Sicherheit bei Cloud Computing

Eugen Wachtel
Betreuer: Heiko Niedermayer
Seminar Innovative Internettechnologien und Mobilkommunikation WS2010/11
Lehrstuhl Netzarchitekturen und Netzdienste, Lehrstuhl Betriebssysteme und Systemarchitektur
Fakultät für Informatik, Technische Universität München
Email: wachtel@in.tum.de

KURZFASSUNG

Cloud Computing ermöglicht die Bereitstellung von IT-Diensten über das Internet, die dynamisch skaliert und kosteneffizient abgerechnet werden. Damit ist Cloud Computing für Organisationen und Service-Anbieter von großem Interesse, erübrigt sich dadurch schließlich eine eigene Hardwarelösung für die Dienste. Doch wie ist es um die Sicherheit von Cloud-Lösungen bestellt? Können Unternehmen mit ihren Systemen in der Cloud die Sicherheitsstandards ohne weiteres einhalten? Dieser Artikel beschäftigt sich mit diesen Fragen und zeigt mögliche Problembereiche sowie einige Lösungsansätze und Best Practices, die in der Praxis Verwendung finden.

Schlüsselworte

Cloud Computing, Sicherheit, Informationssicherheit, Datensicherheit, IT-Sicherheit

1. EINLEITUNG

Die Anforderungen an IT-Lösungen im Internet können sich bezüglich Skalierbarkeit im Betrieb dynamisch ändern, wodurch die Bereitstellung von zusätzlichen oder aber auch die Abschaltung unnötiger Ressourcen schnell und zuverlässig erfolgen muss, um die Wirtschaftlichkeit einer IT-Lösung zu gewährleisten. *Cloud Computing* stellt diesbezüglich eine aktuell sehr populäre Lösung bereit, die dynamisch auf den Ressourcenbedarf reagiert und gleichzeitig eine nutzungsabhängige Abrechnung bereitstellt. Damit ist Cloud Computing für die IT-Welt in vielen Hinsichten relevant. Es unterstützt neben den klassischen auch innovative IT-Dienste und ermöglicht neuartige Geschäftsmodelle im Internet. Das Wachstum für den globalen Cloud Computing-Markt soll aufgrund dieser Vorteile bis 2013 auf einen Wert von 150 Mrd. US-Dollar anwachsen [7]. Demgegenüber sind laut [11, 5] allerdings die Aspekte der Verfügbarkeit, Sicherheit und des Datenschutzes die wesentlichen Gründe für viele Unternehmen eine große Skepsis gegenüber Cloud Computing aufrecht zu erhalten.

1.1 Cloud Computing

Cloud Computing-Systeme (kurz: *Cloud*) setzen sich zum einen aus den Anwendungen (*Services*) und zum anderen aus der Soft- und Hardware, die diese bereitstellt, zusammen. Der Hauptunterschied zwischen konventionellen Systemen und Cloud Computing liegt in der Entkopplung der Daten und Software von den Servern und der Bereitstellung solcher als Services. Abbildung 1 vermittelt den Unterschied in der Architektur-Sicht. Bei konventionellen Client-Server-Systemen sind die verfügbaren Ressourcen unmittelbar sichtbar sowie deren Standort bestimmbar. Beim Cloud Computing hingegen kann von einem unendlichen Ressourcenpool ohne bestimmbare Lokalität der einzelnen Komponenten ausgegangen werden. Dieser Unterschied erlaubt eine flexible und kostengünstige Skalierung sowie Abrechnung der Cloud-Dienste, bringt aber auch problematische Aspekte wie die Erfüllung der Compliance Anforderungen mit sich. Cloud Computing wird mittels moderner Virtualisierungs- sowie Automatisierungs- und Bereitstellungstechnologien umgesetzt [12].

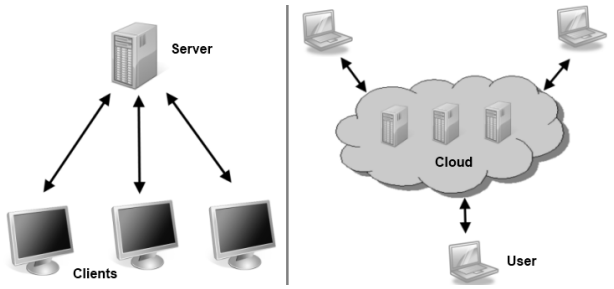

Abbildung 1: Client-Server vs. Cloud Computing-Architektur

Hintergrund. Cloud Computing wird erst in letzter Zeit in der Breite populär, doch die Idee dahinter ist nicht neu und findet bereits seit längerer Zeit Anwendung. Großunternehmen, wie Microsoft oder Amazon, setzen unternehmensintern seit Jahren darauf. Neu ist heutzutage die Verfügbarkeit solcher Systeme für die Öffentlichkeit, die durch die *Cloud Provider* bereitgestellt wird. Wir unterscheiden diesbezüglich zwischen

- *Public Clouds* stellen öffentlich zugängige Clouds dar, bei denen der Cloud Provider die Richtlinien bezüglich Sicherheit festlegt.
- *Private Clouds* gehören einem Unternehmen, das die Kontrolle über die Cloud hat und diesbezüglich auch seine Festlegungen und Standards bezüglich Sicherheit aufstellen kann.
- *Hybrid Clouds* setzen sich aus Public und Private Clouds zusammen.

doi: 10.2313/NET-2011-05-2_10

Wir fokussieren in diesem Artikel insbesondere die Public Clouds.

Genutzt werden Clouds durch Unternehmen sowie IT-Lösungsanbieter, bezeichnet als die so genannten *Cloud User*, deren Dienste ihrerseits den *Service Usern* zur Verfügung gestellt werden (siehe auch Abbildung 2).

