Fraunhofer
AISEC

FRAUNHOFER RESEARCH INSTITUTION AISEC

CLOUD COMPUTING SICHERHEIT

SCHUTZZIELE.TAXONOMIE.MARKTÜBERSICHT.

DR. WERNER STREITBERGER, ANGELIKA RUPPEL

09/2009

Fraunhofer AISEC
Parkring 4
D-85748 Garching b. München

Tel.: +49 (0)89-322-9986-0
Fax: +49 (0)89-322-9986-299
http://www.aisec.fraunhofer.de

Veröffentlicht am 25. September 2009
Stand der Studie: September 2009

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Executive Summary

Die vorliegende Studie zum Thema Cloud-Computing-Sicherheit zielt darauf ab, einen umfassenden Rahmen zur Betrachtung der Sicherheitsproblematik in Cloud-Computing-Systemen zu geben. Adressaten der Studie sind Entscheider in Unternehmen aller Branchen, die aktuell IT-Dienste ausgelagert haben, Cloud-Services bereits einsetzen oder in naher Zukunft einen Einsatz von Cloud-Services in Erwägung ziehen. Weitere Adressaten der Studie sind alle an der Thematik interessierten Personen sowie Anwender, die einen Überblick über Sicherheitsrisiken beim Einsatz von Cloud-Computing-Systemen und über aktuelle Cloud-Computing-Angebote sowie deren Kosten und Sicherheitslösungen gewinnen möchten.

Im Folgenden werden die Ergebnisse kurz vorgestellt und Hinweise gegeben, die aus Sicherheitssicht beim Einsatz von Cloud-Services beachtet werden sollten:

- Das Thema Sicherheit und Verfügbarkeit von Cloud-Computing-Systemen sind eine der wichtigsten Themen, die in jedem Cloud-Projekt betrachtet werden müssen. Fast jeder große Anbieter von Cloud-Services hatte in der Vergangenheit einen größeren Vorfall in einem der beiden genannten Gebiete.
- Kleine und mittlere Unternehmen (KMU) können ihre Sicherheit durch den Einsatz von Cloud-Services erhöhen, da sie zum einen die Möglichkeit haben, Sicherheitslösungen als Service von spezialisierten Anbietern beziehen zu können, und zum anderen von der Erfahrung des Anbieters in der Implementierung und im Betrieb von sicheren Services zu profitieren. Voraussetzung hierfür ist jedoch die Auswahl eines zertifizierten und vertrauenswürdigen Anbieters, dessen Cloud-Services auf Grundlage eines jederzeit überprüfbaren Service-Level-Agreements erbracht wird.
- Große Unternehmen sollten individuell die Sicherheitsfunktionen eines Cloud-Anbieters prüfen und im Einzelfall entscheiden, ob die verfügbaren Sicherheitsmechanismen für den konkreten Anwendungsfall ausreichend sind.
- Vorteile für den Einsatz von Cloud-Computing-Systemen basieren vor allem auf der Ausnutzung von Skaleneffekten zur Kosteneinsparung, der Möglichkeit, Kapazitäten dem aktuellen Bedarf anzupassen, und neuen Einsatzmöglichkeiten in der Organisation bestehender Prozesse.

- Risiken bestehen im Bereich der Sicherheit und Verfügbarkeit der Cloud-Services sowie möglichen Lock-In-Effekten, die bei der Auswahl eines Service auftreten können und hohe Kosten nach sich ziehen, wenn beispielsweise der Service eines Cloud-Anbieters gewechselt wird und durch geringe Standardisierung große Änderungen am bestehenden System vorgenommen werden müssen. Im Bereich Sicherheit und Verfügbarkeit sind die Schutzziele der IT-Sicherheit Vertraulichkeit, Integrität, Authentizität, Zurechenbarkeit, Verbindlichkeit, Verfügbarkeit und Schutz der Privatsphäre anzuwenden und während der Ableitung der Anforderungen festzulegen.
- Die Schutzziele der IT-Sicherheit lassen sich auch auf Cloud-Computing-Systeme übertragen. Sie sind jedoch für die genaue Betrachtung der Cloud-Computing-Systeme und ihre unterschiedlichen Ausprägungen zu allgemein, so dass sie für jeden Cloud-Service neu überprüft und angewandt werden müssen. Der Grund hierfür liegt in einer wenig standardisierten Vorgehensweise bei der Auswahl und dem Einsatz von Sicherheitstechnologien in Cloud-Computing-Systemen.
- Der Aufbau von Cloud-Computing-Systemen in seine vier Schichten Benutzer-, Software-, Plattform- und Infrastrukturschicht und die auf den Schichten agierenden Akteure bilden einen sehr komplexen Rahmen für die IT-Sicherheit. In dieser Studie werden alle wichtigen Schichten und Akteure vorgestellt, die je nach Anwendungsfeld und ausgewähltem Cloud-Service untersucht werden müssen.
- Für Cloud-Computing-Systeme werden zertifizierte Vorgehensmodelle und standardisierte Schnittstellen und Protokolle benötigt, die Cloud-Services zu Grunde liegen. Dies erhöht die Portabilität und Interoperabilität einzelner Cloud-Serviceangebote. Hierfür werden Standardisierungsgremien, Referenzimplementierungen und auf Cloud-Computing-Systeme angepasst Entwicklungsumgebungen benötigt.
- Die Cloud-Sicherheitstaxonomie gibt einen übersichtlichen Rahmen der Sicherheitsfelder, die beim Einsatz von Cloud-Services betrachtet werden sollten. Wegen der schnellen Weiterentwicklung der Technologien und der bestehenden Serviceangebote sollte die Anwendung der Cloud-Taxonomie projektbezogen erfolgen und die Gewichtung einzelner Sicherheitsfelder nach der jeweiligen Anforderung angepasst werden.
- Die aktuellen Cloud-Serviceangebote zeigen, dass vor allem im Bereich der Infrastruktur eine Reihe von Sicherheitstechnologien bereits zum Einsatz kommen. In den Bereichen Architektur, Verwaltung und Compliance ist die Unterstützung von Sicherheitstechnologien seitens der Cloud-Anbieter jedoch noch nicht soweit fortgeschritten, um die geforderten Schutzziele zu erreichen. Hier sind weitere, detaillierte Analysen notwendig, um heraus zu finden, welche aktuellen Technologien hier eingesetzt werden können und ob neue Technologien hierfür entwickelt werden

müssen. Es zeigt sich ein Trend, bestimmte Sicherheitsfunktionen wie beispielsweise Teile der Identitäts- und Zugangsverwaltung von spezialisierten Anbietern als Service zu beziehen.

- Im Bereich der Verwaltung sind Service-Level-Agreements ein wichtiger Bestandteile zur Festschreibung aller Rechte und Pflichten zwischen den Cloud-Benutzern und Cloud-Anbietern. Die bisher angebotenen standardisierten Service-Level-Agreements, die ein Cloud-Benutzer meist nicht frei verhandeln und nur akzeptieren oder ablehnen kann, geben nur minimale Garantien bezüglich der Dienstgüte eines Cloud-Services. Vor allem Sicherheitsgarantien sind nur rudimentär in diesen Service-Level-Agreements vorhanden und müssen ausgebaut werden, um die eingangs vorgestellten Schutzziele zu erreichen. Zusätzlich werden Systeme benötigt, die eine automatisierte Überwachung und Prüfung der vereinbarten Dienstgütekriterien zulassen.
- Aus Sicht der Compliance können Cloud-Services eingesetzt werden. Jedoch bleibt die Verantwortung der Daten meist beim Cloud-Benutzer, so dass dieser genaue Richtlinien definiert sollte, welche Daten wie in einem Cloud-Service abgespeichert und verarbeitet werden dürfen und welche Sicherheitsfunktionen vorhanden sein müssen. Auch aus rechtlicher Sicht sollte im Einzelfall überprüft werden, welche Einschränkungen bei bestimmten Daten gelten und die Verwendung eines Cloud-Services in Betracht gezogen werden kann.
- Die Marktübersicht der Studie gibt einen Überblick über ausgewählte Cloud-Serviceangebote, ihre Preise und Funktionen. Des Weiteren wird die Taxonomie des sicheren Cloud-Computing auf diese Cloud-Services angewandt und deren Sicherheitsfunktionen untersucht. Dabei lässt sich festhalten, dass die Informationen zu den implementierten Sicherheitsfunktionen durch die Cloud-Anbieter nur unzureichend dokumentiert sind. Häufig nimmt die Sicherheit bei der Vorstellung ihrer Angebote nur eine untergeordnete Rolle ein, so dass hier vor der Auswahl und Nutzung eines Cloud-Services beim Anbieter detaillierte Informationen angefordert werden sollten und eventuell ein Proof-of-Concept vor dem eigentlichen Produktiveinsatz eines Cloud-Services realisiert werden sollte.

2 Einführung

Das Thema Cloud-Computing hat für Unternehmen in den vergangenen Jahren eine zunehmende Bedeutung erlangt und dazu geführt, dass Cloud-Services bereits in einer Vielzahl von Anwendungen für Endbenutzer eingesetzt werden [26]. Die Motivation für Unternehmen, sich mit Cloud-Computing zu beschäftigen, begründet sich in den ständig wandelnden Herausforderungen, die mit einer wachsenden Dynamik des Marktes und einer zunehmenden Wettbewerbssituation einhergehen. Dies hat zur Folge, dass eine stetige Anpassung und Überprüfung des eingesetzten Wissens, der Technologie und insbesondere des eigenen Ressourceneinsatzes notwendig sind.

In Unternehmen hat sich der Einsatz von rechenintensiver Informationstechnologie (IT) bereits für den Geschäftsbetrieb als unverzichtbar erwiesen, um Geschäftsprozesse besser auszurichten und neue Geschäftslösungen mit größerer Flexibilität und höherer Geschwindigkeit bereitzustellen. Dieser Situation gegenüber stehen die Kosten für die Anschaffung, den Betrieb und die Wartung der IT. Diese Kosten rechtfertigen jedoch nur selten die vollständige Abdeckung des maximal erwarteten Bedarfs von Software und Ressourcen wie Speicher- und Rechenleistung. So müssen Unternehmen neben Effizienz- und Geschwindigkeitsverbesserungen auch Kosteneinsparungen und Verbesserung der IT-Sicherheit für ihre Infrastruktur realisieren, um wettbewerbsfähig zu bleiben.

Cloud-Computing kann hierzu der nächste Schritt sein, IT-Dienste zu verbessern und bestehende Kapazitäten besser auszulasten. Das hinter Cloud-Computing stehende Konzept beschreibt verschiedene Lösungsansätze zur Umsetzung einer dynamischen Nutzung von IT-Ressourcen wie Speicherkapazität oder Rechenleistung und Diensten innerhalb eines Unternehmens und über Unternehmensgrenzen hinweg. Cloud-Computing-Systeme ermöglichen es, Infrastrukturressourcen und Anwendungsdienste bei Bedarf als IT-Service zu beziehen und damit Dienstleistungen in die Cloud auszulagern.

Im Cloud-Computing-Paradigma werden Informationen auf Rechnern im Internet gespeichert und auf diesen Rechnern Softwareanwendungen ausgeführt [18]. Diese werden den Benutzern auf Anforderung zur Verfügung gestellt [27]. Die Informationstechnologie zur Bereitstellung der Daten und Anwendungen wird häufig von speziellen Anbietern betrieben, die Konfiguration erfolgt meist durch den Benutzer über einen Web-Browser [23].

Da es sich bei Cloud-Computing-Systemen um ein sich kontinuierlich weiterentwickelndes Paradigma handelt, ist es zum aktuellen Zeitpunkt[1] nicht möglich, eine endgültige Definition für den Begriff Cloud-Computing zu geben. Im Rahmen dieser Studie wird auf eine Arbeitsdefinition des National Institute of Standards and Technology (NIST) zurückgegriffen, die in regelmäßigen Abständen aktualisiert und weiterentwickelt wird [28]. Das NIST definiert Cloud-Computing als ein Modell, das einen komfortablen, bedarfsabhängigen und netzbasierten Zugriff auf eine gemeinsam benutze Menge konfigurierbarer Rechenressourcen (z. B. Netzwerk, Server, Speicher, Anwendungen und Dienste) ermöglicht, die schnell, mit geringem Verwaltungsaufwand und ohne (menschliche) Interaktion mit einem Anbieter bereitgestellt und wieder freigegeben werden können. Dieses Modell unterstützt die Verfügbarkeit der Ressourcen.

In Ergänzung dazu, definiert das NIST Cloud-Computing-Systeme über deren Charakteristika, sowie deren Nutzungs- und Bezugsmodelle. Die 5 grundlegenden Charakteristika von Cloud-Computing-Systemen werden in diesem Kapitel vorgestellt, die Nutzungs- und Bezugsmodelle von Cloud-Computing-Systemen werden in Kapitel 4 detailliert betrachtet. Nach Mell und Grance [28] sind die 5 grundlegenden Charakteristika von Cloud-Computing-Systemen Bedarfsbetrieb mit Selbstbedienung, breit verfügbarer Netzwerkzugriff, Ressourcenpoolbildung, schnelle Elastizität und überwachte Serviceausführung (siehe Abbildung 2.1):

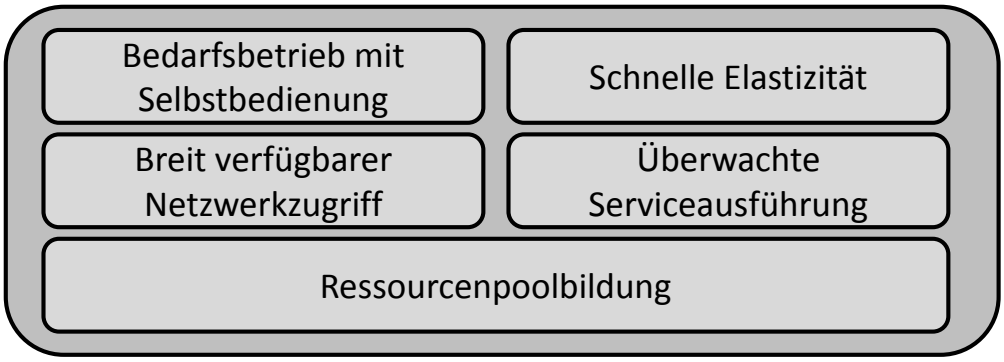

Abbildung 2.1: Grundlegende Charakteristika von Cloud-Computing-Systemen

- Bedarfsbetrieb mit Selbstbedienung: Ein Cloud-Konsument kann unilateral Ressourcen eines Cloud-Computing-Systems wie beispielsweise Rechenleistung oder Speicherplatz nach seinem aktuellen Bedarf selbst anfordern, ohne dass eine menschliche Interaktion mit einem Serviceanbieter erfolgen muss.
- Breit verfügbarer Netzwerkzugriff: Die Ressourcen eines Cloud-Computing-Systems sind über ein Netzwerk verfügbar und werden durch Standardverfahren zugegriffen, die heterogene Endbenutzerplattformen (z. B. Mobiltelefone, Laptops und PDAs) fördern und unterstützen.
- Ressourcenpoolbildung: Die Rechen- und Speicherressourcen eines Cloud-Computing-Anbieters sind zu einem Ressourcenpool zusammengefasst, aus dem verschiedene Konsumenten mit einem Mehrmandantenmodell

[1] Stand: September 2009

bedient werden, wobei verschiedene physische und virtuelle Ressourcen dynamisch und nach Bedarf des Cloud-Konsumenten zugewiesen und angepasst werden. Es gibt in Cloud-Computing-Systemen eine Ortsunabhängigkeit der Art, dass ein Cloud-Konsument keine Kontrolle und kein Wissen über den exakten Ort der bereitgestellten Ressourcen hat, er jedoch möglicherweise den Ort auf einer höheren Abstraktionsebene spezifizieren kann (z. B. Land, Region oder Rechenzentrum). Ressourcenbeispiele sind Speicherkapazität, Rechenleistung, Hauptspeicher, Netzwerkbandbreite, virtuelle Maschine und Dienstinstanz.

- Schnelle Elastizität: Die Ressourcen eines Cloud-Computing-Systems können schnell, elastisch und in einigen Fällen auch vollständig automatisiert bereitgestellt werden, um schnell Ressourcen sowohl nach oben als auch nach unten zu skalieren. Für den Cloud-Konsumenten erscheinen die verfügbaren Ressourcen eines Cloud-Computing-Systems als nahezu unbegrenzt und zu jeder Zeit und fast beliebiger Menge anmietbar.
- Überwachte Serviceausführung: Cloud-Computing-Systeme überwachen automatisiert die Serviceausführung und optimieren optional die Ressourcennutzung, indem sie ihre Messfähigkeiten auf verschiedener Abstraktionsebene abhängig vom Servicetyp (z. B. Speicher, Rechenleistung, Bandbreite, Benutzerprofil) passend einsetzen. Der Ressourcenverbrauch kann überwacht, kontrolliert und berichtet werden und damit für Transparenz sowohl für den Anbieter als auch für den Konsumenten eines Cloud-Services sorgen.

Die 5 grundlegenden Kriterien von Cloud-Computing-Systemen werden im Folgenden auf Grid-Computing-Systeme und Cluster-Computing-Systeme angewandt, um eine Abgrenzung von diesen Systemen darzustellen. Alle drei Systeme sind verteilte Systeme mit ähnlichen Eigenschaften, die in Tabelle 2.1 zusammenfassend gezeigt werden. Die Gemeinsamkeiten beziehen sich auf die Kriterien Ressourcenpoolbildung und den breit verfügbaren Netzwerkzugriff, den alle Systeme erfüllen. Der Netzwerkzugriff erfolgt auf Cluster- und Grid-Computing-Systeme meist von innerhalb eines Unternehmensnetzwerks aus, während auf Dienste eines Cloud-Computing-Systems auch über öffentliche Netzwerke, wie das Internet, zugegriffen werden kann.

