länderübergreifende Gesetze wünschenswert sind [6].

Denn Clouds werden auf dem globalen Markt angeboten und werden auch von deutschen Unternehmen sowie auch von Privatnutzenden für die Verarbeitung personenbezogener Daten verwendet. Diese Form der Datenverarbeitung erfolgt weitestgehend im Verborgenen für die Betroffenen, die Aufsichtsbehörden und die Öffentlichkeit. Dass über konkrete Anwendungen nichts bekannt wird, ist kein Hinweis darauf, dass keine Datenschutzverstöße und Persönlichkeitsverletzungen stattfänden. Keiner der direkt Beteiligten – Nutzende, Cloud-Anbieter sowie Ressourcenanbieter – dürfte ein Interesse daran haben, dass eventuelle Verstöße publik werden. Angesichts der öffentlich zugänglichen Informationen und der Rechtslage muss davon ausgegangen werden, dass heute leider bei sehr vielen Cloud-Anwendungen strukturell Datenschutzrechtsverstöße angelegt sind und auch massenhaft erfolgen.

Beim Cloud-Anbieter und im Cloud-Verbund bedarf es eines dokumentierten Datenschutzmanagements, zu dem ein IT-Sicherheitsmanagement und ein Vorfallmanagement gehören. Hierzu bestehen aber nur sehr lose definierte gesetzliche Regelungen.

Außerdem ist es auffällig, dass die Infrastruktur in den Cloud-Rechenzentren oftmals nicht vollständig auf Sicherheit ausgelegt ist. So ergibt sich aus einer nicht ausreichenden Trennung der in der Cloud gespeicherten Daten eine Vielzahl von Risiken. Der Cloud-Auftrag muss zur Absicherung der Abschottung der einzelnen Auftragsverhältnisse voneinander die Methoden zur Trennung der Daten unterschiedlicher Auftraggeber präzise benennen. Erfolgt dies durch Verschlüsselung, so muss geprüft werden, ob die genutzten Systeme eine hinreichende Sicherheit bieten und nicht durch andere Nutzende oder durch die Anbieter selbst einfach kompromittiert werden können.

Die technischen und organisatorischen Maßnahmen der Datensicherung nach § 9 BDSG müssen dem Nutzer offengelegt werden und sind nach dem in Deutschland geltenden Datenschutzrecht ausdrücklich im Vertrag zu benennen. Es kann also nicht das Prinzip *Sicherheit durch Verschleierung* gelten, so wie dies heute weitgehend praktiziert wird.

Symptomatisch hierfür ist die Darstellung des Google-Managers Kai Gutzeit, Chef für Cloud-Dienste in Mittel- und Nordeuropa, zur von seinem Unternehmen erbrachten Datensicherheit. Diese sei zunächst eine Frage des Vertrauens, das heutzutage ja auch der Kreditkarte und den Banken entgegengebracht würde. Sollte aber jemand tatsächlich in die streng geheimen Google-Rechenzentren eindringen, so fände der Einbrecher „gar nichts“ Verwertbares, nämlich nur „bedeutungslose Bits und Bytes“, da Google eigene Dateisysteme verwende.

Vielmehr sollte *Sicherheit durch Transparenz* gefordert werden. Die Maßnahmen müssen dem Stand der Technik entsprechen. Zwingend ist, dass die Zugriffsmöglichkeiten auf die verarbeiteten Daten, abgesehen von administrativen Rechten, technisch beschränkt werden auf die vom Nutzer genannten Berechtigten. Hierzu sind ein differenzierter Zugriffsmechanismus, Verschlüsselungsmöglichkeiten und möglicherweise auch Pseudonymisierungswerkzeuge geeignet.

Den Anbietern ist zwar die Notwendigkeit von Vertraulichkeit und Integrität bewusst, aber nur aus Gründen der Marktpositionierung, nicht aus Gründen des Grundrechtsschutzes oder wegen der

Notwendigkeit der Beachtung des Datenschutzrechtes. Cloud Computing ist ein weiteres Beispiel dafür, dass im Markt zunächst das praktisch gemacht wird, was technisch und ökonomisch möglich ist und lukrativ ist. Erst durch öffentliche Skandalisierung und durch staatliche und länderübergreifende Kontrollen ist eine zunehmende Orientierung an den rechtlichen Vorgaben zu erwarten.

Hier fordern auch viele aktuelle juristische Veröffentlichungen, dass die Rechtsprechung zu Gunsten des Datenschutzes an die aktuellen technischen Möglichkeiten angepasst wird.