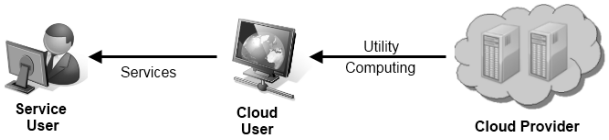

Abbildung 2: Benutzer und Anbieter beim Cloud Computing [4]

Servicemodelle. Cloud Computing ist eine Architektur zur Bereitstellung von Dienstleistungen. Diese können, je nach Cloud Provider, unterschiedlich sein (siehe auch Abbildung 3):

Software as a Service (*SaaS*) bezeichnet die Bereitstellung von Applikationen als Service über das Internet. Der Betrieb und die Instandhaltung der Applikationen wird seitens des Anbieters übernommen, wie beispielsweise bei den Google Apps.

Platform as a Service (*PaaS*) ist durch die Bereitstellung von Entwicklertools und Schnittstellen zur Entwicklung von Webapplikationen gekennzeichnet. Die Dienste werden basierend auf der Infrastruktur des Anbieters programmiert und betrieben. Bekannte Beispiele sind Google App Engine, Microsoft Azure und Salesforce.com.

Infrastructure as a Service (*IaaS*) stellt Speicherplatz oder Rechenleistung zur Verfügung. Prominente Beispiele sind Amazon EC2 und Microsoft Azure.

Chancen. Sowohl für den Cloud User als auch für den Cloud Provider ergeben sich durch das Cloud-Modell Chancen [14]:

Cloud User Der Aspekt der Kostenreduzierung aufgrund der Skalierung bei Bedarf und der Bezahlung nach Verbrauch wurde bereits angesprochen. Hinzu kommen die höhere Flexibilität bei der Wiederverwendung bestehender Systeme sowie eine Verkürzung der Entwicklungszeit zur Marktreife von Diensten. Schließlich werden die Innovationsmöglichkeiten hinsichtlich der Gestaltung neuer Systeme erweitert.

Cloud Provider Neben den wirtschaftlichen Aspekten sind die technischen Verbesserungsmöglichkeiten als Chancen zu sehen. So kann der Betrieb des Rechenzentrums optimiert und die administrativen Prozesse automatisiert werden. Dadurch können verkürzte Innovationszyklen bei der Bereitstellung von neuen Diensten erreicht werden.

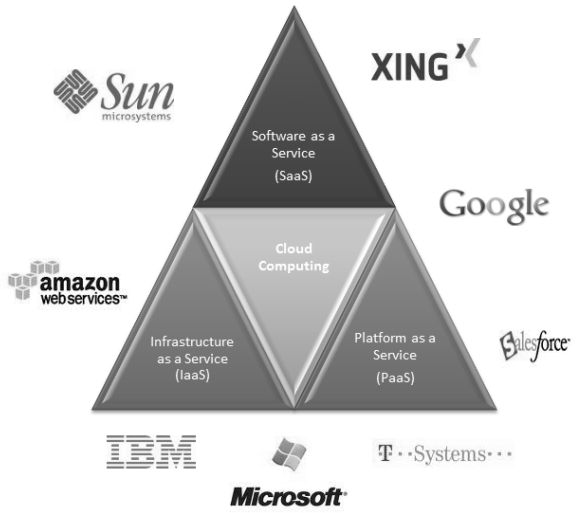

Abbildung 3: Überblick über die Cloud Anbieter sowie die angebotenen Dienstleistungen.

Sicherheit. Cloud Computing ist eine Plattform, die den Unternehmen viele Vorteile bietet, jedoch nach wie vor auf eine große Skepsis bezüglich der Sicherheit stößt. Sicherheitsrisiken können beim Cloud Computing an unterschiedlichen Stellen auftreten, sei es aufseiten des Service Users, bei der Programmierung und Bereitstellung von Diensten seitens des Cloud Users oder aber auch beim Cloud Provider. Im Folgenden diskutieren wir vor allem die Sicherheitsrisiken für den Entwickler von IT-Lösungen, die auf öffentlichen Clouds laufen, weisen allerdings auch auf mögliche Problembereiche bezüglich des Cloud Providers hin.

1.2 Verwandte Arbeiten

Zum Cloud Computing gibt es eine Vielzahl an Literatur, die das Thema der Sicherheit in der Cloud aus unterschiedlichen Blickwinkeln diskutiert. So wird in [6] vor allem die Sicherheit privater Clouds aus Sicht des Unternehmers und des Cloud Providers angesprochen sowie einige Best Practices aufgelistet. Ein Entwurf der BSI [8] listet die Mindestsicherheitsanforderungen auf, die von Cloud Providern erfüllt werden sollen. Die Studie [14] des Fraunhofer-Instituts für Sichere Informationstechnologie liefert neben Erkenntnissen und Lösungsmöglichkeiten zu Sicherheitsbedenken auch eine Taxonomie, die einen Rahmen zur Bewertung der Cloud-Sicherheit schafft.

1.3 Aufbau der Arbeit

Der strukturelle Aufbau dieser Arbeit ergibt sich wie folgt:

Kapitel 2 beschäftigt sich mit dem Thema Sicherheit bei Clouds und betrachtet dieses aus unterschiedlichen Sichten. Zunächst spricht Abschnitt 2.1 die Risiken für den Service User, sprich für den Benutzer der Cloud-Dienste, an. Folgend setzt sich Abschnitt 2.2 mit den Sicherheitsbedenken für den Cloud User auseinander, der die Dienste in der Cloud anbietet. Abschnitt 2.3 vertieft diese Thematik anhand der Cloud Storage-Systeme. Schließlich listet Abschnitt 2.4 problematische Sicherheitsaspekte auf der Seite des Cloud Providers auf.

doi: 10.2313/NET-2011-05-2_10

Kapitel 3 fasst abschließend die Arbeit zusammen und spricht zudem offene Fragen zur Thematik an.

2. CLOUD COMPUTING UND SICHERHEIT

Cloud Computing stellt eine immer populärer werdende Lösung, skalierbare IT-Dienste kosteneffizient im Internet anzubieten. Jedoch bringt die moderne Technologie des Cloud-Modells auch neuartige Sicherheitsprobleme mit sich und eröffnet neue Angriffsmöglichkeiten. In diesem Kapitel wollen wir uns mit Sicherheitsrisiken beim Cloud Computing beschäftigen und diese jeweils aus den Sichten der Service und Cloud User betrachten. Dabei fokussieren wir vor allem die Risiken, die den Cloud User betreffen, im Detail.