Unterschiede zwischen Cloud-Computing-Systemen auf der einen Seite und Grid-Computing-Systemen und Cluster-Computing-Systemen auf der anderen Seite lassen sich auf die Dynamik der Systeme zurückführen. In Grid- und Cluster-Umgebungen findet meist eine Vorreservierung von Ressourcen statt, während Cloud-Computing-Systeme bedarfsgetrieben sind, d. h. der Betrieb der Cloud-Computing-Systeme ist am Bedarf des Konsumenten ausgerichtet. Ebenfalls ist ein Unterschied bei dem Kriterium schnelle Elastizität zu erkennen, das integraler Bestandteil von Cloud-Computing-Systeme ist und üblicherweise nicht von Cluster- und Grid-Systemen unterstützt wird. Eine Überwachung der Servicenutzung findet meist nur in Grid- und Cloud-Computing-Systemen statt,

Tabelle 2.1: Vergleich der verteilten Systeme Cluster-Computing, Grid-Computing und Cloud-Computing

	Cluster	Grid	Cloud
Bedarfsbetrieb mit Selbstbedienung	nein	nein	ja
breit verfügbarer Netzwerkzugriff	ja	ja	ja
Ressourcenpoolbildung	ja	ja	ja
schnelle Elastizität	nein	nein	ja
überwachte Servicenutzung	nein	ja	ja

während Cluster-Umgebungen bei der Überwachung der Servicenutzung meist nur rudimentäre Funktionen bereitstellen.

Unternehmen erhalten mit Cloud-Computing-Systemen im Vergleich zu anderen verteilten Systemen wie Grid- und Cluster-Lösungen eine deutlich flexiblere Lösung. Sie können auf eigene IT-Infrastrukturen verzichten und müssen lediglich für die tatsächlich genutzten Ressourcen und Dienstleistungen aufkommen. Diese können dynamisch an die aktuellen Geschäftsanforderungen und -prozesse angepasst werden. Als Basistechnologien hierfür dienen Virtualisierungstechnologien und dienstorientierte, verteilte Softwaresysteme.

Jedoch gehen mit dem Einsatz von Cloud-Computing-Systemen eine Reihe von Sicherheitsrisiken einher, deren Ursachen meist auf mangelnden Einsatz und Unterstützung von Sicherheitstechnologien zurückzuführen sind. Auch neu zu entwickelnde oder nicht ausgereifte Technologien können eine sichere Benutzung von Cloud-Computing-Systemen verhindern [22]. Dies schränkt aktuell den Einsatz von Cloud-Computing-Systemen ein und erfordert eine detaillierte Betrachtung der Sicherheitsrisiken, da der Benutzer sichere Cloud-Services erwartet, die vergleichbare Sicherheitsanforderungen wie die bisher eingesetzten Systeme erfüllen. Diese Risiken können – beispielsweise bei Diebstahl vertraulicher Informationen – signifikanten Einfluss auf das Geschäftsmodell des jeweiligen Benutzers haben.

Nach einer aktuellen Studie des Beratungsunternehmens IDC[2] ist die Sicherheit von Cloud-Services eine der wichtigsten Gründe warum Cloud-Computing-Systeme nicht in Unternehmen eingesetzt werden. Die Sicherheit wird als eines der wichtigsten Kriterien neben der Verfügbarkeit und den Kosten angeführt, das sichergestellt werden muss, damit Cloud-Services als Alternative zu bestehenden Outsourcing-Angeboten in voller Breite eingesetzt werden können. Da sich bisher nur wenige Unternehmen in Deutschland mit dem Thema auseinander gesetzt haben, ist zu erwarten, dass die Bedeutung der Sicherheit von Cloud-Services in Zukunft noch zunehmen wird.

[2]Weitere Informationen über die Studie findet sich in der Pressemitteilung von IDC vom 2.6.2009: `http://www.idc.com/germany/press/presse_cloudcomp.jsp`

In Tabelle 2.2 werden wichtige Unterschiede zwischen klassischen Outsourcinglösungen und Cloud-Computing-Systemen als eine weitere Outsourcing-Lösung betrachtet. Unter dem Begriff IT-Outsourcing wird die Auslagerung der gesamten IT oder Teilen davon an externe Anbieter verstanden. Das klassische IT-Outsourcing reicht vom selektiven bis zum totalen Outsourcing. Während beim selektiven Outsourcing nur einzelne IT-Funktionen an Drittanbieter ausgelagert werden, wird beim totalen Outsourcing die gesamte IT ausgelagert. Daher kann sich je nach Variante die Infrastruktur und Software entweder beim Kunden oder dem Anbieter befinden, wobei die Systemverwaltung vom Anbieter durchgeführt wird.

Tabelle 2.2: Vergleich von IT-Outsourcing und Cloud-Computing

Merkmale	**Klassisches IT-Outsourcing**	**Cloud-Computing-Systeme**
Technologiestandort	Kunde oder Anbieter	Anbieter
Geschäftsprozess-anpassung	Anbieter	Kunde
Vertragslaufzeit	mittel- bis langfristig	kurz- bis langfristig

Tabelle 2.2 listet die drei wesentlichen Unterschiede anhand der Merkmale Technologiestandort, Geschäftsprozessanpassung und Vertragslaufzeit zwischen klassischem IT-Outsourcing und Cloud-Computing auf. Infrastruktur und Software können sich beim IT-Outsourcing sowohl beim Kunden als auch beim Anbieter befinden. Beim Einsatz von Cloud-Computing-Systemen befindet sich sowohl die Infrastruktur als auch die Software beim Anbieter. Ein weiterer Unterschied existiert in der Anpassung der Anwendungen an die Geschäftsprozesse. Während beim klassischen IT-Outsourcing der Anbieter die Anwendung an die Geschäftsprozesse anpasst, muss der Kunde dies beim Cloud-Computing selbst durchführen, da der Cloud-Anbieter nur die Dienste bereitstellt und deren Betrieb verantwortet. Abhängig von dem Umfang der Auslagerung und der Anpassung der Anwendungen an die Geschäftsprozesse, kann es beim IT-Outsourcing zu Lock-in Effekten kommen, die aus der meist sehr langen Laufzeit der Verträge resultieren können. Das klassische IT-Outsourcing ist durch ein mittel- bis langfristiges Vertragsverhältnis gekennzeichnet, während bei Cloud-Computing-Systemen meist Verträge mir kurzer Laufzeit zustandekommen.

In den folgenden Abschnitten werden die Sicherheitsaspekte verschiedener Endbenutzergruppen von Cloud-Computing-Systemen kurz diskutiert und dabei der Frage nachgegangen, ob das IT-Sicherheitsniveau von unternehmensinternen Sicherheitslösungen erreicht werden kann. Anschließend werden die am häufigsten genannten Vorteile und Risiken von Cloud-Systemen präsentiert und der weitere Aufbau der Studie vorgestellt.

2.1 Sicherheitsaspekte in Cloud-Computing-Systemen

Die IT-Sicherheit der Daten, Prozesse und Anwendungen stellt eines der wichtigsten Problemfelder dar, die für Cloud-Services angegangen werden müssen [26]. Solange Unternehmen keine ausgereiften Sicherheitslösungen einsetzen können, die den 5 grundlegenden Charakteristika von Cloud-Computing-Systemen angepasst sind und diese unterstützen, ist es für sie nur schwer möglich, das volle Potential der Cloud-Services zu nutzen.

Durch den Einsatz von Cloud-Computing-Systemen werden die Sicherheits- und Verfügbarkeitsrisiken für Nutzer von Cloud-Diensten zunehmend intransparent [37]. Gleichzeitig geht durch den hohen Automatisierungsgrad der Cloud-Computing-Systeme ein Kontrollverlust einher, so dass ein Cloud-Konsument nur einen geringen Einfluss auf z. B. den geografischen Ort seiner Daten oder die Zuweisung der Ressourcen hat.

Durch die zunehmende Verbreitung von Cloud-Diensten treten neue Schwachstellen und Bedrohungen der IT-Sicherheit auf, die bei dem Einsatz dieser Systeme berücksichtigt werden müssen. Diese neuen Schwachstellen können zum einen auf Angreifer zurückgeführt werden, die die Rolle eines Konsumenten im Cloud-Computing-System wahrnehmen und Zugriff auf Daten eines anderen Konsumenten erlangen und zum anderen ihren Ursprung in der Komplexität und Dynamik von Cloud-Computing-Systemen haben, die sich in einem ständigen Wandel bedingt durch Ausfälle oder Wartungsarbeiten befinden. Zusätzlich müssen neue Verfahren zur Bewältigung der Risiken evaluiert und die Cloud-Computing-Systeme hinsichtlich ihrer Einhaltung von Gesetzen und Richtlinien überprüft werden. Aktuell unterstützen nur wenige Cloud-Anbieter eine Überprüfung der Prozesse nach vorher festgelegten Sicherheitsrichtlinien [35].

Dies wirft die Frage auf, ob der Einsatz von Cloud-Services ein Absenken des Sicherheitsniveaus erwarten lässt oder ob vielleicht doch eine Verbesserung der IT-Sicherheit durch den Einsatz von Cloud-Services erreicht werden kann. Zentral für die Frage sind die unterschiedlichen Sichtweisen der Anwendergruppen von Cloud-Services. Endbenutzer aus dem Bereich kleiner und mittelgroßer Unternehmen haben häufig nicht die Möglichkeiten detaillierte Sicherheitsrichtlinien für ihr Unternehmen auszuarbeiten und auch nicht die Expertise diese Sicherheitsrichtlinien durchzusetzen[3][4][5]. Für diese Gruppe von Anwendern kann argumentiert werden, dass der Einsatz von Cloud-Services eine Verbesserung ihres bisherigen Sicherheitsniveaus bedeuten kann, da es zu den Kernaufgaben des Cloud-Anbieters gehört, adäquate Sicherheitsmechanismen zu implementieren. Es wird angenommen, dass State-of-the-Art Sicherheitstechnologien und

[3] http://www.ihotdesk.com/article/19055538/SME-security-could-benefit-from-cloud-computing-source-claims

[4] http://www.scmagazineus.com/sme-security-sme-mindset-must-change/article/136052/

[5] http://www.rationalsurvivability.com/blog/

die entsprechenden Prozesse von besonders geschultem Personal des Cloud-Anbieters umgesetzt werden.

Als Gegenargument lässt sich jedoch anführen, dass der Einsatz von Cloud-Services vor allem bei großen Unternehmen stark von den möglichen Kosteneinsparungen getrieben wird und die Anbieter von Cloud-Services versuchen, ihre Dienstleistungen möglichst kostengünstig anzubieten und dabei auf den Einsatz bestimmter Sicherheitsfunktionen verzichten. In einem solchen Szenario kann es zu einer Verringerung des Sicherheitsniveaus kommen, was potentielle Bedrohung der Daten, Prozesse und Anwendungen in der Cloud nach sich ziehen kann. Unternehmen müssen eine Anpassung bestehender Sicherheitssysteme vornehmen, so dass sie auch Cloud-Services mit in ihr Sicherheitskonzept einbeziehen.

In beiden Szenarien müssen neue Konzepte und Verfahren entwickelt werden, die potentielle Sicherheitsrisiken identifizieren können und geeignete Technologien bereitstellen, Bedrohungen zu reduzieren. Idealerweise wird schon beim Entwurf einer Anwendung, ein möglicher Einsatz von Cloud-Services mit einbezogen und die Sicherheitsanforderungen in allen Phasen des Softwareentwicklungszyklus berücksichtigt. Dabei sind die Kosten zu berücksichtigen, die zusätzliche Sicherheitsmechanismen verursachen, sei es durch Zukauf von Dienstleistungen externer Anbieter oder eine direkte Integration in die Anwendungen. Gleichzeitig gibt es einen Mangel an standardisierten Sicherheitstechnologien und Best-Practice-Ansätzen, die eine Bewertung der Sicherheit von Cloud-Services zusätzlich erschweren. Es ist zu erwarten, dass die Sicherheitslösungen für Clouds ähnliche Charakteristika wie die Cloud-Systeme selbst hinsichtlich Skalierbarkeit, Dynamik, Fehlertoleranz und Offenheit ausweisen müssen, um die Skaleneffekte, die durch Cloud-Services ermöglicht werden, zu internalisieren.

Die grundlegenden Herausforderungen der Sicherheitslösungen für Cloud-Services haben ihren Ursprung in den Informationsasymmetrien zwischen den Benutzern und den Anbietern von Cloud-Services. Bei Abschluss eines Vertrags verfügt ein Cloud-Anbieter über mehr Informationen über beispielsweise den Zustand seines Systems als der Benutzer des Cloud-Services. Diese Lücke ist in Cloud-Computing-Systemen besonders groß, da der Benutzer sehr wenig Informationen und Einfluss über die Bereitstellung und Dienstleistungserbringung des Anbieters hat, während der Anbieter sehr detaillierte Informationen darüber besitzt. Die Sicherheitskonzepte für Cloud-Services müssen dazu beitragen, diese Informationsasymmetrien zu verringern, was bedeuten kann, dass dem Benutzer der Zugang zu den Überwachungs- und Messdaten gewährt wird oder eine automatisierte Überprüfung der Sicherheitsfunktionen des Anbieters durch einen vertrauenswürdigen Dritten erfolgt, der die Komplexität des Cloud-Computing-Systems bewerten kann.

Das Ziel der Studie ist, ausgehend von der eingangs aufgeworfenen Frage, ob Cloud-Computing-Systeme mehr Sicherheit für Cloud-Benutzer bieten können, eine Einführung in den Aufbau von Cloud-Computing-Systemen zu geben und

an dessen Aufbau eine mögliche Kategorisierung der Sicherheitsfelder zu definieren, die alle wichtigen Felder, die speziell in Cloud-Computing-Systemen betrachtet werden müssen, aufzeigt. Dieser neuartige Rahmen hilft Unternehmen, die Sicherheitsrisiken besser zu identifizieren und einen strategischen Einsatz von Cloud-Services aus Sicherheitssicht zu betrachten. Exemplarisch wird an ausgewählten Cloud-Services diese Taxonomie angewandt und die aktuell vorhandenen Sicherheitsfunktionen einer Bewertung unterzogen.

2.2 Vorteile und Risiken von Cloud-Services

Unternehmen, die erwägen Cloud-basierte Services einzusetzen, müssen die damit verbunden Risiken identifizieren und verstehen. Dies ist die Grundlage, um detaillierte Szenarien zu definieren und die notwendigen Kontrollen zur Behandlung der Risiken einzuführen, die Unternehmen üblicherweise anwenden, um mit vertraulichen und gesetzlich regulierten Informationen umzugehen. Cloud-Computing-Systeme weisen dabei die gleichen Risiken wie jeder extern erbrachte IT-Service auf. Darüber hinaus gibt es Themen wie beispielsweise Datenintegrität, Wiederherstellung der Daten und Prozesse, den Schutz der Privatsphäre oder spezielle gesetzliche Anforderungen, die besondere Bedeutung in Cloud-Computing-Systemen haben und in die Sicherheitsbetrachtung mit einbezogen werden müssen.

Aus Sicherheits- und Risikoperspektive zielen Cloud-Services darauf ab, dem Benutzer durch Automatisierung der Servicebereitstellung eine detaillierte Kontrolle über die Daten und Prozesse zu entziehen und damit zunehmend intransparent für den Benutzer zu werden. Vor allem die Optimierung der Ressourcen durch den Anbieter kann zu einer nicht-autorisierten Verarbeitung der Kundendaten führen, bei der die Daten getrennt verarbeitet und anschließend an verschiedenen Orten abgespeichert werden.

Demgegenüber stehen die Chancen, die mit dem Einsatz von Cloud-Computing-Systemen einhergehen und meist ökonomisch begründet sind. Ein Unternehmen kann durch den Einsatz von Cloud Services eine Verbesserung der Ressourcenauslastung und der Geschäftsprozesse erreichen und eine verbesserte IT-Flexibilität erwarten. Häufig genannte Vorteile für den Einsatz von Cloud-Computing-Systemen sind:

- Geringere Investitionsrisiken: Der Anbieter trägt die Kosten für die Anschaffung von Software oder IT-Infrastrukturkomponenten und übernimmt damit auch das Investitionsrisiko, während Kunden nur für die aktuelle Nutzung oder den tatsächlichen Verbrauch zahlen.
- Bessere Performanz und Sicherheit: Spezialisierten Providern, für die der Betrieb der Informationstechnologie das Kerngeschäft ist, stehen in der Regel mehr Ressourcen für die Sicherstellung von Performanz und Sicherheit zur Verfügung. Diese zusätzlichen Ressourcen können zu einer Verbesserung der Sicherheit beitragen.

- Skalierbare und flexible IT-Infrastruktur: Cloud-Computing-Systeme geben den Unternehmen die Möglichkeit, dynamische Ressourcen bei Bedarf zu bestehenden Ressourcen hinzuzufügen und wieder freizugeben. Mögliche Projektziele hängen damit nicht mehr davon ab, ob genügend Rechenleistung oder Speicherkapazität vorhanden ist. Häufig werden Service-Level-Agreements eingesetzt, um die Leistung zu messen und zu optimieren.
- Reduzierte Betriebskosten: Cloud-Computing-Systeme setzen Verfahren aus dem Autonomic-Computing ein, wie beispielsweise Self-Healing. Dies führt zu hoher Verfügbarkeit und zur Fähigkeit der selbständigen Optimierung des Systems. IT-Systemadministratoren werden dadurch von einfachen Aufgaben entlastet und können sich auf komplexere Aufgaben konzentrieren.
- Effizienter Einsatz bestehender Hardware und Ressourcen: Durch die verteilte Natur der Cloud-Computing-Systeme kann es unternehmensweit dazu verwendet werden, große Mengen ungenutzter IT-Infrastrukturkapazitäten zu nutzen und die Anschaffung von neuer Hardware auf ein Minimum zu verringern.