Auf internationaler Ebene hat sich die US-dominierte Cloud Security Alliance (CSA) herausgebildet, deren Ziel es ist, Richtlinien für ein sicheres Cloud Computing zu erarbeiten. Die wichtigsten Sicherheitsrisiken, die die CSA benennt, wurden aufgelistet und beschrieben (vgl. 2.1). Mit EuroCloud Deutschland gibt es seit Kurzem einen Verband der deutschen Cloud Computing-Industrie, der in das europäische EuroCloud-Netzwerk eingebunden ist. EuroCloud Deutschland hat sich zur Aufgabe gemacht, dem Benutzer mehr Transparenz zu verschaffen, Rechtsfragen zu klären, ein Gütesiegel einzuführen und den Dialog zwischen Anbietern und Nutzern zu fördern.

Denn ohne die Gewährleistung des nötigen Datenschutzniveaus ist ein professioneller Einsatz dieser Systeme nicht verantwortbar. Fasst man Datenschutz als digitalen Grundrechts- und Menschenrechtsschutz auf, so ist dieser keine Diskriminierung von Cloud-Anbietern, kein Marktverzerrer und kein Technikhindernis, sondern ein Schlüssel für die flächendeckende Verbreitung von Cloud-Computing.

Es scheint recht unwahrscheinlich, dass die genannten Risiken eine Etablierung von Cloud Computing verhindern, da es eine Win-Win-Situation ermöglicht: Sie ist für Anwender bequem und für Anbieter gewinnbringend. Statt diese neue Technologie zu boykottieren, wären das Schaffen von gesetzlichen Rahmenbedingungen und das Aufsetzen von strengen Richtlinien für die Anbieter weitaus sinnvoller.

Durch internationale Regelungen wäre es zweifellos möglich, das Cloud-Computing die Ortsabhängigkeit von Datenverarbeitung bei dieser Art der Verarbeitung aufzuheben und so eine bürokratische und rechtliche Hürde gegenüber Cloud-Nutzern und Anbieter abzubauen. Bisher sind aber keine Bestrebungen dieser Art ersichtlich, denn aufgrund der uneinheitlichen und unzureichenden nationalen Gesetze für die Datenverarbeitung und den Datenschutz sind internationale Normen derzeit noch nicht realistisch.

Forschung, Wirtschaft und Aufsichtsbehörden sind dazu aufgefordert, mit den zuständigen Organisationen Schutzstandards zu erarbeiten sowie Auditierungsverfahren zu entwickeln und zu etablieren.

Das derzeit noch bestehende Grundprinzip der *freien Cloud* genügt nicht den Anforderungen eines modernen Datenschutzes und kann nur als Spiel- oder Versuchsapplikation verstanden werden, aus der sich *vertrauenswürdige Clouds* entwickeln, bei denen Datenschutz- und Datensicherheitsgarantien integriert sind. Diese vertrauenswürdigen Clouds müssen im Markt verfügbar gemacht werden – oder der Grundsatz des Cloud Computing kann zumindest für jede Art von schützenswerten Daten keinen Bestand haben.

Es wird nicht möglich sein, dass volle Potential der nächsten Generation von Internet und Cloud Computing auszuschöpfen ohne zuvor die offene Fragen in Bezug auf digitale Identitäten und Datenschutz zu klären. Glücklicherweise entsteht Fortschritt durch das Entwickeln und zur Verfügung stellen der richtigen Technologien.

Auch wie sich die Identität des Nutzers im Zuge der Etablierung von Cloud-Computing entwickeln wird, bleibt abzuwarten. Beim Schutz der Nutzeridentität sollte immer das höchstmögliche Sicherheitsniveau gewährleistet sein [4]. Ein möglicher Ansatz, wäre das Aufteilen der Benutzeridentität in viele kleine verschlüsselte Teile auf möglichst viele Maschinen. Nur wenn man im Besitz aller Teile ist, kann man die Benutzeridentität herausfinden, was aber so gut wie unmöglich sein sollte. Dies erfordert allerdings einen hohen Rechen- und Verwaltungsaufwand für die Daten, wodurch das Cloud-Geschäft für die Betreiber natürlich weniger lukrativ ist. Aber wir dürfen

wirtschaftliche Interessen nicht über die der Sicherheit und des Datenschutz stellen, denn sonst wird Cloud Computing zum echten Risiko und das 1984-Szenario wäre wieder ein Stück näher gerückt.

Derzeit haben Anbieter von Cloud-Computing-Diensten noch freie Hand. Jedoch setzt mit der zunehmenden Etablierung von Cloud Computing beim Endkunden ein Wandel ein. Mittelfristig werden die Provider zur Einhaltung von Standards verpflichtet sein, wenn sie weiterhin ihre Dienste anbieten möchten. Auch das Schaffen von eindeutigen gesetzlichen Regelungen gehört dazu.

Die Benutzer können die Vorzüge von Cloud Computing nur genießen, wenn sich die Gesetzgeber und Unternehmen weltweit der Lösung der Datenschutz- und Sicherheitsprobleme widmen, die durch die Speicherung und Austausch personenbezogener Daten entstehen.