2.1 Risiken für den Service User

Der Service User greift über das Internet auf einen bestimmten Dienst zu. Demzufolge gelten hier die gleichen Risiken wie bei jedem IT-Dienstzugriff über das Internet. Genauer genommen ist es für einen Benutzer nicht direkt erkennbar, ob ein Dienst in der Cloud läuft oder nicht. Es ist für ihn aber auch nicht weiter von Bedeutung. Das Problem des Identifikationsbetrugs ist auch in der Cloud ernst zu nehmen. Generell ist *Fraud Protection* eine herausfordernde Aufgabe, die täglich neuen Angriffsarten ausgesetzt ist. Behelfen kann man sich beispielsweise durch Risikoauthentifizierung, bei der neben der Eingabe eines Benutzernamens und Passwords noch zusätzliche benutzerspezifische Informationen abgefragt werden.

Somit sind beim Zugriff auf einen Dienst unter anderem Brute-Force Attacken auf beispielsweise Benutzerpasswörter, Trojaner, Malware oder Phishing die wesentlichen Angriffe/Risiken für einen Service Benutzer. Weitere Informationen diesbezüglich können [3] entnommen werden.

Ein weiteres Risiko ergibt sich für den Service User bei der Nutzung von *Software as a Service* Angeboten[1]. So versprechen Dienste wie beispielsweise Google Mail einen reibungslosen Email-Verkehr, sie sind allerdings in der Regel weder vertraglich verbunden die Dienste immer und jederzeit verfügbar zu machen, noch können sie bei Datenverlusten zur Rechenschaft gezogen werden. Zudem ist die Datenschutz-Thematik bei SaaS-Angeboten mehr als nur beachtenswert. Viele Anbieter formalisieren eine vertragliche Nutzung der Daten für Eigenangebote oder sogar für Drittanbieter. Vielen Benutzern solcher Dienste ist das in der Regel aber nicht bekannt. Diese und weitere SaaS-Problematiken sind jedoch wieder nicht cloudspezifisch, sondern gelten grundsätzlich für die SaaS-Angebote.

2.2 Risiken für den Cloud User

Die Verlagerung der IT-Dienste oder IT-Infrastruktur kann, wie bereits angesprochen, finanziell große Vorteile aufweisen und zusätzlich operative Freiräume in der Gestaltung der IT-Landschaft gewährleisten. So kann die Infrastruktur leicht ohne zusätzliche Hardware/Software-Investitionskosten ausgebaut werden und die überflüssigen Wartungsausgaben entfallen. Der Transfer auf eine cloudbasierte Lösung ist allerdings für den Cloud User mit Sicherheitsbedenken verbunden. So kann die bereits vorhandene Sicherheitsstrategie eines Unternehmens auch in der Cloud verwendet werden, sie muss allerdings an die spezifischen Gegebenheiten des Cloud-Modells angepasst und erweitert werden. Beim Programmieren von Services für die Cloud sind zudem einige Besonderheiten zu beachten, die beispielsweise in der konventionellen Webentwicklung unproblematisch sind. Ressourcen unterliegen in der Cloud einer gemeinsamen Nutzung, Kontrolle, Verwaltung sowie Teilung, so dass auch hier Anpassungen in bewährten Sicherheitsmaßnahmen notwendig sind.

Die administrative Seite des Cloud Computing ist insbesondere bei den Public Clouds ein weiterer Angriffspunkt. In der Regel wird über ein vom Cloud-Anbieter angebotenes Verwaltungsportal die Administration vorgenommen (Speicher/Maschinen hinzufügen oder abbestellen, etc.). Damit ist die administrative Schnittstelle ein lohnendes Angriffsziel, das mit hohen Risiken verbunden ist. Der Cloud User muss unternehmensintern eine klare Trennung der Zugriffsrechte durchsetzen, sodass nur autorisierte Mitarbeiter Änderungen an der Cloud-Plattform vornehmen können. Andererseits muss der Cloud Provider auch Schutzmaßnahmen ergreifen, um die Verwaltungsportale vor Angriffen zu schützen.

Gerade aus wirtschaftlicher Sicht ist die oben angesprochene Angriffsmöglichkeit auf administrative Verwaltungsportale problematisch, da beim Cloud Computing nach einem *Payper-Use* Modell abgerechnet wird. Das bedeutet aber auch, dass generell eine nicht-autorisierte Nutzung einen ökonomischen Schaden verursacht. Das ist beispielsweise bei Dateien gegeben, die unberechtigt geladen werden, aber eigentlich vom System nur gegen Entgelt übers Internet angeboten werden.

In diesem Abschnitt wollen wir uns mit den Risiken für den Lösungsanbieter von IT-Diensten in der Cloud beschäftigen und neben der Auflistung der Probleme auch Lösungsmöglichkeiten vorschlagen. Dabei wird die Thematik der Sicherheit aus der Sicht der Unternehmenssicherheit bei der Nutzung des Cloud-Modells (Verfügbarkeit, Datenschutz, Informationssicherheit) betrachtet.

Damit soll dem Leser ein umfassendes Bild über die Sicherheitsbedenken im Cloud Computing aufseiten des Cloud Users gegeben werden.

2.2.1 Compliance

Unter *IT-Compliance* wird die Einhaltung gesetzlicher und verträglicher Regelungen verstanden, die sich insbesondere auf die Richtlinien des Datenschutzes und -aufbewahrung, Informationssicherheit sowie Verfügbarkeit beziehen. Unternehmen müssen solchen Verpflichtungen, die auch oft landesspezifische Unterschiede aufweisen, nachgehen, denn bei Nichteinhaltung drohen hohe Geldstrafen. Die Studie zur IT-Sicherheit und IT-Compliance [10] von ibi research an der Universität Regensburg unterstreicht die Relevanz der Compliance- und Sicherheitsanforderungen für Unternehmen

[1] Ein Beispiel hiervon lässt sich beim Smartphone „Sidekick“, das von T-Mobile in den USA angeboten wurde, feststellen. Besitzer des Smartphones konnten persönliche Daten im Internet speichern, die nach einem Problem in der zugehörigen Cloud-Lösung größtenteils unwiederbringlich verloren wurden [2].

doi: 10.2313/NET-2011-05-2_10

und zeigt, dass beide Themen auch aktuell einen hohen Stellenwert genießen. Gerade in der Cloud wird aber die Einhaltung der Compliance-Regelungen und Vorgaben für ein Unternehmen erschwert.