Für die Anbieter von Cloud-Services liegt der Reiz in der hohen Skalierbarkeit, die es ermöglicht, Skaleneffekte durch Standardisierung zu erzielen. Zwar entstehen höhere Fixkosten beim Aufbau der Infrastruktur, die variablen Kosten durch Wartung und Support fallen jedoch wesentlich geringer aus. Aus technischer Sicht werden Cloud-Computing-Systeme durch Virtualisierungstechnologien und -konzepte unterstützt, die es möglich machen, Ressourcen in einem gemeinsamen Ressourcenpool zu nutzen.

Mithilfe von Virtualisierungstechnologien werden physikalische IT-Ressourcen dabei in logische Einheiten aufgeteilt, die unterschiedlichen Benutzern zur Verfügung stehen und somit eine gleichzeitige Nutzung der Ressourcen durch verschiedene Benutzer ermöglichen. Ein Cloud-Service bekommt keinen bestimmten Server oder Speicherplatz mehr exklusiv zugeteilt, sondern nur ein von der Hardware abstrahiertes Ressourcenbündel wie beispielsweise eine virtuelle Maschine. Bei Bedarf werden zusätzliche, freie Kapazitäten aus einem Ressourcenpool zur Verfügung gestellt. Dies bedeutet, dass mehrere Kunden logisch getrennt über eine gemeinsam genutzte Infrastruktur bedient werden können. Ein Anbieter von Cloud-Services kann somit seine Infrastruktur besser auslasten.

2.3 Cloud-Computing-Szenarien

Cloud-Computing-Systeme können sehr flexibel in verschiedenen Szenarien eingesetzt werden, wie die Arbeiten der Cloud Computing Use Case Discussion Group zeigen [8]. Die beiden Szenarien, die für die vorliegende Studie wichtig sind, werden im weiteren Verlauf dieses Kapitels näher erläutert und ihre Anforderungen vorgestellt. Abbildung 2.2 stellt die Szenarien grafisch dar. Das erste

Szenario betrachtet die Sichtweise eines Endbenutzers, der einen Cloud-Service benutzt und das zweite Szenario die Sichtweise eines Unternehmens, das auf Ressourcen eines Cloud-Computing-Systems zurückgreift und einsetzt.

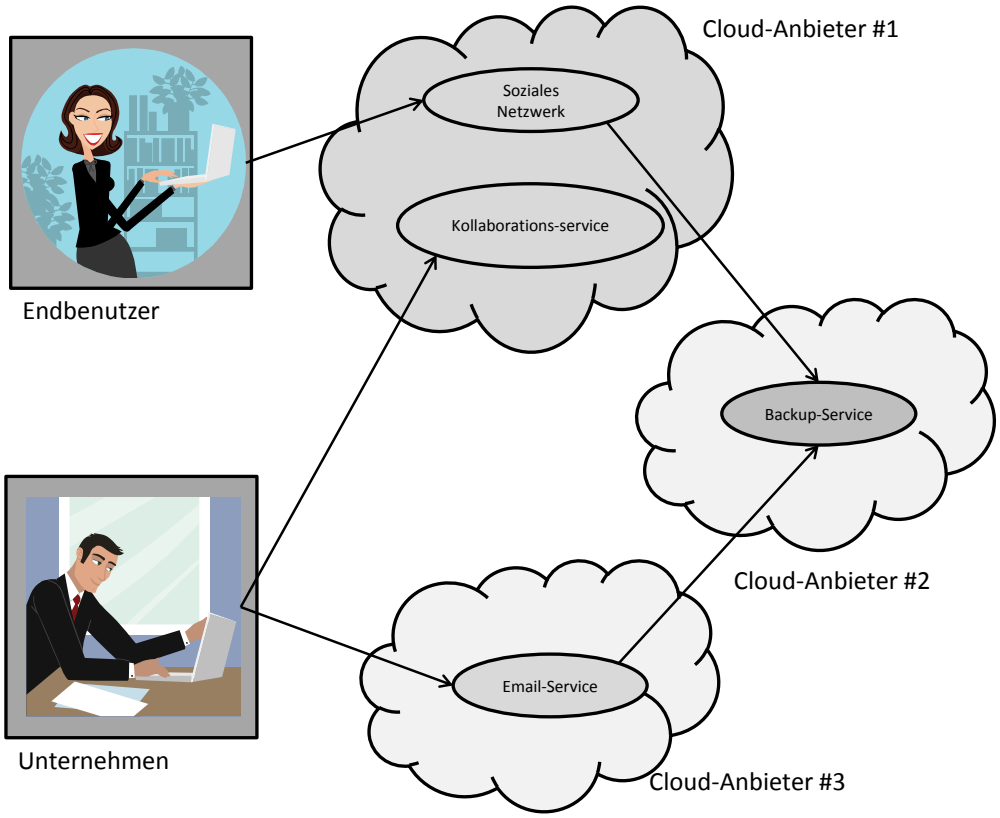

Abbildung 2.2: Die Cloud-Szenarien Endbenutzer – Cloud und Unternehmen – Cloud

Szenario 1: Endbenutzer – Cloud In diesem Szenario greift ein Endbenutzer auf Daten oder Anwendungen in einem Cloud-Computing-System zu. Häufig genutzte Anwendungen sind in diesem Szenario beispielsweise Email-Lösungen wie GoogleMail oder Webseiten sozialer Netzwerke (z. B. Facebook oder Twitter), auf die Endbenutzer über einen Webbrowser von fast jedem beliebigen Endgerät aus zugreifen und ihre Daten abrufen oder verändern können. Ein Endbenutzer authentifiziert sich über den Benutzernamen und das dazugehörige Passwort gegenüber dem Cloud-Service; seine Daten sind in einem Cloud-Computing-System gespeichert und werden auch dort verwaltet. Ein wichtiger Punkt in diesem Szenario ist, dass der Endbenutzer kein Wissen über die darunterliegende Architektur besitzt. Sobald er eine Internetverbindung hat, möchte er auf seine Daten unabhängig z. B. vom geografischen Ort oder technischen Einschränkungen zugreifen können.

Die wichtigsten Anforderungen in Szenario 1 sind:

- Identität: Der Cloud-Service muss einen Endbenutzer authentifizieren.
- Offener Zugriff: Die Nutzung des Cloud-Services sollte keine bestimmte Plattform oder Technologie benötigen, die den Zugriff auf den Cloud-Service einschränkt.

- Sicherheit: In einem Szenario zwischen Endbenutzer und Diensten eines Cloud-Computing-Systems sollten Standard-Sicherheitsverfahren, wie eine verschlüsselte Verbindung zum Cloud-Service, Möglichkeiten zur Konfiguration des Schutzes der Privatsphäre und weitere Sicherheitsaskpekte, vorhanden sein, die im Rahmen dieser Studie näher betrachtet werden.
- Service-Level-Agreements (SLAs): Obwohl die Service-Level-Agreements für Endbenutzer üblicherweise viel einfacher sind als diejenigen für Unternehmen, müssen Cloud-Anbieter auch für Endbenutzer ihrer Services möglichst präzise Aussagen darüber treffen, welche Leistungen ihr Dienst einem Endbenutzer bereitstellt und mit welchen Einschränkungen zu rechnen ist. Ein Endbenutzer sollte die SLAs verschiedener Cloud-Services vergleichen, bevor er einen Service auswählt.

Szenario 2: Unternehmen – Cloud Dieses Szenario betrachtet ein Unternehmen, das Cloud-Services in seinen internen Prozessen einsetzt und das häufigste Szenario für die Cloud-Nutzung ist [8]. Eine weitere Variante dieses Szenarios ist die Verwendung von Diensten eines Cloud-Computing-Systems durch ein Unternehmen mit dem Ziel, Cloud-Services nicht nur für die unternehmensinternen Prozesse einzusetzen, sondern diese auch externen Akteuren wie beispielsweise Geschäftspartnern oder Endbenutzern zur Verfügung zu stellen. Ein Unternehmen kann in Szenario 2 beispielsweise Cloud-Speicherdienste für die Datensicherung, virtuelle Maschinen in der Cloud zur Erweiterung ihrer Rechenkapazitäten und Auffang von Spitzenlasten oder Anwendungen in der Cloud für bestimmte Unternehmensprozesse (z. B. Email, Kalender, CRM, Kollaboration, usw.) einsetzen.

Die wichtigsten Anforderungen, die sich aus Szenario 2 ergeben, sind:

- Identität und Identitätsverwaltung: Der Cloud-Service muss den Benutzer authentifizieren. Da ein Benutzer, der einem Unternehmen angehört, häufig schon eine Identität innerhalb eines Unternehmens besitzt, sollte diese auch für den Zugriff auf Dienste eines Cloud-Computing-Systems verwendet werden. An dieser Stelle sind gegebenenfalls weitere Sicherheitsanforderungen z. B. zum Schutz der Privatsphäre des Benutzers zu beachten.
- Offener Zugriff: Die Nutzung des Cloud-Services sollte keine bestimmte Plattform oder Technologie benötigen, die den Zugriff auf den Cloud-Service einschränkt.
- Ortsbezug: Cloud-Anbieter übernehmen im Auftrag des Unternehmens verschiedene Verwaltungs- und Administrationsaufgaben, die auch die Zuweisung der Daten und Anwendungen zu den physischen Ressourcen des Cloud-Computing-Systems beinhaltet. Hieraus können sich sicherheitsrelevante Anforderungen ergeben, wenn beispielsweise Daten Ländergrenzen überschreiten. Es sollte deshalb für ein Unternehmen immer

nachvollziehbar bleiben, in welchen Rechenzentren ihre Daten und Anwendungen geografisch aufzufinden sind.

- Verbrauchsmessung und Überwachung: Alle Cloud-Services sollten während ihrer Ausführung überwacht und bezüglich ihres Verbrauchs gemessen werden, um den Verbrauch abrechnen zu können und Vertragsverletzung und Sicherheitsprobleme feststellen zu können.
- Sicherheit: Wie bereits in den vorangegangenen Abschnitten erwähnt, stellt die Sicherheit von Cloud-Computing-Systemen eine große Herausforderung dar. Anforderungen bezüglich der Sicherheit müssen die 5 Charakteristika von Cloud-Computing-Systemen berücksichtigen. Die Sicherheitsaspekte von Cloud-Computing-Systemen stehen in Fokus dieser Studie und werden im weiteren Verlauf detailliert betrachtet.
- Interoperabilität und Portabilität: Anwendungen, Daten und virtuelle Maschinen sollten zwischen den verschiedenen Cloud-Computing-Systemen der Cloud-Anbieter portabel sein. Dazu wird eine einheitliche, möglichst standardisierte Menge an Schnittstellen für den Zugriff auf Cloud-Services, wie beispielsweise Speicherdienste oder Middleware- bzw. Plattformdienste, benötigt, um Lock-in-Effekte zu vermeiden und Cloud-Services verschiedener Anbieter verknüpfen zu können.
- Verteilung: Eng mit der Interoperabilität und Portabilität verknüpft ist die Verteilung der Anwendungen und Daten in einem Cloud-Computing-System. Anforderungen bei der Verteilung können auch extern durch Compliance-Richtlinien vorgegeben sein.
- Service-Level-Agreements (SLAs): Zusätzlich zu den Anforderung an SLAs des Szenarios für Endbenutzer, benötigen Unternehmen die Möglichkeit, SLAs kontinuierlich zu überwachen (siehe Verbrauchsmessung und Überwachung). In einem SLA muss eindeutig festgehalten werden, was der Cloud-Anbieter liefern wird und wie dies gemessen wird.
- Lebenszyklusverwaltung: Unternehmen müssen auch bei der Nutzung von Cloud-Services die Möglichkeit haben, den Lebenszyklus ihrer Anwendungen, Daten oder Identitäten verwalten zu können. Dazu werden entsprechende Prozesse und Sicherheitsmechanismen gefordert, die dies unterstützen und nachvollziehbar umsetzen.
- Governance: Öffentliche Cloud-Computing-Anbieter machen es sehr einfach, sich ein Benutzerkonto zu eröffnen und ihre Dienste zu nutzen. Diese Einfachheit birgt jedoch Risiken, da sie es Einzelnen sehr leicht ermöglicht, z. B. sensible Daten auf ein Cloud-Computing-System zu transferieren. Governance Anforderungen können auch Sicherheitsaspekte von Cloud-Computing-Systemen betreffen und sollten aus diesem Grund in einem Sicherheitskonzept berücksichtigt werden.
- Industriespezifische Standards und Protokolle: Werden bestehende Systeme unter Verwendung von Cloud-Computing-Ressourcen betrieben, sind

Anforderungen bestehender Industriestandards und Protokolle zu berücksichtigen. Industriespezifische Anforderungen werden in der Studie nicht weiter betrachtet, da dies den Rahmen der Studie sprengen würde.

Die beiden Szenarien und ihre Anforderungen stellen die Grundlage für die weitere Betrachtung der Sicherheitsaspekte von Cloud-Computing-Systemen in den folgenden Kapiteln dar. Dabei wird vorrangig auf die Benutzersicht eingegangen, die in den obigen Szenarien beschrieben wurde. Im folgenden Abschnitt werden die 10 Do's and Dont's der Cloud-Computing-Sicherheit eingeführt, die Unternehmen beachten sollten, wenn sie überlegen, Cloud-Services einzusetzen.

2.4 Cloud-Computing-Sicherheit: Die 10 Do's and Dont's

Die 10 Do's and Dont's der Cloud-Computing-Sicherheit geben eine Übersicht über die wichtigsten Tätigkeiten und Prozesse bei der Nutzung von Cloud-Services. Sie sollten berücksichtigt werden, um das volle Potential von Cloud-Computing-Systemen ausschöpfen zu können und gleichzeitig die Sicherheitsrisiken beherrschbar zu machen.

Die 10 Do' and Dont's sind:

1. Anwendung eines gesamtheitlichen Sicherheitskonzepts: Cloud-Computing-Systeme sind komplexe, verteilte Systeme bestehend aus vielen Komponenten und Diensten auf unterschiedlichen Schichten. Daher sollten Cloud-Services nach den Sicherheitsaspekten der Taxonomie des Fraunhofer AISEC für Cloud-Computing-Systeme, die in dieser Studie vorgestellt wird, betrachtet werden, um eine ganzheitliche Sichtweise der IT-Sicherheit von Cloud-Computing-Systemen zu erreichen. Je nach Anwendungsfall müssen die Bereiche Infrastruktur, Anwendung und Plattform, Verwaltung und Compliance näher analysiert werden.
2. Integration in ein bestehendes Sicherheitskonzept: Cloud-Services sollten in ein bestehendes Sicherheitskonzept integriert werden und die entsprechenden Maßnahmen getroffen werden, damit dieses Sicherheitskonzept auch angewandt und durchgesetzt wird. Hierfür müssen bestehende Systeme auf Cloud-Systeme angepasst werden, um z. B. weiterhin eine zentrale Verwaltung der IT-Systeme zu gewährleisten.
3. Herstellen einer Vertrauensbeziehung zwischen Cloud-Konsument und Cloud-Anbieter: Durch den hohen Automatisierungsgrad von Cloud-Computing-Systemen muss es nicht mehr notwendigerweise zu einer menschlichen Interaktion zwischen dem Cloud-Konsumenten und Cloud-Anbieter kommen. Aus diesem Grund sollte ein Cloud-Konsument vor der Nutzung eines Cloud-Services ein Treffen mit dem Cloud-Anbieter vereinbaren, um vor Ort ein Bild von den Rechenzentren, den Mitarbeitern

und den Prozessen des Anbieters zu bekommen. Auch sollten Ansprechpartner vereinbart werden, die bei Auftreten von Problemen kontaktiert werden können. Dies kann das Vertrauensverhältnis zwischen Cloud-Konsument und Cloud-Anbieter vor der Nutzung der Cloud-Services verbessern.

4. Schutz der Netzinfrastruktur: Dienste der Cloud-Computing-Systeme werden grundsätzlich über ein Netzwerk – häufig sogar über das Internet – bezogen, so dass die Netzinfrastruktur hinsichtlich der Sicherheit und Zuverlässigkeit als besonders schutzbedürftig eingestuft werden sollte. Standardverfahren wie Firewalls, Verschlüsselung und virtuelle, private Netze (VPN) oder redundante Netzanbindung sollten hier berücksichtigt werden. Es sollte immer eine verschlüsselte Verbindung zum Cloud-Anbieter verwendet werden.

5. Nutzung innovativer Sicherheitslösungen für Cloud-Computing-Systeme: Sicherheitslösungen für Cloud-Computing-Systeme müssen nicht zwingend als Softwareprodukt eingekauft oder selbst entwickelt werden, sondern können häufig auch von externen Anbietern angemietet werden, die speziell auf die Charakteristika von Cloud-Computing-Systeme angepasste Lösungen anbieten. Das Ziel sollte das Erreichen einer Ende-zu-Ende Sicherheit sein, die die Möglichkeit bietet, alle Benutzerzugriffe und Aktionen auf dem Cloud-Computing-System sowohl seitens des Cloud-Konsumenten als auch seitens des Cloud-Anbieters nachvollziehen zu können. Dies ist besonders wichtig, wenn weitere, dem Unternehmen oder dem Endbenutzer unbekannte Akteure bei der Bereitstellung und der Nutzung eines Cloud-Services beteiligt sind.