Referenzen

- [1] Dan Schaefer: „*Cloud Computing: A Blast From the Past?*“ www.ureadit.com/dansblog/91-cloud-computing-a-blast-from-the-past.html, 2010.
- [2] Christof Weinhardt und Arun Anandasivam et al.: „*Cloud Computing - Eine Abgrenzung, Geschäftsmodelle und Forschungsgebiete*“, Universität Karlsruhe (TH), 2009.
- [3] Dr. Carsten Schulz: „*Rechtliche Aspekte des Cloud Computing im Überblick*“, 2008.
- [4] Dieter Klumpp and Herbert Kubicek et al.: „*Netzwelt - Wege, Werte, Wandel*“, Alcatel – Lucent Stiftung für Kommunikationsforschung, Springer, 2010,
- [5] Dieter Klumpp and Herbert Kubicek et al.: „*Mensch, Technik, Kommunikation - Beiträge zur Informatisierung in Gesellschaft, Recht, Ökonomie und Technik*“, Alcatel-Lucent Stiftung für Kommunikationsforschung, Stuttgart, 2009.
- [6] Dieter Klumpp: „*Leitbildkonvergenz in der Netzwelt. Informationsgesellschaft vor der vierten Diskursdekade*“, Alcatel-Lucent Stiftung für Kommunikationsforschung 2010,
- [7] Ann Cavoukian: „*Privacy in the clouds*“, Information and Privacy Commissioner of Ontario, www.ipc.on.ca, 2008.
- [8] William Jeremy Robison: „*Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*“, University of California, 2010.
- [9] Dion Hinchcliffe: „*The cloud computing battleground takes shape. Will it be winner-take-all?*“, 2010.
- [10] Harald Weis: „*'Cloud Computing bringt Ghost Server'*“, silicon.de, 2.11.2010
- [11] Johannes Gernert: „*Wächter der Wolke*“, *Die Zeit*, 07/2010.
- [12] Thilo Weichert: „*Cloud Computing und Datenschutz*“, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, 2009.
- [13] Magnus Kalkuhl: „*Freier Blick für die Zukunft: Cloud-Computing und Cloud-Sicherheit*“, Kaspersky, www.viruslist.com/de/analysis?pubid=200883647, 2009.
- [14] Johannes Gernert: „*Wächter der Wolke*“, *Die Zeit*, 07/2010.
- [15] Andreas Sebayang: „*Security Nightmares X*“, Golem.de, 2010.
- [16] Peter Mell and Tim Grance: „*The NIST Definition of Cloud Computing*“, National Institute of Standards and Technology, 2009.
- [17] Nicolas Zeitler: „*Cloud Computing - Die 7 größten Sicherheitsgefahren*“, CIO, 2010.
- [18] Jerry Archer, Paul Kurtz et al.: „*Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*“, Cloud Security Alliance, 2009.
- [19] Angelika Ruppel: „*Angriffsarten und Angreifertypen in Cloud-Computing-Systemen*“, Fraunhofer SIT, 2010.
- [20] Christopher Ketcham: „*The Cloud Panopticon*“, Investigative Fund at the Nation Institute, www.theinvestigativefund.org/investigations/rightsliberties/1274/thecloudpanopticon/2010.
- [21] Leo Stiles: „*Is the future of gaming in the clouds?*“, www.joe.ie/tech/future-tech/is-the-future-of-gaming-in-the-clouds-004520-1, 2010.
- [22] Rene Reutter and Thorsten Zenker: „*Security Risiken beim Cloud Computing*“, 2009.
- [23] Carl Moses: „*Amazon Security Whitepaper*“, 2010.
- [24] Charlie Kaufman, Ramanathan Venkatapathy: „*Windows Azure Security Overview*“, 2010.

-
- [25] „*Security Whitepaper: Google Apps Messaging and Collaboration Products*“, Google Inc.", 2010.
- [26] Lofi Dewanto: „*Autorisierungsdienste mit OAuth*“, Heise Developer, 2009.
- [27] Lofi Dewanto: „*Identity Management: Authentifizierungsdienste mit OpenID*“, Heise Developer, 2009.
- [28] Bruce Schneiers Blog: www.schneier.com/blog/archives/2006/02/
- [29] Martin Dommer: „*Zum Schweigen verpflichtet*“, FAZ, www.faz.net/~00m3og, 2009
- [30] OAuth Security Advisory 2009.1: oauth.net/advisories/2009-1/
- [31] Kieran Sullivan: „*Identity Management for e-government Use Case*“, www.think-trust.eu, 2009
- [32] Bundesamt für Sicherheit in der Informationstechnik: „*BSI-Mindestsicherheitsanforderungen an Cloud-Anbieter*“
- [33] Bundesministerium für Wirtschaft und Technologie: „*Aktionsprogramm Cloud Computing*“, www.bmwi.de, 2010
- [34] Greenpeace: „*Make IT Green: Cloud Computing and its Contribution to Climate Change*“ www.greenpeace.org/usa/en/media-center/reports/make-it-green-cloud-computing, 2010