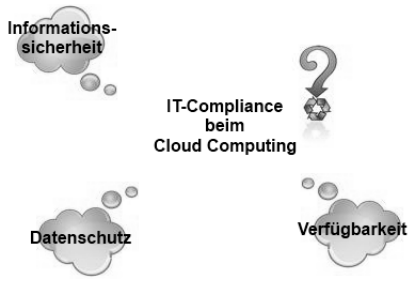

Abbildung 4: Aspekte der IT-Compliance in der Cloud.

Wie werden datenschutzrechtliche Anforderungen vom Cloud-Anbieter erfüllt und wie lässt sich ein verantwortungsvoller Umgang mit IT-Compliance sicherstellen? Gerade diese Fragen beschäftigen viele Unternehmen, die einen Umstieg auf das Cloud-Modell erwägen. Das liegt in erster Linie daran, dass die Verantwortung für personenbezogene Daten auch bei der Nutzung der Cloud-Services nach dem Bundesdatenschutzgesetz beim Cloud User als Auftraggeber liegt. Deshalb sind hier vertrauensvolle Cloud Anbieter wichtig, die datenschutzkonforme Cloud-Services transparent anbieten, so dass seitens des Cloud Users die Einhaltung der gesetzlichen Regelungen überprüft werden kann.

Für kleine bis mittelgroße Unternehmen wird aufgrund der IT-Compliance der Umstieg auf das Cloud-Modell plötzlich problematisch. Sie haben sich in der Regel soweit nur geringfügig mit den gesetzlichen Anforderungen auseinandergesetzt und haben diesbezüglich auch keine Strategie entwickelt. Beim Cloud Computing müssen sie sich aber mit diesem zentralen Thema auseinandersetzen. Anders ist es bei Großunternehmen, die in vielen Ländern vertreten sind und deshalb bereits Strategien zur Einhaltung der Compliance-Vorgaben erarbeitet haben.

In den folgenden Abschnitten werden wir die Aspekte der vertraglichen Regelungen der IT-Compliance näher vorstellen und aus der Sicht des Cloud Users diskutieren.

2.2.2 *Verfügbarkeit*

Hohe Verfügbarkeit und Stabilität der IT-Dienste ist für ein Unternehmen eine Grundvoraussetzung, um einen erfolgreichen Geschäftsbetrieb zu ermöglichen. Bereits der Ausfall von Teilbereichen der IT-Infrastruktur kann zu großen Beeinträchtigungen führen und im größeren Ausmaß sogar existenzbedrohend sein. Das gilt für Klein- als auch insbesondere für Großunternehmen. Damit sind die Anforderungen an Verfügbarkeit vor allem bei Cloud-Modellen seitens der Cloud User entsprechend hoch. Problematisch wird das beim Cloud-Modell gerade aufgrund der Erreichbarkeit der Dienste und der Daten von überall und zu jeder Zeit über das Internet. Hochverfügbarkeit ist beim Cloud Computing damit ein sehr herausforderndes Thema, schließlich sind die meisten Cloud-Systeme vielen Internet-Attacken (beispielsweise *Denial of Service*) ausgesetzt. Die Sicherstellung der Verfügbarkeit liegt hierbei in erster Linie beim Cloud Anbieter, die sich allerdings vertraglich in der Regel dazu nicht binden lassen. Vor allem in Public Clouds sind Ausfälle möglich.

Beispiel: Google Mail - Ausfälle

Google bietet mit der Cloud-Lösung *Google Apps* Dienste für Klein bis Großunternehmen an. Dazu gehört auch Google Mail, das allerdings in der Vergangenheit Ausfälle verzeichnete [13] und über gewisse Zeitspannen nicht erreichbar war (z.B.: Webinterface ca 100 Minuten [1]). Das kann für Unternehmen sehr problematisch sein, vor allem wenn bei derartigen Ausfällen Emails verloren gehen.

Zur Absicherung des Unternehmens bezüglich der Verfügbarkeit von IT-Diensten muss in erster Linie ein vertrauenswürdiger Cloud Anbieter gewählt werden, der einen hohen Stellenwert bei den Kriterien Stabilität und Verfügbarkeit aufweist. Allerdings reicht das insbesondere bei größeren Unternehmen in der Regel nicht aus, denn technische Mängel sind in der Cloud sehr wohl möglich, nicht erreichbare IT-Dienste können aber existenzbedrohend sein. Daher kann die Erhaltung der Teile eigener Infrastruktur als Lösungsvorschlag genannt werden, die zumindest die wesentlichen IT-Services abdecken. Somit können diese beim Ausfall der Cloud die für das Unternehmen essentiell notwendigen Funktionalitäten anbieten.

2.2.3 *Datenschutz*

Der Schutz persönlicher Daten ist für Unternehmen ein sehr wichtiges Thema. Neben den gesetzlichen Bindungen und den damit bei Verletzungen drohenden Strafen, ist auch ein Imageverlust für die meisten Unternehmen ein großes Problem. Gerade in der Cloud ist die Erfüllung gesetzlicher Vorgaben bezüglich Datenaufbewahrung und -übertragung nicht einfach, denn die Lokalität der einzelnen Server kann im Cloud-Serverpool nicht ohne weiteres festgestellt werden.