6. Verwendung von Basisdiensten: Cloud-Services bieten meist über die Plattformen der jeweiligen Anbieter eine Reihe von Basisservices aus den Bereichen Sicherheit, Verteilung, Bereitstellung oder Integration, die genutzt werden sollten. Mithilfe dieser Basisdienste kann meist schnell und ohne hohen Aufwand ein hohes Sicherheitsniveau erreicht werden. Dabei sollte darauf geachtet werden, dass für diese Cloud-Services ein Sicherheitstestat vorliegt, das eine externe Überprüfung der Sicherheit eines Cloud-Services nachweist.

7. Beachtung von Lock-in-Effekten: Die Verwendung von Industriestandards und offenen Protokollen erleichtert die Interoperabilität und Portabilität von Daten und Anwendungen in Cloud-Computing-Systemen. Jedoch sind aktuell noch keine Standards für Cloud-Computing-Systeme vorhanden und es ist noch unklar, welche Technologien sich mittel- bis langfristig etablieren werden. Aus diesem Grund kann es zu Lock-in-Effekten kommen, die mit hohen Wechselkosten verbunden sind, wenn ein Cloud-Anbieter gewechselt wird.

8. Einfordern von Sicherheitszertifikaten und Sicherheitstestaten: Das Einfordern von Sicherheitszertifikaten und Sicherheitstestaten kann einen

Hinweis auf die Sicherheit eines Cloud-Computing-Systems geben. Es ist im Einzelfall zu überprüfen, welche Prozesse durch ein Sicherheitszertifikat von einem externen Unternehmen untersucht wurden und wie diese beim Cloud-Anbieter umgesetzt werden. Für Cloud-Services, die für ein Unternehmen kritische Funktionen bereitstellen, sollte ein Sicherheitstestat eingefordert werden, das von externen Unternehmen ausgestellt wurde und beispielsweise die Anwendung eines sicheren Softwareentwicklungszyklus oder die Durchführung eines Penetrationstests bescheinigt.

9. Kein Verzicht auf Sicherheitskonzepte aus ökonomischen Überlegungen heraus: Es sollte nicht aus rein ökonomischen Überlegungen heraus auf Sicherheitskonzepte verzichtet werden, die z. B. in den Sicherheitsrichtlinien eines Unternehmens gefordert werden.
10. Einsatz von Service-Level-Agreements: Zentral für die Nutzung von Cloud-Services sind Service-Level-Agreements, in denen alle Rechte und Pflichten der beteiligten Akteure festgeschrieben werden müssen. Die von den meisten Cloud-Anbietern standardmäßig angebotenen SLAs sollten kritisch hinterfragt werden und bei Bedarf individuelle SLAs mit einem Cloud-Anbieter ausgehandelt werden. Des Weiteren sollten SLAs möglichst automatisiert durch entsprechende Systeme überwacht werden, auf deren Messergebnissen schließlich regelmäßige Compliance-Überprüfungen stattfinden sollten.

2.5 Gliederung der Studie

Nach der Einführung in Cloud-Computing-Systeme und Darstellung der Problemstellung in diesem Kapitel, werden in Kapitel 3 die Schutzziele vorgestellt und definiert. Eine möglichst detaillierte Festlegung der Schutzziele setzt den Rahmen, den die Sicherheitsfunktionen eines Cloud-Services unterstützen sollen.

Kapitel 4 beschreibt den Aufbau von Cloud-Computing-Systemen anhand eines Schichtenmodells, den wichtigsten Akteuren und weiteren Größen, die einen Einfluss auf die Sicherheit von Cloud-Computing-Systemen haben. Aufbauend auf den Ergebnissen aus Kapitel 4 wird in Kapitel 5 eine Taxonomie abgeleitet, die alle wichtigen Sicherheitsfelder von Cloud-Services umfasst, angefangen von der Architektur und Infrastruktur, über die Verwaltung von Cloud-Services bis hin zur Compliance von Cloud-Computing-Systemen.

In Kapitel 6 werden zuerst weit verbreitete Cloud-Service-Angebote vorgestellt und diese anschließend auf ihre Sicherheitsfunktionen nach der Cloud-Taxonomie evaluiert. Eine Bewertung der Sicherheitsfunktionen schließt dieses Kapitel ab. Den Abschluss der Studie bildet Kapitel 7, das die Ergebnisse der Studie zusammenfasst und einen Ausblick auf zukünftige Entwicklungen im Bereich Sicherheit für Cloud-Services gibt.

Abbildung 2.3 zeigt eine Übersicht der Schutzziele, technischen Abstraktionsebene, Bedrohungen und Schutzstrategien, die in den folgenden Kapiteln betrachtet werden. Hierbei entspricht die technische Abstraktionsebene dem Schichtenmodell in Kapitel 4 und die Bedrohungen beziehen sich auf die Sicherheitsfelder die in Kapitel 5 erläutert werden.

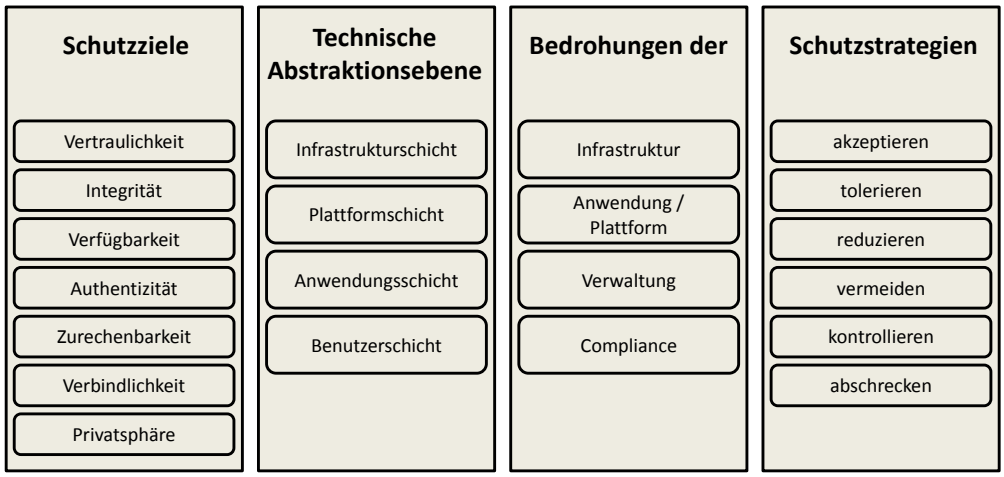

Abbildung 2.3: Übersicht der Cloud-Computing-Sicherheit

3 Schutzziele

Die Grundlage für die Anforderungen an die Sicherheit, die ein IT-System im Allgemeinen und Cloud-Computing-Systeme im Speziellen erfüllen sollten, stellen die Schutzziele dar. Diese Ziele werden meist im Rahmen der Anforderungsdefinition für ein bestimmtes Szenario festgelegt und sind Teil der nichtfunktionalen Anforderungen an den Anbieter des Cloud-Services und den Cloud-Service selbst.

In den folgenden Abschnitten werden die 6 wichtigsten Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Zurechenbarkeit und Pseudonymität eingeführt und beispielhaft an ausgewählten Cloud-Computing-Szenarien näher erläutert. Abhängig vom Cloud-Szenario können einzelne Schutzziele beispielsweise bei der Speicherung von vertraulichen Daten stärker gewichtet werden oder haben eine eher untergeordnete Rolle beim Betrieb von z. B. Testsystemen in der Cloud. An dieser Stelle kann das Konzept der mehrseitigen Sicherheit angewandt werden, das eine Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte bei der Nutzung z. B. eines Cloud-Services betrachtet.

3.1 Vertraulichkeit

Ein System gewährleistet die Informationsvertraulichkeit, wenn es keine unautorisierte Informationsgewinnung ermöglicht [17]. Die Gewährleistung der Eigenschaft Informationsvertraulichkeit erfordert in datensicheren Systemen die Festlegung von Berechtigungen und Kontrollen der Art, dass sichergestellt ist, dass Subjekte nicht unautorisiert Kenntnis von Informationen erlangen. Dies umfasst den von Benutzern autorisierten Zugriff auf gespeicherte Daten und Daten, die über ein Netzwerk übertragen werden. Berechtigungen zur Verarbeitung dieser Daten müssen vergeben und entzogen werden können und Kontrollen vorhanden sein, die eine Einhaltung dieser Rechte durchsetzen. Zum Schutz der Vertraulichkeit kommen üblicherweise kryptografische Verfahren zum Einsatz und Zugriffskontrollen, die auf starker Authentisierung basieren.

Durch die dynamische und offene Natur von Cloud-Computing-Systemen sind die Daten in diesen Systemen sehr häufig in Bewegung. Anbieter von Cloud-Ressourcen müssen zur Optimierung ihrer Infrastrukturkapazität und Sicherstellung der Performanz die Daten auf von ihnen ausgewählten Rechner speichern können und eventuell diese Daten auch kopieren und duplizieren dürfen. Diese Prozesse liegen üblicherweise außerhalb der Einflussmöglichkeiten der Kunden

und können zu Vertraulichkeitsproblemen führen, wenn die Daten beispielsweise Landesgrenzen überschreiten oder auf weniger sicheren Systemen gespeichert werden. Auch kann durch die eingesetzten Algorithmen und Datenstrukturen seitens der Anbieter nicht immer garantiert werden, dass die Daten verschlüsselt auf einem Speichermedium vorliegen. In den Geschäftsbedingungen der meisten Cloud-Anbieter gibt es zusätzlich keine Zusicherungen darüber, wo die Daten gespeichert werden und wie ihre Vertraulichkeit geschützt wird [20]. Häufig ist es sogar dem Kunden selbst überlassen, entsprechende Sicherheitsverfahren anzuwenden. Dabei sollten ruhende Daten immer verschlüsselt auf dem Speichermedium oder in der Datenbank vorliegen. Dies schließt Unternehmensinterna, Behörden- und Verwaltungsdaten, personenbezogene Daten und weitere vertrauliche und gesetzlich geregelte Daten wie Kreditkartennummern mit ein.

In einem typischen Cloud-Szenario sind meist nicht nur ein Konsument und ein Anbieter in einer bilateralen Geschäftsbeziehung verbunden, sondern eine Reihe weiterer Anbieter in verschiedenen Rollen, wie beispielsweise als Intermediär oder Konsument weiterer Cloud Services, involviert. Kann im ersten Fall einer bilateralen Geschäftsbeziehung die Vertraulichkeit mit bestehenden Verfahren wie beispielsweise SSL/TLS zur sicheren Datenübertragung zugesichert werden, so wird im zweiten Fall eine breite Unterstützung von Technologien benötigt, die die Vertraulichkeit zwischen einer Gruppe von beteiligten Akteuren sicher stellt. Dies umfasst sowohl Richtlinien seitens des Anbieters zum Umgang mit vertraulichen Daten und deren Überprüfung, sowie unterstützende Technologien zum Verwalten von Schlüsseln für die Ver- und Entschlüsselung der Daten.

Neue Herausforderungen entstehen auch bei der Verwaltung von Berechtigungen in Cloud-Systemen, die zur Sicherstellung des Schutzziels Vertraulichkeit unerlässlich sind. Auch hier besteht die Herausforderung darin, die Vielzahl an Akteuren durch effiziente Verfahren verwalten zu können. In bisherigen Unternehmensarchitekturen werden die Daten meist durch den Aufbau einer Sicherheitszone durch eine Firewall geschützt, die potentielle Angreifer daran hindert, auf diese Daten zuzugreifen. Es ist eine Trennung von Berechtigungen innerhalb und außerhalb der Firewall durchzusetzen. In einer Cloud sind die Daten über mehrere Systeme verteilt, die sich an geografisch verschiedenen Standorten befinden und von verschiedenen Anbietern betrieben werden können. Dieses Szenario erfordert neue Verfahren zum Zugriff auf Daten und Systeme, um das Schutzziel Vertraulichkeit sicher zu stellen.

3.2 Integrität

Ein System gewährleistet die Datenintegrität, wenn es Subjekten nicht möglich ist, die zu schützenden Daten unautorisiert und unbemerkt zu manipulieren [17]. Die Integrität von Daten, Nachrichten und Informationen bezeichnet deren Unverfälschtheit bzw. Vertrauenswürdigkeit. Ein Cloud-Computing-System gewährleistet die Integrität der zu schützenden Daten, wenn es einem

Dritten nicht möglich ist, diese zu verändern. Ist das Schutzziel Integrität für Cloud-Services gefordert, so sollte nicht nur der Cloud-Service selbst, der vom Endbenutzer verwendet wird, das Schutzziel erfüllen, sondern auch alle weiteren beteiligten Komponenten eines Cloud-Computing-Systems. In einem komplexen, verteilten System wie einem Cloud-Computing-System kann dies eine sehr komplexe Aufgabe darstellen, die vom Anbieter eines Cloud-Services durchgeführt werden muss.

Daten, die beispielsweise auf einem virtuellen Festplattenspeicher abgelegt sind, müssen vor nicht autorisierten Manipulationen, die von beteiligten Systemen zur Verarbeitung der Daten oder externen Angreifern ausgehen können, geschützt werden. Auch Fehler in der Konfiguration der Systeme eines Cloud-Anbieters können zu einer Integritätsverletzung führen, so dass die Daten in Cloud-Computing-Systemen immer mit einer kryptografischen Prüfsumme versehen werden sollten, wobei die Originalprüfsumme bei einem vertrauenswürdigen Dritten zum Vergleich hinterlegt werden kann. Diese sollte zudem auch bei jedem Zugriff auf Daten in Cloud-Computing-Systemen überprüft werden.

Neben der Datenintegrität sind in Cloud Systemen auch die Softwareintegrität, die Konfigurationsintegrität und die Nachrichtenintegrität wichtig. Die Softwareintegrität stellt sicher, dass die Software, die eingesetzt wird, um ein Cloud-Computing-System zu betreiben, intakt vom Softwarehersteller geliefert wurde und beispielsweise keine Hintertüren und ähnliche Verfälschungen aufweist. Die Konfigurationsintegrität stellt sicher, dass die Konfiguration einer Cloud-Ressource oder eines Cloud-Services nur durch autorisierte Personen geändert werden kann. Dies ist in Cloud-Systemen besonders wichtig, da meist eine Cloud-Umgebung automatisiert über Konfigurationsskripte aufgesetzt und verwaltet wird.

Da es sich bei Cloud-Computing-Systemen um eine Ausprägung von verteilten Systemen handelt, ist die Integrität der Nachrichten eine weitere wichtige Anforderung, die sowohl innerhalb einer Cloud als auch zwischen verschiedenen Clouds und den Systemen des Benutzers sichergestellt werden muss. Vor allem Verwaltungs- und Steuerinformationen von Cloud-Systemen bedürfen besonderem Schutz, da auch diese Nachrichten häufig über ein öffentliches Netzwerk transportiert werden.

Sind mehrere Cloud-Services bei der Nutzung eines komplexen Service für einen Endbenutzer beteiligt, kann es zu Integritätsverletzungen kommen, wenn mindestens ein Cloud-Service nicht ausgeführt werden kann. Das Problem wird weiter verschärft, wenn ein Teil der beteiligten Cloud-Service Transaktionen unterstützt und ein anderer keine Transaktionen unterstützt. Transkationen in verteilten Umgebungen wie Cloud-Computing-Systemen dienen dazu, Aktionen mehrerer beteiligter Akteure konsistent zu halten. Üblicherweise werden dabei Protokolle verwendet, die dem Alles-oder-Nichts-Prinzip folgen und nur bei erfolgreicher Ausführung die durchgeführten Änderungen oder Berechnungen auch persistent ablegen. Diejenigen der Cloud-Services, die keine Transaktionen unterstützen, müssen bei einer fehlgeschlagenen Ausführung wieder in einen

Zustand überführt werden, der vor der Teilausführung bestanden hat, um die Datenintegrität zu gewährleisten.

Häufig werden Cloud-Services mit XML-basierten Schnittstellen – z. B. auf Grundlage von auf SOAP oder REST basierten Web Services – über das Hyper-Text-Transfer-Protokoll (HTTP) bezogen. HTTP unterstützt auf Protokollebene weder eine garantierte Zustellung noch Transaktionen, so dass Funktionen zur Sicherstellung des Schutzziels Integrität auf Anwendungsebene erfolgen muss.

3.3 Verfügbarkeit

Die Verfügbarkeit eines Systems wird durch die DIN 40042 als die Wahrscheinlichkeit definiert, ein System zu einem Zeitpunkt in einem funktionsfähigen Zustand anzutreffen. Ein Cloud-Computing-System soll seinen Benutzern zu jeder Zeit den vereinbarten Zugriff auf die genutzten Ressourcen erlauben. Die Verfügbarkeit darf nicht durch nicht autorisierte Aktionen oder gezielte Angriffe externer Akteure beeinträchtigt werden.

Dieses Schutzziel stellt eine große Herausforderung an Cloud-Computing-Systeme dar, da diese meist über ein öffentliches Netzwerk erreichbar sind und den bekannten Gefahren öffentlicher Netzwerke wie beispielsweise verteilten Denial-of-Service-Angriffen ausgesetzt sind. Vor allem fehlerhafte Systemkonfigurationen und eine zu große Anzahl von Cloud-Serviceanfragen auf die Infrastruktur des Cloud-Anbieters, die nicht nur einen einzelnen Service sondern das ganze Cloud-Computing-System beeinträchtigen, führten in der Vergangenheit zu einer Beeinträchtigung der Verfügbarkeit eines Cloud-Services.

Durch den Einsatz von Cloud-Computing-Systemen verschieben sich die Strategien zur Sicherstellung einer hohen Verfügbarkeit von Maßnahmen auf Hardwareebene wie beispielsweise redundante Netzteile zu Maßnahmen auf Softwareebene. Der Grund ist der Einsatz von meist handelsüblichen Hardwarekomponenten, die zu großen Farmen zusammengeschalten werden. Dies senkt zwar zum einen die Investitionskosten des Infrastrukturanbieters, erhöht aber zum anderen die Wahrscheinlichkeit eines Hardwaredefekts, der durch geeignete Softwaremechanismen ausgeglichen werden muss.