Beispiel: Datenaufbewahrung- und übertragung in Deutschland [6]

Betrachten wir beispielsweise die Vorgaben zur Datenaufbewahrung und -übertragung in Deutschland (Bundesdatenschutzgesetz), so sind Unternehmen zwingend verpflichtet, persönliche Daten der Bundesbürger auf Server zu übertragen oder speichern, die sich im Gültigkeitsbereich der deutschen Rechtsprechung befinden. Gerade in der Cloud ist das aber nicht unproblematisch, denn hier bilden viele Server einen einzelnen Server-Pool (die Cloud) und die Lokalität einzelner Server kann sehr unterschiedlich sein. Damit könnten tatsächlich persönliche Daten auf Server gelangen, die nicht den Vorlagen der IT-Compliance in Deutschland entsprechen. Die Einforderung der Einhaltung von Compliance-Regeln seitens des Cloud Anbieters ist nicht einfach, schließlich handelt es sich beim Cloud Computing um eine Form des Auslagerns und dieses ist immer mit juristischen Tücken verbunden.

---

doi: 10.2313/NET-2011-05-2_10

Zur Lösung der obigen Problematik stehen Unternehmen unter anderem die folgenden Möglichkeiten zur Verfügung:

1. Nutzung von Private Clouds: Aufgrund der Exklusivität der Benutzung einer Cloud von einem einzelnen Unternehmen lassen sich Regelungen besser verhandeln als bei Public Clouds. Somit können Unternehmen bei vertrauenswürdigen Cloud Anbietern auch IT-Compliance Regelungen durchsetzen und sich vertraglich zusichern lassen.

2. Vertrauenswürde Public Cloud Anbieter: Auch bei Public Clouds gibt es Anbieter, die landesspezifisch die IT-Compliance Vorgaben erfüllen können. Allerdings verlangt die Nutzung der Angebote solcher Anbieter auch nach einem gewissen Grad an Vertrauen und nach einer entsprechenden Transparenz beim Anbieter, so dass die compliancegerechte Datenspeicherung überprüft werden kann.

3. Unternehmerspezifische Lösung: Eine weitere Lösungsmöglichkeit der Problematik kann in der Auslagerung der Datenspeicherung auf ein spezifisch hierfür entwickeltes Eigensystem des Unternehmens thematisiert werden. Allerdings ist das zwangsläufig mit dem Verlust der Cloud Vorteile verbunden.

2.2.4 Informationssicherheit

Die Informationssicherheit beschäftigt sich mit dem Schutz von Systemen, die Information verarbeiten oder speichern. Dabei soll die Integrität, die Vertraulichkeit und die Verfügbarkeit der Daten sichergestellt werden. Im Rahmen des Cloud Computings ergeben sich gegenüber konventionellen Systemlösungen weitere Risiken. So nehmen in der Cloud neben den üblichen Mensch-Maschine Kommunikationen zusätzlich Maschine-Maschine Transaktionen zu. Die Feststellung der Anwenderidentität muss hierbei sichergestellt werden, um nicht zulässige IT-Transaktionen auszuschließen. Problematisch wird das durch die Automatisierung der Transaktionen in der Cloud. Eine Maschine kann nämlich auch für einen Menschen agieren, so dass der Authentifizierung und der Verwaltung von Identitäten eine große Wichtigkeit zukommt.

Auch der Weg des Nachrichtenaustauschs muss abgesichert werden. In einem Mensch-Maschine Szenarium ist das über das Internet beispielsweise mittels Verschlüsselung und der richtigen Benutzung entsprechender Protokolle durchführbar. In der Cloud selbst, bei Maschine-Maschine Transaktionen, muss die Sicherheit durch den Cloud Provider hergestellt werden.

Die Auslagerung von Diensten beziehungsweise von Teilen der IT-Infrastruktur bedeutet gleichzeitig, dass sich Teile der Unternehmensdienste und der damit verbundenen Daten im Besitz Dritter befinden. Somit müssen aufseiten des Cloud Users insbesondere bei vertraulichen Daten Verschlüsselungsalgorithmen angewandt werden, um die Daten zu schützen. Das ist insbesondere bei sensiblen Daten wichtig, die zudem auch separiert werden sollten. Gleichzeig ist beim Cloud Anbieter sicherzustellen, dass der physikalische und der virtuelle Raum geschützt ist und keine Zugriffe seitens benachbarter Systeme möglich sind.

Der Cloud User muss sich bei der Wahl des Cloud Anbieters zudem vergewissern, dass dieser die Standards zur Informationssicherheit einhält. Das kann beispielsweise über den Nachweis von Zertifizierungen erfolgen.

2.3 Risiken bei der Cloud Storage

IT-Anwendungen sowie ihre Benutzer produzieren immer mehr Daten, die geschützt, archiviert und zur Weiterverwendung zur Verfügung gestellt werden müssen. Der Datenzuwachs wird für viele Unternehmen immer problematischer, so dass eine kostengünstige und skalierbare Lösung notwendig ist. Genau in diesem Zusammenhang kommt die *Cloud Storage* ins Spiel. Initial für die Archivierung und Backups gedacht, bietet Cloud Storage mittlerweile sehr viele Formen der Datenspeicherung. So können beispielsweise Datenbanksysteme auch in der Cloud genutzt werden oder aber die Datensicherung in rein tabellarischer Form erfolgen. Für Unternehmen ergeben sich durch die kostengünstige und skalierbare Form der Datenhaltung beim Cloud Storage enorme Vorteile. Sie können durch die Cloud-Nutzung ihre Daten über ein hochverfügbares System anbieten und müssen dafür nur einen Bruchteil des Preises einer traditionellen Lösung bezahlen.

In diesem Abschnitt wollen wir uns mit der Sicherheit von Cloud Storage aus der programmiertechnischen Sicht auseinandersetzen. Generelle Sicherheitsbedenken zum Datenschutz und Verfügbarkeit sowie der Informationssicherheit können auch bei Cloud Storage angewandt werden, so dass hier darauf nicht weiter eingangen wird. Als Beispiele für prominente Cloud Storage Systeme können *Microsoft Windows Azure Storage Services* und *Amazon Simple Storage Service* (S3) genannt werden, anhand derer die Analyse der Sicherheit geführt werden soll. Hierbei beziehen wir uns vor allem auf die Lösung von Microsoft [9], Details zu der Cloud Storage von Amazon können entsprechend auch [9] entnommen werden.