Technische Lösungen können beispielsweise Checkpoint-und-Recovery-Mechanismen einsetzen, um den Zustand nach einem Ausfall herzustellen, oder verschiedene Verfahren auf Grundlage von Redundanz berücksichtigen. Externe Angriffe auf die Verfügbarkeit der Cloud-Computing-Systeme durch die bereits erwähnten verteilten Denial-of-Service-Angriffe werden meist durch die Begrenzung der Ressourcen für einen einzelnen Benutzer eingeschränkt oder die Auswirkungen durch die Konfiguration des Netzwerks reduziert. Sowohl ein Cloud-Serviceanbieter als auch ein Cloud-Benutzer muss sich dieses Risikos bewusst sein und geeignete Strategien implementieren, die mit diesen Risiken umgehen können und gleichzeitig eine hohe Verfügbarkeit gewährleisten.

3.4 Authentizität

Unter der Authentizität eines Objekts bzw. Subjekts wird die Echtheit und Glaubwürdigkeit des Objekts bzw. des Subjekts, die anhand einer eindeutigen Identität und charakteristischen Eigenschaften überprüfbar ist [17]. Die Authentizität einer Information ist die sichere Zuordnung zum Sender und der Nachweis, dass die Informationen nach der Erstellung und dem Versand nicht mehr verändert worden sind. Dies umfasst die sichere Identifikation der Kommunikationspartner und Mechanismen zur Einhaltung der Authentizität. Diese Mechanismen sind in der Lage, die Authentizität der zu schützenden Informationen entweder zu bestätigen oder zu widerlegen. Einem Teilnehmer des Systems ist es nicht möglich, Nachrichten und Daten im Namen eines anderen Subjekts zu erstellen und zu versenden.

Wenn ein Unternehmen damit beginnt, Cloud-Services einzusetzen, ist die Sicherstellung der Authentizität der Benutzer eine Schlüsselanforderung. Dabei sind die allgemeinen Probleme der Identitätsverwaltung anzugehen wie beispielsweise die Verwaltung der Berechtigungsnachweise, ausreichend starke Authentifizierungsmechanismen und die Verwaltung von Vertrauensverhältnissen zwischen Cloud-Services und zwischen verschiedenen Cloud-Computing-Systemen.

Zur Sicherstellung der Authentizität werden in Cloud-Computing-Systemen üblicherweise digitale Signaturen, Sicherheitstoken oder Passwörter eingesetzt, die es ermöglichen, den Unterzeichner der Nachricht bzw. den Ersteller der Signatur zu identifizieren. Ebenfalls möglich sind föderierte Identitätsverwaltungskonzepte, die auf Attributen basieren und diese Attribute meist verteilt von verschiedenen Identitätsanbietern beziehen. Das Ziel ist es, die Authentizität aller Kommunikationspartner im System zu gewährleisten.

Die Authentifizierung zwischen einem Cloud-Benutzer und einem Cloud-Service kann auf den Austausch von Authentifizierungsdaten zurückgeführt werden, die getrennt und unabhängig von der Übertragung der Anwendungsdaten erfolgen kann. In Cloud-Computing-Systemen sollte sich nicht nur der Cloud-Benutzer gegenüber dem Cloud-Service authentifizieren, sondern auch der Cloud-Service gegenüber dem Cloud-Benutzer. Dies verhindert mögliche Man-in-the-Middle-Angriffe oder die Übertragung und Verarbeitung von Daten durch bösartige Cloud-Services.

3.5 Zurechenbarkeit

Das Schutzziel Zurechenbarkeit erfordert die eindeutige Zuweisung von Handlungen zu einem Akteur im System und stellt sicher, dass die Urheberschaft eines Ereignisses oder einer Aktion im System nicht zurückgewiesen werden kann. In Cloud-Computing-Systemen sollten alle Handlungen einem Akteur zurechenbar sein, auch wenn daraus eine Vertragsverletzung entstehen kann. Die

Zurechenbarkeit transportiert daher auch immer die Identität des Urhebers der Aktion und einen Zeitstempel. Sie ist eine sehr wichtige Voraussetzung für die Rechtsverbindlichkeit elektronischer Geschäftstransaktionen wie die Nutzung eines Cloud-Service. Das Schutzziel Zurechenbarkeit stellt bei der Nutzung eines Cloud-Service sicher, dass alle Aktionen nachweislich, insbesondere gegenüber Dritten, von einem bestimmten Akteur des Cloud-Computing-Systems durchgeführt wurden und somit beispielsweise zur Abrechnung der verbrauchten Ressourcen herangezogen werden können.

Als Voraussetzung zur Erreichung des Schutzziels Zurechenbarkeit dienen Service-Level-Agreements, die bestimmte Leistungsgarantien festschreiben. Diese Garantien müssen von entsprechenden Systemen überwacht und Abweichungen von diesen Garantien mitprotokolliert werden. Des Weiteren müssen alle weiteren Aktionen der Akteure eines Cloud-Computing-Systems protokolliert werden, damit eine eindeutige Zuordnung gewährleistet ist.

Die Zurechenbarkeit eines Cloud-Service kann durch Mechanismen wie qualifizierte Signaturen, Verschlüsslung und Mechanismen zur Sicherstellung der Datenintegrität zur Verfügung gestellt werden. Üblicherweise gliedert sich der Verbindlichkeitsnachweis in 4 Phasen, die von einem Verbindlichkeitsprotokoll genau spezifiziert werden: Beweiserzeugung, Beweistransfer und -speicherung, Beweisverifikation und Konfliktauflösung. Der Beweis könnte in Cloud-Computing-Systemen beispielsweise durch die Verwendung von digitalen Signaturen erzeugt werden, die ein Dritter validieren kann.

Ein Ressourcenanbieter ändert beispielsweise die Richtlinien für die Ressourcenzuweisung der virtuellen Maschine. Dies wirkt sich auf die Performanz der Anwendung aus, die ein Serviceanbieter an einen Servicekonsumenten bereitstellt. Die Ressourcenänderung kann zu einer Verletzung des Service-Level-Agreements führen, das der Serviceanbieter mit dem Servicekonsumenten abgeschlossen hat. Durch das Schutzziel Zurechenbarkeit muss sichergestellt werden, dass die Verletzung des Service-Level-Agreements auf eine Änderung der Ressourcenzuweisung zurückzuführen ist.

3.6 Pseudonymität und Schutz der Privatsphäre

Das Schutzziel der Pseudonymität dient dem Schutz der Privatsphäre. Ein IT-System, das die Privatsphäre seiner Nutzer schützt, sollte nur so viele Daten über seine Benutzer erheben und abspeichern, wie für die Erbringung des Dienstes notwendig sind und diese auch nur für autorisierte Personen einsehbar machen. Die hierfür eingesetzten technischen und organisatorischen Maßnahmen sollen sicherstellen, dass keine Profile über das Verhalten der Benutzer erstellt werden können. Eine anonyme Nutzung von Diensten ist die strikteste Form der Privatsphäre.

Die Forderung des Schutzziels Anonymität ist für Cloud-Benutzer nur eingeschränkt anwendbar, da für die Abrechnung der benutzen Ressourcen detaillierte Profile über die Aktionen der Benutzer erfolgen müssen. Aus diesem Grund sollten in Cloud-Computing-Systemen Pseudonyme eingesetzt werden, die es einem Akteur (z. B. Konsument oder Anbieter) ermöglicht, die sich hinter dem Pseudonym versteckten Identität zu Abrechnungszwecken aufdecken zu können. Zusammen mit dem Schutzziel Zurechenbarkeit kann eine Überwachung wichtiger Elemente der Privatsphäre wie beispielsweise Transparenz, Zusicherungen oder Einhaltung der Richtlinien erfolgen [30]. Hierfür sind maschinenlesbare Richtlinien zum Schutz der Privatsphäre notwendig, die auf Anwendungsebene möglichst unabhängig von der Implementierung der Anwendung hinsichtlich des Schutzziels überprüft werden können.

Unabhängig von den einzelnen Schichten der Cloud-Architektur dürfen nicht autorisierten Benutzern nur anonymisierte Daten zur Verfügung gestellt werden. Es ist bei der Auswahl der entsprechenden Anbieter bzw. Services darauf zu achten, welche Prozesse dieser zur Sicherstellung dieses Ziels anwendet. Beim Einsatz von verschiedenen Anbietern ist darauf zu achten, dass der Schutz der Privatsphäre auch über die Grenzen eines Anbieters hinweg eingehalten wird.

Benutzern eines Cloud-Services, wie beispielsweise eines sozialen Netzwerks auf Cloud-Ressourcen, ist häufig nicht bewusst, dass ihre Daten auf einer Cloud gespeichert werden, die beispielsweise eine Zweitnutzung ihrer Daten ermöglicht und damit ihre Privatsphäre verletzt. In diesem Szenario ist es wichtig, den Benutzern eines Service die Kontrolle über ihre Daten zu geben und damit eine transparente Nutzung des Services zu ermöglichen.

4 Aufbau von Cloud-Computing-Systemen

Dieses Kapitel führt in den Aufbau von Cloud-Computing-Systemen ein und stellt dessen wichtigsten Schichten, Akteure, Nutzungs- und Bezugsmodelle vor, die in der erweiterten Cloud-Computing-Definition des NIST festgehalten sind [28]. Das Ziel des Kapitels ist es, ein einheitliches Verständnis für die Konzepte in Cloud-Computing-Systemen zu schaffen und die sich daraus ergebenden Bedrohungen für die in Kapitel 3 eingeführten Schutzziele aufzuzeigen. Auf Grundlage des in diesem Kapitel vorgestellten Aufbaus und der daraus resultierenden Bedrohungen wird im folgenden Kapitel eine Taxonomie der Cloud-Sicherheitsrisiken abgeleitet.

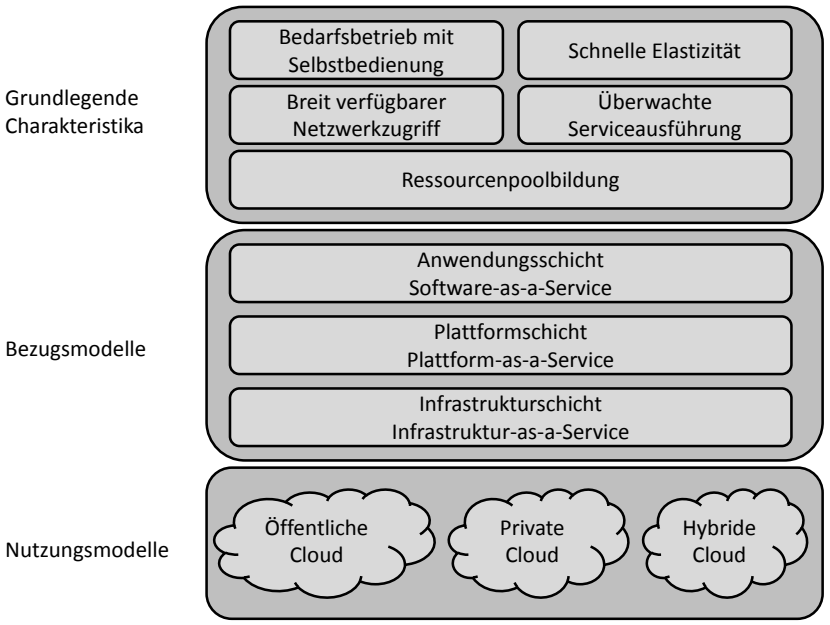

Abbildung 4.1: Charakteristika, Bezugs- und Nutzungsmodelle von Cloud-Computing-Systemen

Abbildung 4.1 greift die in Kapitel 2 eingeführten Charakteristika auf und erweitert diese um die häufigsten Nutzungs- und Bezugsmodelle von Cloud-Computing-Systemen, die die Grundlage für den Aufbau der Cloud-Computing-Systeme bilden. Die Schichten und Ausprägungen der Nutzungs- und Bezugsmodelle werden in den folgenden Abschnitten des Kapitels detailliert vorgestellt.

Abschnitt 4.1 führt das Schichtenmodell für Cloud-Computing-Systeme ein, das im Fokus der Bezugsmodelle von Cloud-Services steht und sich an den Diensten orientiert, die Cloud-Computing-Systeme anbieten. Die Schichten erstrecken

sich von der Infrastruktur über Plattformen bis hin zu den Anwendungen. Zusätzlich zu der üblichen Dreiteilung der Bezugsmodelle wird im Rahmen dieser Studie als zusätzliche Schicht die Benutzerschicht eingeführt, die alle den Konsumenten betreffenden Akteure und Systeme umfasst. Dabei orientiert sich die Studie an den Cloud-Computing-Szenarien der Cloud Computing Use Case Discussion Group [8]. Für jede dieser Schichten werden die wichtigsten Akteure vorgestellt, Sicherheitsbedrohungen besprochen und Beispiele für Services geben.

Abschnitt 4.2 gibt einen Überblick über die Benutzerschicht des Modells. Je nach Ausprägung der Cloud-Computing-Systeme verwenden die Endbenutzer der Benutzerschicht eine oder mehrere der darunter liegenden Services der Anwendungsschicht in Abschnitt 4.3, der Plattformschicht in Abschnitt 4.4 oder der Infrastrukturschicht in Abschnitt 4.5. Verschiedene Nutzungsmodelle der Cloud-Services werden schließlich in Abschnitt 4.6 eingeführt und die Nutzung der Cloud-Services über ein öffentlich zugängliches oder privates Cloud-Computing-System betrachtet sowie hybride Modelle diskutiert.

4.1 Schichtenmodell

Das Schichtenmodell, das in dieser Studie verwendet wird, orientiert sich an den Serviceangeboten, die unter Verwendung von Cloud-Ressourcen kommerziell erhältlich sind. Diese Services lassen sich in die Bereiche Infrastruktur, Plattform und Anwendung gliedern. Zusätzlich zu diesen drei Schichten wird eine Benutzerschicht hinzugefügt, die die Sichtweise des Endbenutzers auf Cloud-Services kapselt [8]. Das Modell wird in Abbildung 4.2 dargestellt.

Die Benutzerschicht kann in diesem Modell verschiedene Ausprägungen von Cloud-Services, die von den darunter liegenden Schichten angeboten werden, annehmen. Verwendet ein Cloud-Benutzer beispielsweise Services der Infrastrukturschicht, kann er seine eigenen Anwendungen auf den Ressourcen einer Cloud-Infrastruktur betreiben und muss sich um Pflege, Wartung und Sicherheitsfunktionen seiner Anwendung weiterhin selbst kümmern. Bezieht er einen Service auf der Anwendungsschicht, werden diese Aufgaben üblicherweise von dem Anbieter des Cloud-Services übernommen. Daraus ergibt sich für den Cloud-Benutzer eine flexible Möglichkeit, genau die Cloud-Services zu benutzen, die er für seine Anforderungen benötigt. Gleichzeitig muss ein Cloud-Benutzer jedoch einen Kontrollverlust bezüglich des geografischen Orts der Daten und Anwendungen.

Jede der in Abbildung 4.2 dargestellten Schichten wird in den folgenden Abschnitten beschrieben, ihre wichtigsten Akteure vorgestellt und die Bedrohungen diskutiert, die zu einer Verletzung der in Kapitel 3 diskutierten Schutzziele führen können.

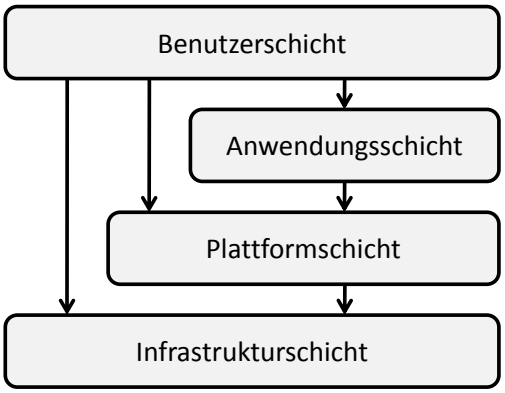

Abbildung 4.2: Schichtenmodell der Cloud-Computing-Systeme

4.2 Benutzerschicht

Die Benutzerschicht des Cloud-Modells umfasst alle Systeme, Komponenten und Geräte, die es einem Endbenutzer ermöglichen, auf Cloud-Services der darunter liegenden Schichten zuzugreifen. Der Zugriff kann automatisiert durch bestehende Systeme des Benutzers oder durch eine manuelle Auswahl des Dienstes über ein Portal erfolgen. Eine Herausforderung auf der Benutzerschicht stellt die Anpassung der bestehenden Sicherheitsfunktionen für die Nutzung von Cloud-Services dar und ist aktueller Gegenstand der Forschung [9]. Dabei ist aktuell nicht hinreichend untersucht, ob Erweiterungen bestehender Systeme ausreichen oder neue Sicherheitstechnologien für den Einsatz von Cloud-Computing-Systemen, insbesondere für Systeme mit hohen Sicherheitsanforderungen, entwickelt werden müssen.

Als Beispiel lässt sich an dieser Stelle die Identitäts- und Rechtverwaltung anführen, die in Unternehmensnetzwerken sehr weit verbreitet ist. Viele Lösungen aus diesem Bereich bieten aktuell noch keine Integration von externen Cloud-Services an, so dass entweder bestehende Systeme erweitert werden müssen oder neue Lösungen eingeführt, die bestehende Systeme ersetzen können.

Akteure der Benutzerschicht sind entweder Softwareagenten, die in die Systeme und Anwendungen eines Endbenutzers integriert sind und meist anhand vorher definierter Richtlinien agieren, oder menschliche Benutzer, die als Konsumenten von Cloud-Services auftreten. Konsumenten von Cloud-Services wiederum können entweder Mitarbeiter von Unternehmen oder private Benutzer sein, wobei davon ausgegangen werden kann, dass die Anzahl der privaten Benutzer von Cloud-Services deutlich höher als die von Unternehmensnutzern liegt, wie die Benutzerzahlen Cloud-basierter Angebote von Google (z. B. GoogleMail) oder sozialer Netzwerke (z. B. Facebook) zeigen. In einem Cloud-Computing-System sind die Benutzer Abonnenten oder Mieter, die die Angebote eines Systems nach Aufwand von einem Serviceanbieter in Anspruch nehmen. Daraus ergibt sich, dass Cloud-Benutzer keine oder nur geringe Investitionskosten haben und eine elastische und beinahe unbegrenzte Rechen- und Speicherkapazität mieten können. Auf diese Kapazitäten kann von einer Reihe an unterschiedliche

mobilen und stationären Geräten zugegriffen werden, da sie meist als Webservice bereitgestellt werden.

Aus Sicht des Akteurs Endbenutzer gibt es eine Reihe von Vorteilen durch die Verwendung von Cloud-Services, die vor allem aus der Pflege und Wartung der Systeme resultieren, die in der Regel in Cloud-Computing-Systemen vom Serviceanbieter durchgeführt werden. Dabei ist genau zu überprüfen, welche administrativen Routineaufgaben vom Cloud-Serviceanbieter übernommen werden und welche Aufgaben der Endbenutzer selbst übernehmen muss. Durch die Übertragung von Routineaufgaben an den Cloud-Serviceanbieter lassen sich freigewordenen Kapazitäten beispielsweise zur Entwicklung innovativer Anwendungen nutzen und eine Konzentration auf die Kernkompetenzen des Unternehmens erreichen.

Jedoch muss der Endbenutzer die Risiken und den Nutzen abwägen, die der Einsatz von Cloud-Services mit sich bringt. Es ist also für den Endbenutzer ein Muss, Expertise in der Bewertung der Risiken – vor allem der Sicherheits- und Zuverlässigkeitsrisiken – aufzubauen und monetäre Größen in die Entscheidung mit einzubeziehen. Aus Endbenutzersicht eines Unternehmens lässt sich eine Veränderung des Anforderungsprofils der IT-Mitarbeiter wie beispielsweise Administratoren erkennen, weg von Routineaufgaben in der Wartung und Pflege der Systeme und hin zu der Bewertung der Risiken und der Kosten für den Einsatz der Cloud-Services.

Auch private Benutzer können ähnlich von Cloud-Services profitieren, indem sie keine Wartung und Pflege ihrer Anwendungen mehr durchführen müssen und trotzdem immer die aktuellste Version einer Anwendung als Service über einen Webbrowser nutzen können. Weitere Vorteile können private Benutzer auch aus der einfachen Freigabe und gemeinsamen Nutzung von Daten erzielen, um sie beispielsweise dem Freundeskreis zugänglich zu machen.

4.3 Anwendungsschicht: Software-as-a-Service (SaaS)

Die Anwendungsschicht ist die Schicht des Cloud-Modells, die gegenüber dem Endbenutzer einer Cloud sichtbar ist und deren Services ein Endbenutzer üblicherweise verwendet. Der Zugriff erfolgt meist über ein Webportal und Service-orientierte Architekturen auf Grundlage von Webservice-Technologien. Sie erfordert die Hinterlegung einer Kreditkarte oder Bankverbindung, über die die Nutzungsgebühren der Services abgerechnet werden.

Die Services der Anwendungsschicht können als Weiterentwicklung des Application-Service-Provider-Modells (ASP) gesehen werden, bei dem ein Serviceanbieter eine Anwendung betreibt, wartet und pflegt. Unterschiede zum klassischen ASP-Modell liegen bei den Services der Anwendungsschicht in der Kapselung der Anwendung als Service, dem dynamischen Bezug und der verbrauchsabhängigen Abrechnung. Das Ziel einer Konzentration auf Kernkompetenzen durch die Auslagerungen von Anwendungen verfolgen jedoch beide Modelle.

Da eine Cloud-Anwendung auf der Infrastruktur des Anbieters anstatt auf den Rechnern eines Benutzers bereitgestellt wird, ergeben sich eine Reihe von Vorteilen sowohl für den Servicekonsumenten als auch für den Serviceanbieter der Anwendungsschicht. Ein Servicekonsument ist in der Regel ein Akteur, der einen Cloud-Service benutzt und dabei meist an Regeln seiner zugehörigen Organisation (z. B. Unternehmen oder Abteilung) gebunden ist, die er einhalten muss. Solche Regeln können Mindestanforderungen an den Cloud-Anbieter bezüglich funktionale oder nicht-funktionale Kriterien wie Dienstgüte oder die Sicherheitsfunktionen eines Cloud-Services zur Folge haben, die von einem Cloud-Serviceanbieter bereitgestellt werden müssen.

In Ausnahmefällen kann der Servicekonsument auch eine Bedrohung für den Cloud-Service darstellen, wenn er beispielsweise übermäßig viele Serviceanfragen an das System schickt und dieses mit der Abarbeitung der Anfragen überlastet ist oder wenn Schwachstellen eines Dienstes für das Einschleusen von Fremdcode ausgenutzt werden.

Serviceanbieter der Anwendungsschicht bieten einen Anwendungsdienst an, dessen Bereitstellung unter Verwendung der Plattformschicht oder der Infrastrukturschicht erfolgt. Serviceanbieter, die keine eigene Infrastruktur betreiben, mieten sich diese bei einem Ressourcenanbieter an.

Der Vorteil der zentralen Bereitstellung eines Service durch einen Serviceanbieter für eine große Anzahl an Servicekonsumenten besteht insbesondere auf der Anwendungsschicht in der effektiven Wartung und die Möglichkeit kurzer Innovationszyklen, da der Service auf einer bekannten, sehr homogenen Plattform bereitgestellt wird und nicht auf einer Vielzahl unterschiedlicher Systemkonfigurationen getestet werden muss. Cloud-Services können dem Servicekonsumenten so immer in der aktuellsten Version zugänglich gemacht und durch die Verwendung einer serviceorientierten Architektur in bestehende Prozesse schnell integriert werden.

Trotz der Vorteile von Cloud-Services der Anwendungsschicht, sind vor allem die Sicherheitsfunktion und die Verfügbarkeit Problemfelder, die eine sichere Nutzung von Services der Anwendungsschicht einschränken [37]. Die Sicherheit der Servicenutzung muss nicht nur zwischen der Benutzerschicht und der Anwendungsschicht sichergestellt werden sondern auch zwischen Services auf der Anwendungsschicht und den Services der darunter liegenden Schichten. Durch die Integration einer Reihe von Services anderer Service- oder Ressourcenanbieter kann der Ausfall eines Teilservice signifikanten Einfluss auf die Diensterbringung eines Service auf Anwendungsschicht zur Folge haben. Im schlimmsten Fall kann ein Endbenutzer seinen Service nicht mehr nutzen. Aus diesem Grund muss sich ein Endbenutzer von Cloud-Services zum einen der Risiken bewusst sein und zum anderen Informationen vom Serviceanbieter eines Anwendungsservice einholen und verschiedene Szenarien und deren Konsequenzen mit dem ausgewählten Cloud-Serviceanbieter besprechen.

Unter dem Begriff Software-as-a-Service sind aktuell bereits Cloud-Services aus

verschiedenen Anwendungskategorien verfügbar. Die wichtigsten Anwendungskategorien sind [38][25]:

- Skalierbare Webseiten: In diese Kategorie fallen Anwendungen, auf die über das Internet zugegriffen wird und die eine große Anzahl an Benutzer aufweisen. Häufige Komponenten, die in diesen Anwendungen eingesetzt werden, sind Lastverteiler, verteilte Datenbanken und skalierbare Portale. Beispiele sind webbasierte Officeanwendungen, soziale Netzwerke oder webbasierte Desktopumgebungen.
- Datenhaltung und Datenverteilung: Häufig werden im Zusammenhang mit skalierbaren Webseiten Services eingesetzt, die diese Daten speichern und weltweit über Content-Delivery-Netzwerke (CDN) verteilen. Weitere Anwendungen im Bereich Datenhaltung sind Online-Backup-Services.
- Softwareentwicklung und Softwaretests: Cloud-Services im Bereich Softwareentwicklung bieten verschiedenen Möglichkeiten der Zusammenarbeit an, wobei beispielsweise ein gemeinsames Verzeichnis zum Datenaustausch, zur Quellcodeverwaltung und weiteren Dienstleistungen als Service angemietet werden kann. Im Bereich Softwaretests können Cloud-Ressourcen verwendet werden, um eine weltweit verteilte Testumgebung aufzubauen und Skalierbarkeitstests durchzuführen.
- Interaktive, mobile Anwendungen: In dieser Anwendungskategorie wird die Anwendungslogik eines Cloud-Services dem Benutzer eines mobilen Endgeräts zur Verfügung gestellt. Ein Cloud-Service kann beispielsweise die Daten und die Anwendung möglichst nahe am Ort des mobilen Endgeräts bereitstellen, so dass Verzögerungen beim Zugriff auf Cloud-Services vermieden werden.
- Wissenschaftliches Rechnen: Eine weitere Anwendungskategorie ist der Einsatz von Cloud-Services der Anwendungsschicht zum wissenschaftlichen Rechnen. Da es sich in diesem Umfeld meist um Berechnungen handelt, die über einen bestimmten Zeitraum große Mengen an Rechen- und Speicherressourcen benötigen, bieten sich Cloud-Ressourcen als kostengünstige Alternative zu Grid-Systemen oder Cluster-Systemen an.

  Das Hauptproblem bei der Umsetzung wissenschaftlicher Anwendungen ist jedoch die hohe Latenz bei der Kommunikation zwischen den Knoten eines Cloud-Computing-Systems, da die meisten wissenschaftlichen Anwendungen entworfen wurden, um auf dedizierten Knoten mit Hochgeschwindigkeitsnetzwerken ausgeführt zu werden. Die Anwendungen müssen angepasst werden, um zum einen die hohe Latenz in Cloud-Computing-Systemen mit einzubeziehen und zum anderen Performanceschwankungen des Cloud-Computing-Systems zu berücksichtigen.

Abbildung 4.3 zeigt schematisch das Modell von Cloud-Services der Anwendungsschicht. Anwendungen aus z. B. den Bereichen Finanzen, Beschaffungswesen oder Kollaboration werden als Service einem Cloud-Konsumenten bereit-

gestellt. Wie die Ausführungsumgebung eines Services auf Anwendungsebene aussehen kann, kann jedoch von Serviceanbieter zu Serviceanbieter variieren. In Abbildung 4.3 werden bei der Ausführung von Anwendungsservices, Services der Plattformschicht verwendet, die wiederum auf Service der Infrastrukturschicht aufsetzen. In einem solchen Szenario können drei verschiedene Cloud-Anbieter unterschiedlicher Schichten bei einer Serviceausführung beteiligt sein.

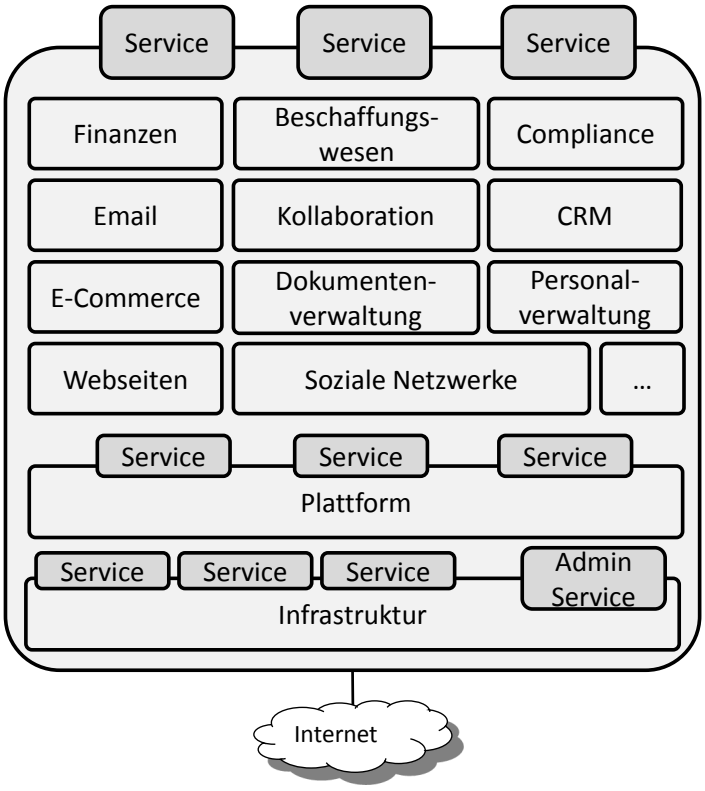

Abbildung 4.3: Cloud-Services der Anwendungsschicht

Varianten dieses Modells sind Ausführungsumgebungen, bei denen ein Anbieter von Cloud-Services der Anwendungsschicht keine weiteren Services einer Plattform oder Infrastruktur eines anderen Cloud-Anbieters benutzt oder bei denen zwei Serviceanbieter, nämlich eine Anwendungs- und eine Plattformanbieter, bei der Servicelieferung, involviert sind. Die Ausführungsumgebung kann Auswirkungen auf die Sicherheit des Cloud-Services auf Anwendungsschicht haben, wenn beispielsweise unterschiedliche Sicherheitsstandards und -richtlinien von den beteiligten Cloud-Anbietern verwendet werden.

4.4 Plattformschicht: Plattform-as-a-Service (PaaS)

Die Plattformschicht stellt die Umgebung für die Entwicklung und Bereitstellung von Cloud-Anwendungen zur Verfügung. Zielgruppe dieser Schicht sind meist Entwickler, die eine Cloud-Anwendung für eine bestimmte Plattform entwickeln und betreiben möchten. Dabei werden sie von den Betreibern einer Plattform mit einer offenen oder proprietären Sprache, einer Reihe grundlegender Basisservices zur Unterstützung der Kommunikation, der Überwachung oder der

Abrechnung der Leistungen und weiteren Komponenten unterstützt, die z. B. die Inbetriebnahme beschleunigen oder die Skalierbarkeit und/oder die Elastizität einer Anwendung bereitstellen können. Die Verteilung der Anwendung auf die darunter liegende Infrastruktur übernimmt üblicherweise der Betreiber der Cloud-Plattform. Die angebotenen Services (siehe Abbildung 4.4) einer Cloud-Plattform stellen häufig einen Kompromiss zwischen Komplexität und Flexibilität dar, die es ermöglicht, schnell Anwendungen zu implementieren und diese ohne hohen Konfigurationsaufwand in die Cloud zu laden. Nachteile können Einschränkung der unterstützten Programmiersprachen, das Programmiermodell, die Zugriffsmöglichkeiten auf Ressourcen oder der Einschränkungen hinsichtlich der Persistenz darstellen.

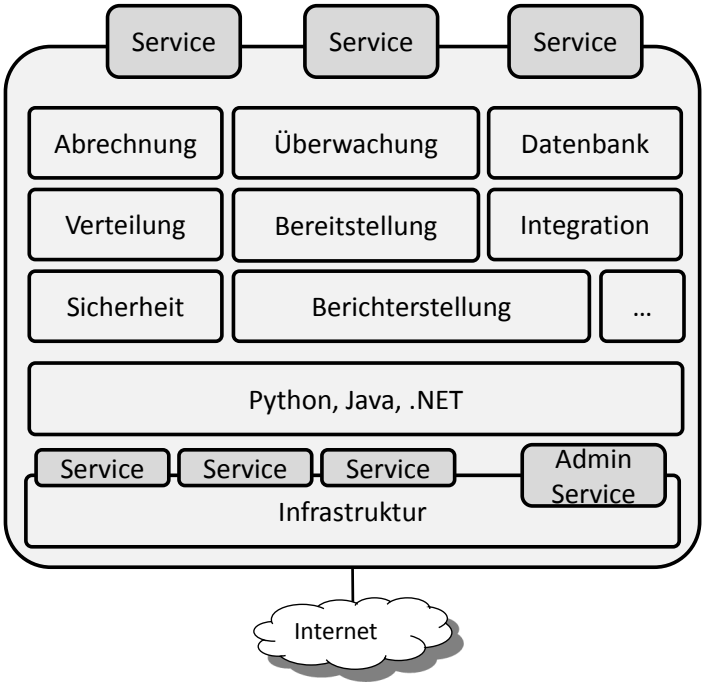

Abbildung 4.4: Cloud-Services der Plattformschicht

Da es keine einheitliche Spezifikationen gibt, welche Services und Komponenten von einer Plattform angeboten werden, ist hier eine Einzelfallanalyse der Zielplattform durchzuführen, um eine geeignete Plattform für eine Anwendung zu finden. Häufig wird der Begriff Plattform-as-a-Service (PaaS) als Sammelbegriff für alle Services und Komponenten verwendet, die auf der Plattformschicht angeboten werden. Beispiele für Plattformen sind die Google App Engine[1] oder die Microsoft Azure Plattform[2]. Beide Plattformen, Google App Engine und Microsoft Azure, bieten Basisdienste an, die es ermöglichen Webseiten zu entwickeln, bestehende Anwendungen in ein Cloud-Computing-System auszulagern oder spezielle Anwendungen für Kunden zu entwickeln.