Microsoft Windows Azure Storage. Microsoft bietet mit den Windows Azure Storage Services mehrere Möglichkeiten zur persistenten Speicherung von Daten in einem Cloud-System an:

- *Blob Service*: *Binary Large Objects* (Blobs) sind binäre Objekte, die im Rahmen der Blob Storage gespeichert werden können. Dabei kann es sich beispielsweise um Bilder, Videos oder Musikdateien handeln. Die Blobs können öffentlich zugängig sein oder aber auch nur bestimmten autorisierten Benutzern vorbehalten bleiben. Für jedes Blob ist eine maximale Größe von 1TB festgelegt.

- *Table Service*: Table Services ermöglichen es Anwendungsbesitzern frei-formatierte Daten in Tabellen abzuspeichern. Dabei kann jeder Eintrag mehrere Eigenschaften aufweisen, die zwischen den Einträgen auch unterschiedlich sein können. Die so gespeicherten Daten liegen zwar in tabellarische Form vor, sie sind allerdings nicht mit relationalen Datenbanktabellen zu verwechseln. Konzepte wie *Foreign Keys* sind bei Table Services nicht vorhanden. Die Tabellen selbst können

doi: 10.2313/NET-2011-05-2_10

sehr groß werden (Billionen von Zeilen) und mehrere Terrabyte an Daten beinhalten.

- *Queue Service*: Die Queue Services werden in der Regel für die Kommunikation zwischen Anwendungen genutzt. So können hierbei Nachrichten hinzugefügt und gelesen werden.
- *SQL Azure*: SQL Azure ermöglicht den Zugriff auf eine relationale Datenbank in der Cloud, die über die meiste Funktionalität einer Datenbanklösung wie Microsoft SQL verfügt. Die Kommunikation mit SQL Azure erfolgt über das Protokoll TCP, so dass Software, die zur Verwaltung oder zum Zugriff sowie zur Kommunikation mit der Microsoft SQL-Plattform geschrieben wurde, hier genauso für SQL Azure verwendet werden kann.

Bei der Betrachtung der Sicherheit sowie möglicher Angriffsszenarien beziehen wir uns vor allem auf Blob und Table Services. Für SQL Azure gelten dieselben Sicherheitsbedenken wie bei klassischen Datenbanken, so dass wir sie in diesem Artikel nicht weiter behandeln.

Zugriffs-API. Zum Zugriff auf die Daten der Blob, Table und Queue Services wird die so genannte *REST API* verwendet. Dabei sind die Schreib- und Lesevorgänge einfache POST/PUT und GET-Requests. So kann ein öffentlich zugängliches Blob wie folgt gelesen werden:

```
GET http://accountname.blob.core.windows.net/
    containername/blobname?snapshot=datetime
    HTTP/1.1
```

Ein Lesezugriff auf eine Tabelle kann wie folgt erfolgen:

```
GET http://accountname.table.core.windows.net/
    tablename(PartitionKey='partitionkey',
    RowKey='rowkey') HTTP/1.1
```

Dabei werden die gefundenen Daten in der Tabelle im XML-Format zurückgegeben. Bei geschützten Blobs oder Tabellen sind zusätzliche HTTP-Header notwendig, die die Authentizität sicherstellen.

Zum Schreiben von Blobs oder Tabellen werden PUT-Befehle verwendet. Eine vereinfachte Darstellung einer Schreiboperation bei Blobs sieht wie folgt aus (eine genauere Darstellung kann [9] entnommen werden):

```
PUT http://myaccount.blob.core.windows.net/
    mycontainer/myblockblob HTTP/1.1
*HTTP Headers*
*Content*
```

Bei Tabellen sieht der strukturelle Aufbau von Schreibnachrichten wie folgt aus (siehe auch [9])

```
POST http://myaccount.table.core.windows.net/
    GuestBookEntry HTTP/1.1
*HTTP Headers*
*XML-Content*
```

Neben der REST API kann bei Azure Storage auch eine .NET plattformspezifische Bibliothek verwendet werden (Teil der *Windows Azure SDK*). Durch die Verwendung der .NET API verringern sich viele programmiertechnische Risiken, so dass wir uns im Folgenden bei der Analyse der Sicherheit vor allem auf die REST API konzentrieren.

2.3.1 Klassische Datenbankattacken

In einer Webapplikation ist die eigentliche Datenbank in der Regel für einen Angreifer nicht direkt erreichbar und wird durch die Wahl der Architektur somit geschützt. Allerdings werden Datenbanken über Nachrichten mit Benutzereingaben angesteuert, so dass ein Angriff durch eine sinnvolle Manipulation solcher Eingaben durchaus geschehen kann. Die wohl bekannte Angriffsweise, die genau dieses Prinzip ausnutzt, ist *SQL Injection*. Eine weitere Methode, *XML Injection*, nutzt Mechanismen von XML-Parsern aus, um Nachrichtenein- und -ausgaben zu manipulieren. Beide Angriffsweisen sind nicht cloudspezifisch, können aber in der Cloud sehr wohl auftreten. Weitere Information zu SQL und XML Injection können [9] entnommen werden.

2.3.2 Bedrohungen von Cloud Systemen

In diesem Abschnitt wollen wir Angriffsmöglichkeiten [9] auf Systeme näher diskutieren, die zur Datenspeicherung Azure Storage Services verwenden. Dabei werden, bedingt durch die Nutzung von XML durch die REST API, XML-basierende Attacken thematisiert. Hierzu definieren wir uns zunächst ein Beispiel, anhand dessen die einzelnen Attacken näher erläutert werden können:

Betrachten wir beispielsweise eine einfache MP3-Verkaufsplattform, so können dort beim Kauf einer Musikdatei die Lieferadresse sowie ein Kommentar hinterlassen werden. In Azure Table Store könnte die Schreiboperation eine strukturierte Nachricht wie folgt verwenden:

```
<content type="application/xml">
 <m:properties>
  <d:Address>Meine Adresse...</d:Address>
  <d:UserID>523</d:UserID>
  <d:FileID>123231</d:FileID>
  <d:Comment>Mein Kommentar...</d:Comment>
  ***weitere Felder***
 </m:properties>
</content>
```

Folgend versuchen wir einige Attacken auf diesen einfachen MP3-Shop anzuwenden.