Akteure auf der Plattformschicht sind, neben den oben bereits erwähnten Entwicklern von Cloud-Services, die Plattformanbieter, die eine Plattform betreiben

[1] http://code.google.com/intl/de-DE/appengine/
[2] http://www.microsoft.com/azure/default.mspx

und deren Basisservices anbieten, und die Werkzeuganbieter, die Entwicklerwerkzeuge und/oder Programmiersprachen zur Verfügung stellen. Entwickler können durch die Integration bestehender Services der Plattform in ihre Anwendung die Komplexität ihrer Softwareentwicklungsaufgaben reduzieren, ihre Entwicklungszeit beschleunigen und die Anzahl der Programmierfehler und damit potentieller Schwachstellen durch Wiederverwendung von bestehendem Quellcode verringern, da davon ausgegangen werden kann, dass es im Interesse des Plattformanbieters ist, Basisservices hoher Qualität bereitzustellen.

4.5 Infrastrukturschicht: Infrastruktur-as-a-Service (IaaS)

Die Infrastrukturschicht stellt Services zur Benutzung von grundlegenden IT-Ressourcen bereit, die unter dem Begriff Infrastructure-as-a-Service (IaaS) zusammengefasst werden. Zu den grundlegenden IT-Ressourcen zählen Serviceangebote im Bereich Rechenressourcen, Speicherressourcen und der Kommunikationsverbindung. Diese können verwendet werden, um bisherige Anwendungen auf Cloud-Ressourcen bereitzustellen oder neue Services auf den darüber liegenden Schichten zu realisieren. Auf dieser Schicht lassen sich drei wichtige Akteure identifizieren: Ressourcenkonsument, Ressourcenanbieter, Ressourcenintermediär.

Ein Ressourcenkonsument nutzt die von einem Ressourcenanbieter bereitgestellten Ressourcen, um Anwendungen auszuführen und Dienste auf höheren Schichten des Cloud-Computing-Systems bereitzustellen. Aufgabe eines Ressourcenkonsumenten ist die Spezifikation der benötigten Ressourcen und deren Dienstgüte in Form von Service-Level-Agreements, die ein Ressourcenanbieter einzuhalten hat. Die Nachfrage nach Ressourcen erfolgt in Cloud-Computing-Systemen häufig automatisiert, indem neue Ressourcen zu den bestehenden Ressourcen hinzugefügt werden, um eine gleich bleibende Dienstgüte bei Lastspitzen, Ausfällen und ähnlichen Ereignissen zu garantieren. Da mit der Benutzung weiterer Ressourcen auch häufig Mehrkosten verbunden sind, ist es Aufgabe des Ressourcenkonsumenten, Regeln festzulegen, wie die Nachfrage nach Ressourcen bei bestimmten Ereignissen erfolgen soll. Er kann dabei auf eigene Erfahrungen, Berichte in Foren und Zeitschriften, Best-Practice-Ansätzen, wie sie beispielsweise von Vereinigungen wie der Cloud Security Alliance entworfen werden, und historische Überwachungsdaten zurückgreifen. Die Auswahl und der Zugriff auf die Ressourcen eines Anbieters erfolgen in Cloud-Computing-Systemen entweder direkt oder über einen Intermediär, der Ressourcen von verschiedenen Anbietern vermittelt.

Ein Ressourcenanbieter stellt in einem Cloud-Computing-System virtualisierte Ressourcen zur Verfügung. Virtualisierte Ressourcen sind Rechenressourcen, die üblicherweise CPU und RAM, Speicherressourcen (Blockspeicher und Datenbanken) und Netzwerkressourcen umfassen (siehe Abbildung 4.5. Diese Ressourcen werden von einem Ressourcenanbieter einheitlich zur Verfügung gestellt. Häufig werden die Einzelressourcen zu Ressourcenbündeln zusammengefasst und in

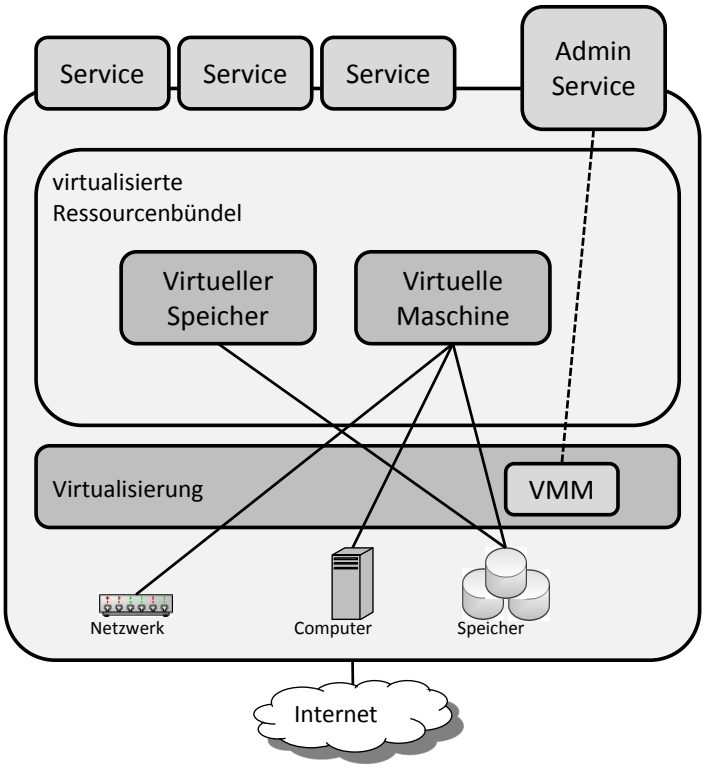

Abbildung 4.5: Cloud-Services der Infrastrukturschicht

verschiedenen Größen zur Verfügung gestellt. Ein Ressourcenanbieter betreibt häufig ein eigenes Rechenzentrum, in dem er die Ressourcen in einem Ressourcenpool zusammengefasst hat und die physischen Ressourcen mithilfe einer Virtualisierungssoftware abstrahiert. Die am häufigsten anzutreffende Variante einer Virtualisierungssoftware stellt der Virtual Machine Monitor (VMM) dar, der die Ressourcenzuweisung der physikalischen Ressourcen übernimmt und die Erstellung virtueller Ressourcenbündel ermöglicht. Die physikalische Ressource wird durch Virtualisierung abstrahiert, so dass sich auf den virtuellen Ressourcen mehrere Betriebssysteme und Benutzerumgebungen die Ressourcen teilen können, ohne sich im Idealfall gegenseitig zu beeinflussen.

Neben den Ressourcenanbietern, die ihre Ressourcen selbst produzieren und Ressourcenkonsumenten anbieten, lässt sich noch eine weitere Ausprägung von Ressourcenanbietern identifizieren. Diese Ressourcenanbieter treten als Intermediäre von Ressourcen auf. Sie vermitteln ungenutzte Kapazitäten von Ressourcenproduzenten an Ressourcennachfrager. Dies kann mithilfe von Marktplätzen oder spezialisierten Portalen erfolgen.

Rechenressourcen Rechenressourcen sind die zentralen Ressourcen von Cloud-Computing-Systemen und werden als Service durch ein Bündel an Einzelressourcen angeboten. Üblicherweise bestehen Rechenressourcen aus dem Ressourcentripel CPU, Haupt- und Festplattenspeicher, die meist die Leistungsfähigkeit einer virtuellen Maschine beschreiben. Der Benutzer einer virtuellen Maschine kann entweder die Einzelressourcen des Ressourcentripels selbst wählen

oder zwischen vorgefertigten Größen auswählen und damit die Ressourcenkonfiguration wählen, die er für die Lösung einer bestimmten Aufgabe benötigt.

Die grundlegende Technologie, die es ermöglicht Rechenressourcen als Service anzubieten, wird durch verschiedene Virtualisierungstechnologien realisiert, die dem Anbieter eine flexible Möglichkeit bietet, dynamisch unterschiedliche Größen virtueller Maschinen zu konfigurieren und gleichzeitig die physische Infrastruktur des Anbieter schützt. Zusätzlich ermöglichen Virtualisierungstechnologien die Isolation mehrerer virtueller Maschinen auf einem physischen Knoten, was hilfreich ist, um z.B. das Sicherheitsziel Integrität zu realisieren. Im Allgemeinen sind die Virtualisierungsprodukte durch den Anbieter von Rechenressourcen als Service sehr stark angepasst und vom Kunden nicht einsehbar, so dass eine Bewertung der Sicherheit sehr schwierig ist. Besonderen Schutz bedarf der entfernte Administrationszugang der virtuellen Maschinen, der meist über ein öffentliches Netzwerk zugegriffen wird und häufig die Möglichkeit anbietet, zusätzliche Instanzen einer virtuellen Maschine zu erzeugen oder bestehende Instanzen zu löschen, was eines oder mehrere Schutzziele verletzen kann.

Speicherressourcen Eine weitere grundlegende Ressource stellen Speicher dar, die die Möglichkeit bieten, Daten der Akteure und Anwendungen auf entfernten Festplatten und verteilten Datenstrukturen (z. B. verteilte Datenbanken) abzulegen und dadurch von jedem Ort aus zugreifbar zu machen. Die Speicherressourcen werden als Cloud-Service angeboten und erleichtern Cloud-Anwendungen über die limitierten Grenzen der virtuellen Maschine oder des Servers hinaus hinsichtlich der Speicherkapazität zu skalieren. An Datenspeicherdienste werden besondere (Sicherheits-)Anforderungen gestellt, wenn sie beispielsweise dazu verwendet werden, Benutzerdaten oder andere vertrauliche Informationen zu speichern. Neben hoher Verfügbarkeit, Zuverlässigkeit, Skalierbarkeit und Datenkonsistenz, sollten auch alle, in Kapitel 3 eingeführten Schutzziele erfüllt sein.

Eine Besonderheit bei Cloud-Services zur Speicherung von Daten stellen die eingesetzten Verfahren und Algorithmen dar. Sie basieren meist zur Vereinfachung der Verarbeitung von großen Datenmengen auf dem von Google eingeführten MapReduce-Rahmenwerk und weiteren Verfahren zur Verwaltung von Datenreplica [16]. Freie Implementierungen dieser Verfahren wie beispielsweise Hadoop bieten nur rudimentäre Authentifizierungsverfahren an, was das Schutzziel Authentizität bedrohen kann [12]. Ein weiteres potentielles Sicherheitsproblem stellen die Anzahl der Replicas und deren Synchronisation und Löschung dar. Daten können bei der Erstellung eines Replikats Landesgrenzen oder Grenzen von Organisationsstrukturen verlassen und damit beispielsweise den Schutz der Privatsphäre verletzen. Der Benutzer hat häufig nicht die Möglichkeit, die Anzahl der Replica, Verschlüsselungsverfahren oder Bewegungen seiner Daten nachzuvollziehen.

Aus den eingesetzten Verfahren zur Speicherung von Daten lassen sich eine Reihe von Sicherheitsimplikationen ableiten, die bei der Definition von Sicher-

heitsrichtlinien und deren Umsetzung durch den Cloud-Infrastrukturbetreiber eingehalten werden müssen. Dazu gehören beispielsweise die Festlegung zulässiger Speicherorte, Mechanismen zur Manipulation der Daten oder die Langzeitspeicherung der Daten.

Kommunikationsverbindung Die Bedeutung der Ressource Kommunikationsverbindung wächst mit der weiteren Verbreitung von Cloud-Computing-Systemen und wird zu einer zentralen Komponente der Cloud-Infrastruktur, da alle Cloud-Services über eine Kommunikationsverbindung bezogen werden. Cloud-Computing-Systeme müssen aus diesem Grund einige Fähigkeiten mitbringen, um dynamische, Service-orientierte Infrastrukturen zu unterstützen und eine zugesicherte Dienstgüte zuverlässig erbringen zu können. Um diese Ziele zu erreichen zu können, werden verschiedene Konzepte angewandt, die darauf abzielen, die Kommunikationsverbindungen der Benutzer voneinander zu isolieren und eine verschlüsselte Punkt-zu-Punkt- oder Ende-zu-Ende-Kommunikation bereitzustellen.

Aus Cloud-Computing-Sicht stellen die Verfügbarkeit der Kommunikationsverbindung und die Sicherstellung der Vertraulichkeit und Integrität eine der wichtigsten Ziele dar, die eine Kommunikationsverbindung für Cloud-Services erfüllen muss. Die Verfügbarkeit wird vor allem durch verteilte Denial-of-Service-Angriffe bedroht [34], die in der Vergangenheit auf fast alle Anbieter von Cloud-Computing-Systemen erfolgreich ausgeführt wurden [9]. Abwehrmaßnahmen gegen verteilte Denial-of-Service-Angriffe in Cloud-Computing-Systemen zielen vor allem auf die schnelle Erkennung eines Angriffs und Begrenzung der Ressourcen ab, die ein Cloud-Service aus dem Ressourcenpool des Cloud-Anbieters beziehen kann.

Zur Sicherstellung der Vertraulichkeit und Integrität der Kommunikationsverbindung sollten alle Nachrichten zwischen zwei Endpunkten verschlüsselt übertragen werden. Dabei sollte auch darauf geachtet werden, dass die Kommunikation innerhalb der Cloud und weiteren beteiligten Serviceanbietern, die für den Endbenutzer nicht sichtbar sind, mit einbezogen werden.

4.6 Nutzungsmodelle von Cloud-Services

Cloud-Services können auf verschiedene Arten, abhängig von der Organisationsstruktur und dem Ort der Bereitstellung, genutzt werden. Üblicherweise werden drei Nutzungsmodelle unterschieden, die im Folgenden näher betrachtet und in Abbildung 4.6 gezeigt werden: öffentliche, unternehmensinterne bzw. private und hybride Nutzung von Cloud-Services.

- Öffentliche Cloud: Die Nutzung eines öffentlichen Cloud-Computing-Systems bezieht sich sowohl auf die öffentliche Verfügbarkeit des Cloud-Serviceangebots als auch auf das öffentliche Netz, über das die Kommu-

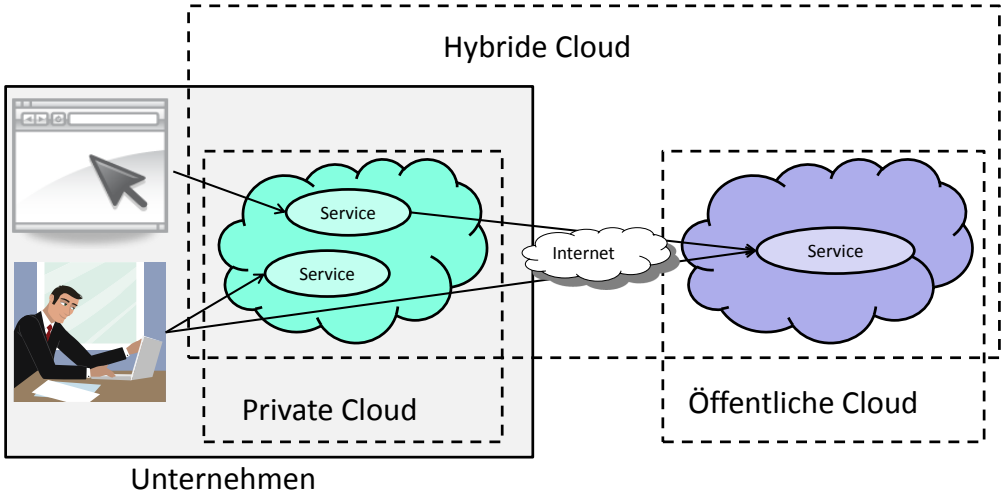

Abbildung 4.6: Privates, öffentliches und hybrides Cloud-Nutzungsmodell

nikation mit dem Cloud-Service erfolgt. Die Cloud-Services und Cloud-Ressourcen werden aus sehr großen Ressourcenpools bezogen, die unter allen Benutzern geteilt werden. Diese IT-Fabriken sind meist speziell für den Betrieb von Cloud-Computing-Systemen gebaut und stellen die Ressourcen in genau der benötigten Menge bereit. Durch die Optimierung des Betriebs, der Pflege und Wartung beim Cloud-Anbieter können hohe Skaleneffekte erzielt werden, die in günstigen Preisen für Cloud-Ressourcen resultieren. Zusätzlich kommen in öffentlichen Cloud-Angeboten Verfahren zur Ressourcenoptimierung zum Einsatz, die jedoch transparent für den Benutzer sind und eine potentielle Bedrohung der Systemsicherheit darstellen. Hat ein Cloud-Anbieter beispielsweise mehrere Rechenzentren, hat er die Möglichkeit, seine Ressourcen so zuzuweisen, dass alle Rechenzentren gleichmäßig ausgelastet werden. Dies kann, wie bereits erwähnt, mit einem Kontrollverlust seitens des Konsumenten einhergehen.

- Unternehmensinterne bzw. private Cloud: Unternehmensinterne bzw. private Cloud-Computing-Systeme sind Cloud-Computing-Systeme, die öffentliche Cloud-Serviceangebote innerhalb der Unternehmensgrenzen und innerhalb des internen Netzwerks nachbilden. In unternehmensinternen Cloud-Computing-Systemen kommen Virtualisierungslösungen zum Einsatz, wobei der Fokus auf der Konsolidierung dezentraler IT-Services liegt. Die Vorteile dieser Systeme liegen in der vollständigen Kontrolle der Daten, der Sicherheitsrichtlinien und der Systemperformanz durch das Unternehmen selbst.

  Allerdings erfordert eine unternehmensinterne Cloud weiterhin den Kauf, den Betrieb und die Wartung der IT-Komponenten, die bei einem öffentlichen Cloud-Computing-System vom Anbieter durchgeführt werden. Des Weiteren lassen sich nur in wenigen Fällen Werte wichtiger Key-Performance-Indikatoren – beispielsweise ein Wert von mehr als 1000 Rechner je Administrator – wie in öffentlichen Cloud-Computing-Systemen erreichen, so dass unternehmensinterne Cloud-Computing-

Systeme gleichzeitig deutlich geringere Kosteneinsparungen bei gleichzeitig aber deutlich geringerem Sicherheitsrisiko erwarten lassen.