Direct Node Injection. Diese Attacke greift die Operationen der REST API an in der Annahme, dass zum Verarbeiten von XML Sax-Parser eingesetzt werden, die den XML-Datenstrom sequentiell abarbeiten. Welche Parsertypen von Cloud Storage Systemen tatsächlich verwendet werden, ist in der Regel (wie z.B. bei Microsoft oder Amazon) nicht bekannt. Bei der *Direct Node Injection* wird nun versucht, Daten der Eingabefelder zu manipulieren, um beispielsweise ein anderes Verhalten zu erreichen.

Im obigen Beispiel des MP3-Shops ist das Kommentarfeld der Angriffspunkt. Ein manipulierter Kommentarwert wie

doi: 10.2313/NET-2011-05-2_10

```
</d:Comment><d:UserID>100</d:UserID><d:Comment>
    Mein Kommentar...
```

würde die ursprüngliche Nachricht wie folgt verändern

```
<content type="application/xml">
 <m:properties>
  <d:Address>Meine Adresse...</d:Address>
  <d:UserID>523</d:UserID>
  <d:FileID>123231</d:FileID>
  <d:Comment></d:Comment><d:UserID>100</d:
      UserID><d:Comment>Mein Kommentar...</d:
      Comment>
 </m:properties>
</content>
```

und damit den Kauf einer MP3 als Benutzer mit der ID 100 ausführen. Es ist klar, dass diese Attacke in der Regel blind ausgeführt werden muss, denn die einzelnen Datenstrukturen einer Applikation sind im Normalfall nicht bekannt. In der Praxis wurden jedoch solche Attacken auch schon erfolgreich durchgeführt. Bei Windows Azure funktioniert die *Direct Node Injection*-Attacke nicht, es wird ein „400 Bad Request“ als Antwort zurückgegeben, was auf einen DOM-Parser zur Verarbeitung von XML schließen lässt. Dabei ist allerdings nicht zwingend gegeben, dass ein DOM-Parser auf der Cloud Provider-Seite zum Einsatz kommt. Cloud Provider geben in der Regel nicht ohne weiteres bekannt, welche Parsertypen sie verwenden.

CDATA and XML Comment Injection. Diese Attacke greift XML-Parser an, die über das volle XML-Verständnis verfügen und somit auch mit Kommentaren und CDATA-Feldern umgehen können (beispielsweise DOM-Parser). Hierbei wird versucht, zwei manipulierbare Felder so zu füllen, dass sie die dazwischen vorkommenden Felder auskommentieren. Im MP3-Shop Beispiel könnte dazu das Adressfeld mit

```
Meine Adresse...</d:Address><!--
```

und das Kommentarfeld mit

```
--><d:UserID>200</d:UserID><d:FileID>123231</d:
    FileID><d:Comment>Mein Kommentar...
```

gefüllt werden, um somit das folgende XML zu erhalten:

```
<content type="application/xml">
 <m:properties>
  <d:Address>Meine Adresse...</d:Address><!--</
      d:Address>
  <d:UserID>523</d:UserID>
  <d:FileID>123231</d:FileID>
  <d:Comment>--><d:UserID>200</d:UserID><d:
      FileID>123231</d:FileID><d:Comment>Mein
      Kommentar...</d:Comment>
 </m:properties>
</content>
```

Damit können nun für User sowie File beliebige IDs und Lieferadressen festgelegt werden. Diese Attacke *funktioniert* nach [9] bei Azure Storage.

Ein ähnlicher Angriff kann auch mittels des CDATA-Tags formuliert werden, wie in [9] thematisiert wird.

Enumeration. Im MP3-Shop Beispiel haben wir soweit programmiertechnische Lücken im XML-Parser des Cloud Anbieters untersucht. Eine genauso interessante Sicherheitsproblematik ergibt sich beim Anbieten von Dateien für Shop-Benutzer, die nicht jedem zugängig sein sollen und nur von Benutzern geladen werden dürfen, die auch tatsächlich die entsprechenden Dateien erworben haben. Diese Sicherheitsthematik beschränkt sich natürlich nicht nur auf unseren MP3-Shop, sondern ist für jeden Anbieter, der Content (MP3, Ebooks, Videos, ...) kostenpflichtig übers Internet anbietet relevant. Cloud Storage-Systeme bieten eine sehr kostengünstige Art und Weise Content übers Internet anzubieten, doch wie ist es um die Zugriffsicherheit beim Content bestellt?

Zunächst gibt es natürlich die Thematik der Sicherheit durch Verborgenheit. Dateien erhalten sehr lange Namen (bspw. Guids) und entsprechend auch lange Pfade, so dass die einzelnen Dateien nicht von jedermann erraten werden können. Das Problem hierbei liegt allerdings in der illegalen Verteilung solcher Pfade, die das System sehr gefährden kann. Weiterhin kann bei Containern (Bucket bei Amazon S3), die die Blobs und somit den Content enthalten, auch der gesamte Inhalt anhand seines Namens ausgelesen werden, was bei Amazon S3 mit dem so genannten *S3 Ripper* nach [9] tatsächlich möglich ist. Bei Windows Azure hängt es hingegen von den vergebenen Zugriffsrechten auf Container und Blobs ab, so dass im schlimmsten Fall hier eine Enumeration des Inhalt durch einen einfachen Browserbefehl möglich ist[2].

Zur Lösung der oben beschriebenen Sicherheitsproblematiken können unterschiedliche Mechanismen eingesetzt werden. Empfehlenswert nach [9] sind die so genannten *Shared Access Signatures* in Windows Azure und die *Signed URLs* in Amazon S3. Das Prinzip dahinter liegt in der Verwendung einer Zugriffssignatur. Dabei kann festgelegt werden, wie lange ein Zugriff möglich ist und welche Zugriffsrechte erlaubt sind. Über einen *Access Token* wird die Richtigkeit der Daten einer Signatur abgesichert. Im MP3-Shop Beispiel könnten wir so Downloads von Dateien nur für eine Stunde zulassen, so dass hier beim Verteilen der Links nur ein sehr begrenzter Schaden entstehen würde.

2.4 Risiken beim Cloud Provider

Der Cloud Provider bietet Benutzern vordefinierte Dienste nach dem Cloud-Modell an. Sind Sicherheitsprobleme bereits beim Cloud Provider vorhanden, so sind sie gleichermaßen für alle Benutzer aktuell. Hier muss aufseiten des Cloud Providers Aufwand investiert werden, um Probleme von vornherein zu vermeiden. Die folgenden Risiken können unter Anderem auftreten [14]:

Host Zugriff auf die Daten/Applikationen benachbarter Benutzer; Denial of Service; fehlerhafter Ressourcenzuweisung; Zugriffe auf den Host seitens externer Angreifer sowie durch andere Anbieter.

Netz Klassische netzbasierte Angriffe; verteilte Denial-of-Service Angriffe.

Virtualisierung Bedrohung von Privacy durch Verschiebung von Maschinen oder durch Datenreplica; Fehler-

[2]Enumerationen werden durch die REST API unterstützt.

doi: 10.2313/NET-2011-05-2_10

hafte Konfiguration und Sicherheitslücken in der Virtualisierungslösung.

3. ZUSAMMENFASSUNG

Cloud Computing bietet Unternehmen und Lösungsanbietern vielfältige Chancen die Wettbewerbsfähigkeit zu steigern, indem Innovationszeiträume verkürzt, neuartige Geschäftsmodelle ermöglicht und die generelle Wirtschaftlichkeit der eigenen IT-Systeme erhöht wird. Allerdings ist die Nutzung von Cloud Computing mit einer Vielzahl von Sicherheitsrisiken verbunden. So müssen die Sicherheitsproblematiken der IT-Compliance wahrgenommen und die Bedrohungen der Privatheit, Vertraulichkeit, Verfügbarkeit und Integrität entsprechend beachtet werden. Die Wahl des Cloud Providers gestaltet sich hierbei als nicht unproblematisch und muss deshalb wohlüberlegt getroffen werden. Schließlich ist die Auslagerung von IT-Architektur oder die Verlagerung von IT-Abläufen in die Cloud immer mit der Übergabe von Daten/Systemen in Besitz Dritter verbunden und sollte somit mit äußerster Vorsicht vonstattengehen.

Zur Minderung der Vorbehalte gegenüber der Sicherheit beim Cloud Computing wären Standardisierungsmaßnahmen von Vorteil, die cloudspezifisch ausgelegt neben der Risikominimierung auch das Vertrauen in die Cloud-Plattform steigern würden. Damit könnten derzeit zögernde Benutzer umgestimmt sowie weitere potentielle Cloud User gewonnen werden.

4. LITERATUR

[1] Google Mail - Ausfall statt höherer Verfügbarkeit. Golem Online: http://www.golem.de/0909/69510.html, September 2009.

[2] T-mobile, microsoft und das sidekick-desaster. Stern Online: http://www.stern.de/digital/online/cloud-computing-t-mobile-microsoft-und-das-sidekick-desaster-1514865.html, Oktober 2009.

[3] A Joint Report of the US Department of Homeland Security, SRI International Identity Theft Technology Council, and the Anti-Phishing Working Group. The crimeware landscape: Malware, phishing, identity theft and beyond. Online: http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf, Oktober 2006.

[4] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. Above the Clouds: A Berkeley View of Cloud Computing. UC Berkeley Reliable Adaptive Distributed Systems Laboratory: http://radlab.cs.berkeley.edu, Februar 2009.

[5] Avanade. Globale Avanade-Studie zeigt: Sicherheitsbedenken beim Cloud Computing bremsen Einzug der Technologie in Unternehmen - trotz wirtschaftlicher Vorteile. Online: http://www.avanade.com/de-de/about/avanade-news/press-releases/Documents/avanadecloudcomputingg250209877376.pdf, Februar 2009.

[6] E. Baize, R. Cloutier, B. Hartman, S. Herrod, C. Hollis, U. Rivner, and B. Verghese. Cloud Computing mit Sicherheit - Best Practices für vertrauenswürdige Umgebungen. RSA Serurity Brief, Online: http://www.rsa.com/innovation/docs/10764_CLWD_BRF_1009_DE.pdf, November 2009.

[7] BITKOM. Cloud Computing - Evolution in der Technik, Revolution im Business. Online http://www.bitkom.org/files/documents/BITKOM-Leitfaden-CloudComputing_Web.pdf, Oktober 2009. Seite 15.

[8] BSI. BSI-Mindestsicherheitsanforderungen an Cloud-Computing-Anbieter. Online: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Sonstige/Cloud_Computing_Mindestsicherheitsanforderungen.pdf?__blob=publicationFile, Oktober 2010.

[9] G. Bugher. Secure Use Of Cloud Storage. Online: http://media.blackhat.com/bh-us-10/whitepapers/Bugher/BlackHat-USA-2010-Bugher-Secure-Use-of-Cloud-Storage-wp.pdf, July 2010.

[10] ibi research. Vorstellung der Studienergebnisse: IT-Sicherheitsstandards und ITCompliance 2010. Online: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/3GS_Tag2010/IBI_Kronschnabel.pdf?__blob=publicationFile, Oktober 2010.

[11] IDC. IDC Enterprise Panel, August 2008. n=244.

[12] G. Kaefer. Cloud Computing Architecture. 4th Generation Datacenter IEEE Spectrum, http://www.sei.cmu.edu/library/assets/presentations/Cloud%20Computing%20Architecture%20-%20Gerald%20Kaefer.pdf, Februar 2009.

[13] T. Kleinz. Google Mail für Stunden offline. Focus Online: http://www.focus.de/digital/internet/google/it-ausfall-google-mail-fuer-stunden-offline_aid_374310.html, Dezember 2009.

[14] W. Streitberger and A. Ruppel. Cloud-Computing - eine Herausforderung für die Sicherheit, September 2009.