Unternehmensinterne Cloud-Computing-Systeme können bei der Bewertung unterschiedlicher Szenarien als Referenzszenario dienen, an dem verschiedene Lösungen verglichen werden. Es ist aber wegen hohen Investitionskosten zu erwarten, dass nur die Unternehmen ein privates Cloud-Computing-System einsetzten werden, die einen hohen Nutzen aus der Konsolidierung bestehender Rechenzentren auf ein privates Cloud-Computing-System realisieren können. Kosteneinsparungen können beispielsweise durch die Ausnutzung der in Kapitel 2 vorgestellten Charakteristika von Cloud-Computing-Systemen und die zentrale und weitgehend automatisierte Administration des Systems entstehen.

- Hybrider Bezug von Cloud-Services: In einem hybriden Modell der Nutzung von Cloud-Services werden Cloud-Services sowohl von einem privaten Cloud-Computing-System als auch von einem öffentlichen Cloud-Computing-System kombiniert, um die geforderten Prozesse zu realisieren. Das hybride Modell der Nutzung von Cloud-Services können auch Unternehmen wählen, die bereits ein vollständiges Outsourcing in der Vergangenheit durchgeführt haben. Sie können Teile ihrer ausgelagerten Services von kostengünstigeren Cloud-Anbietern beziehen und damit die Kosten ihrer bestehenden Outsourcingverträge senken.

Allen Bezugsmodellen ist gemein, dass die Cloud-Serviceangebote durch den Benutzer selbst ausgewählt werden und über das Netzwerk mit Hilfe von Webportalen oder unter Verwendung von Webservice-Technologien genutzt werden. Die Ressourcen werden mit anderen Benutzern geteilt, was eine Sicherheitsimplikation darstellen kann, und es wird nach verbrauchten Ressourcen abgerechnet.

Welches der drei Bezugsmodelle von Cloud-Services in Unternehmen zum Einsatz kommen wird, hängt häufig von den Richtlinien ab, die Unternehmen im Bezug auf die Sicherheit und die gesetzliche Bestimmungen einzuhalten haben. Es ist jedoch zu erwarten, dass die Entscheidung abhängig vom Prozess oder der Anwendung getroffen wird. Kritische Systeme würden durch Konsolidierung interner Rechenzentren in ein privates Cloud-Computing-System transferiert, während für standardisierte Prozesse ein öffentliches Cloud-Computing-System genutzt werden würde. Durch dieses Vorgehen würde ein hybrides Nutzungsmodell von Cloud-Computing-Systemen entstehen, was für die meisten Unternehmen einen Kompromiss zwischen Risiko und Nutzen darstellen kann.

5 Taxonomie der Sicherheitsaspekte von Cloud-Computing-Systemen

Nach der Vorstellung der Schutzziele in Kapitel 3 und des Aufbaus von Cloud-Computing-Systemen aus Servicesicht in Kapitel 4 wird in diesem Kapitel eine Taxonomie des Sicherheitsaspekte von Cloud-Computing-Systemen eingeführt. Diese Taxonomie umfasst die wichtigsten Sicherheitsaspekte, die beim Einsatz von Cloud-Services beachtet werden müssen. Das Ziel der Taxonomie ist die Definition eines flexiblen Rahmens, der es Entscheidern und IT-Verantwortlichen ermöglicht, je nach Einsatzbereich eines Cloud-Services, einzelne Bereiche in Bezug auf das angestrebte Sicherheitsniveau stärker zu gewichten, und der eine Gesamtbewertung der Cloud-Sicherheitsrisiken zulässt. Die Sicherheitsrisiken können beispielsweise in eine detaillierte Risiko-Nutzen-Analyse einfließen und als Grundlage für die Evaluierung geeigneter Sicherheitsmaßnahmen herangezogen werden.

Dieses Kapitel stellt das methodische Vorgehen bei der Analyse der Risiken von Cloud-Services vor. Im Fokus stehen dabei die Schutzziele, die beim Einsatz von Cloud-Services erreicht werden sollten, aufgegliedert nach verschiedenen Problemfeldern, die eine Einschränkung eines oder mehrerer Schutzziele zur Folge haben können. Da bei der Auswahl und Bewertung von Cloud-Services jedoch häufig auch die Kosten der Dienste eine sehr wichtige Rolle spielen, werden auch ökonomische Kriterien für Cloud-Services beschrieben, die neben den Sicherheitskriterien zur Auswahl herangezogen werden.

Für die Erarbeitung der Taxonomie wurden verschiedene Vorarbeiten von Gartner [24] und der Cloud-Security-Alliance [10] verwendet, die eine erste Einordnung der Cloud-Sicherheitsthematik vorgenommen haben. Die Taxonomie dieser Studie erweitert diese Vorarbeiten und spezifiziert eine detailliertere Taxonomie der Cloud-Sicherheitsaspekte. Die Taxonomie der Cloud-Computing-Risiken kann als Landkarte angesehen werden, die wichtige sicherheitsrelevante Aspekte beim Bezug von Cloud-Services betrachtet und damit als Ausgangspunkt für eine tiefer gehende Sicherheitsbetrachtung dienen kann.

Die vier Bereiche der Taxonomie, nämlich Infrastruktur, Anwendung und Plattform, Verwaltung und Compliance und deren weitere Untergliederung wird in Kapitel 5.1 eingeführt. In Abschnitt 5.2 werden Sicherheitsaspekte der Infrastruktur beschrieben und in Abschnitt 5.3 werden Sicherheitsaspekte der Anwendung und Plattform vorgestellt. Die weiteren Bereiche der Taxonomie, Verwaltung und Compliance, werden in Abschnitt 5.4 und Abschnitt 5.5 betrachtet.

5.1 Aufbau der Taxonomie

Der Aufbau der Taxonomie orientiert sich an den Schichten des Bezugsmodells von Cloud-Computing-Systemen, das in Kapitel 4 eingeführt wurde und erweitert diese um die zwei Querschnittsbereiche Verwaltung und Compliance. Abbildung 5.1 zeigt den Aufbau der Taxonomie. In dieser Abbildung ist eine Änderung an dem bekannten dreigliedrigen Bezugsmodell zu erkennen. Für die Taxonomie wurden die Anwendungs- und Plattformschicht zusammengefasst. Die Unterscheidung der beiden Schichten erfolgt durch untergeordnete Sicherheitsaspekte innerhalb des zusammengeführten Bereichs aus Anwendungs- und Plattformschicht.

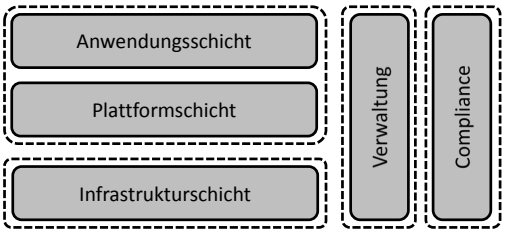

Abbildung 5.1: Taxonomie der Sicherheitsaspekte von Cloud-Computing-Systemen

Abbildung 5.2 gibt eine Übersicht über den Aufbau der Taxonomie der Sicherheitsaspekte von Cloud-Computing-Systemen und ihrer untergeordneten Sicherheitsrisiken. Sie gliedert sich in die 4 Hauptbereiche Infrastruktur, Anwendung und Plattform, Verwaltung und Compliance. Jeder dieser Hauptbereiche und die dazugehörigen Sicherheitsrisiken werden in den folgenden Abschnitten detailliert vorgestellt und eine Checkliste mit Fragen spezifiziert, die ein Cloud-Konsument einen Cloud-Anbieter fragen sollte.

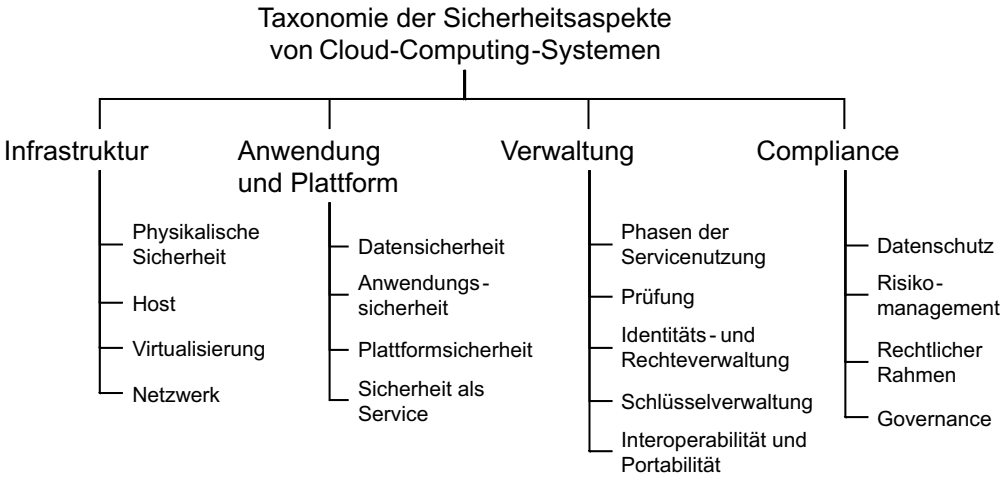

Abbildung 5.2: Taxonomie der Sicherheitsaspekte von Cloud-Computing-Systemen

Zur weiteren Erläuterung, wie die Taxonomie angewandt werden kann, werden im Folgenden die Abhängigkeiten der einzelnen Bereiche näher analysiert und in Abbildung 5.3 dargestellt. Ein Pfeil zwischen den Bereichen bedeutet, welcher Bereich von einem anderen abhängig ist. Die Anzahl der eingehenden Pfeile bedeutet die Wichtigkeit des Bereichs für das Gesamtrisiko der Sicherheit eines Cloud-Service. Nach diesem Schema ist die Sicherheit der Infrastruktur als

am wichtigsten einzuordnen gefolgt von der Sicherheit des Bereichs Anwendung und Plattform. Der Bereich der Verwaltung weißt die geringsten Abhängigkeiten mit nur einem eingehenden Pfeil auf.

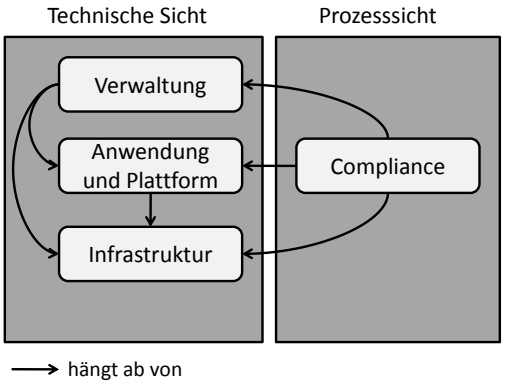

Abbildung 5.3: Abhängigkeiten der einzelnen Bereiche der Taxonomie

Des Weiteren integriert die Taxonomie zwei verschiedene Sichten auf die Sicherheit von Cloud-Computing-Systemen. Die technische Sicht umfasst die Bereiche Infrastruktur, Anwendung und Plattform und Verwaltung, während die Prozesssicht den Bereich Compliance beinhaltet. Die Abbildung zeigt, dass die Verwaltung von den technischen Gegebenheiten der Infrastruktur, der Anwendung und der Plattform abhängt. Ein Cloud-Konsument kann nur die Verwaltungsfunktionen nutzen, die ihm ein Cloud-Anbieter zur Verfügung stellt. Die Compliance hängt wiederum von der technischen Sicht ab, da die Compliance für den Cloud-Konsumenten nur sehr schwierig ohne Unterstützung des Cloud-Anbieters und dessen technischer Systeme und organisatorischer Prozesse zu realisieren ist. Aus diesem Grund ist es für einen Cloud-Konsumenten wichtig, möglichst alle Sicherheitsaspekte der Taxonomie bei der Auswahl eines Cloud-Anbieters zu untersuchen und Maßnahmen mit ihm abzustimmen, um die Sicherheitsrisiken auf ein durch den Cloud-Konsumenten vorher definiertes Niveau zu reduzieren.

5.2 Infrastruktur

Der Infrastrukturbereich der Taxonomie betrachtet die Sicherheitsrisiken, denen Services auf der Infrastrukturschicht ausgesetzt sind. Die Infrastrukturschicht gliedert sich in die vier Bereiche physikalische Sicherheit, Host, Virtualisierung und Netzwerk, die die Kernkomponenten der Cloud-Infrastruktur bilden. Ein Benutzer eines Cloud-Infrastrukturservices hat im Allgemeinen keinen Einfluss auf diese Kernkomponenten, er sollte sich aber der möglichen Sicherheitsbedrohungen auf dieser Ebene bewusst sein. Auch eine Evaluierung der Sicherheit einer Cloud-Infrastruktur ist wegen deren Komplexität für einen Benutzer nur sehr schwer durchzuführen, so dass er an dieser Stelle meist dem Cloud-Ressourcenanbieter vertrauen muss.

5.2.1 Physikalische Sicherheit

Die physikalische Sicherheit von Cloud-Computing-Systemen umfasst die Gebäude und die Gebäudetechnik, in denen die Cloud-Computing-Systeme untergebracht sind. Im Einzelnen sind hier die Stromversorgung und Kühlung der Rechner, aber auch die Zutrittskontrolle des Gebäudes, Videoüberwachung sowie Ort und Aufbau des Gebäudes aus Sicherheitssicht relevant [10] [21]. Ein Stromausfall kann beispielsweise Auswirkungen aus das Schutzziel Verfügbarkeit haben [39]. Werden Rechner aus dem Gebäude durch z. B. Diebstahl entfernt, kann dies eine Verletzung des Schutzziels Vertraulichkeit darstellen. Der Aufbau des Gebäudes kann Auswirkungen auf die Erweiterbarkeit des Cloud-Computing-Systems haben und zu Engpässen hinsichtlich der Performanz bei starkem Wachstum eines Cloud-Anbieters führen.

Die meisten Unternehmen beauftragen externe Unternehmen mit der Bewachung ihrer Gebäude [7]. Es ist zu überprüfen, wer Zugang zu welchen Bereichen eines Rechenzentrums besitzt und dies gegebenenfalls schriftlich bei einem Cloud-Anbieter einfordern. Zusätzlich sollte festgehalten werden, welche Ereignisse der Cloud-Anbieter einem Cloud-Konsumenten mitteilen muss. Kandidaten hierfür sind Stromausfälle, Ausfall der Videoüberwachung, Änderung der Zugangskontrolle des Gebäudes oder der Umzug der Rechner in ein neues Rechenzentrum.

Checkliste der physikalischen Sicherheit

- Besteht Zugriff auf die Videoüberwachung oder die Aufzeichnungen der Zutrittskontolle des Cloud-Anbieter bei einem meldepflichtigen Vorfall?
- Verwenden alle Rechenzentren des Cloud-Anbieters die gleichen Standards bezüglich der physikalischen Sicherheit?
- Welche Maßnahmen zur Sicherstellung der physikalischen Sicherheit besitzt das Rechenzentrum, in dem die Daten des Cloud-Konsumenten liegen?
- Wie ist das Rechenzentrumsgebäude gesichert?
- Wie sind die Zugänge zum Gebäude gesichert?
- Werden Zugangskarten, biometrische Verfahren, Videoüberwachung, Gebäudebewachung, und eine ständige Begleitung von Gästen im Rechenzentrum garantiert?
- Welche Alarmsysteme werden eingesetzt?

5.2.2 Host

Der Host stellt die Umgebung dar, auf dem die Prozesse und deren Berechnungen zur Ausführung kommen. Dies stellt besondere Anforderungen an die Sicherheit im Hinblick auf den Schutz der Daten, die verarbeitet werden, der Verfügbarkeit des Hosts und der Zuverlässigkeit der Ausführung von Berechnungen auf dem Host.

Mögliche Bedrohungen der Schutzziele der Daten haben ihren Ursprung meist in den ausgeführten Anwendungen, die außerhalb der Benutzerumgebung laufen und Daten der Benutzerumgebung beeinflussen können. Wenn eine Anwendung eines potentiellen Angreifers die Möglichkeit hat, lokale Daten – lokal bezieht sich auf den gleichen physischen Rechner auf dem Angreifer und Benutzer ihre Anwendungen ausführen – zu beeinflussen, so kann er diese verändern, zerstören oder die lokale Umgebung nicht mehr benutzbar zu machen. Isolierung hilft dabei, externe Anwendungen von potentiellen Angreifern in einer geschützten Umgebung zu halten und auszuführen, so dass es einer bösartigen Anwendung im Idealfall nicht möglich ist, seine ihm zugewiesene Umgebung zu verlassen. In Cloud-Computing-Systemen kommt das Konzept der Virtualisierung zum Einsatz, um eine Isolierung von mehreren Benutzerumgebungen zu erreichen. Der direkte Zugriff auf die Ressourcen des Hosts ist nicht mehr erlaubt, sondern wird durch einen Virtual Machine Monitor gesteuert. Es sollte zu jeder Zeit nachvollziehbar sein und dokumentiert werden, welcher Prozess oder welcher Akteur auf den Host zugegriffen hat. Dies erleichtert die Überprüfung der Sicherheit des Systems durch den Benutzer.

Eine weitere Bedrohung der Schutzziele stellt die Ausführung von Anwendungen durch einen Benutzer dar. Für die Ausführung einer Anwendung müssen Ressourcen des Hosts häufig über die Abstraktionsebene einer virtuellen Maschine zugewiesen werden. Dabei kann es zu einem sogenannten Verhungern einer Anwendung kommen [41] [14]. Von einem Verhungern einer Anwendung wird gesprochen, wenn eine benachbarte Anwendung oder eine Anwendung höherer Priorität sehr viele Ressourcen eines Host verbraucht und damit die Ausführung einer anderen Anwendung unmöglich macht. Die Bedeutung dieses Szenarios hängt stark von der Intensität ab, mit der Anwendungen Ressourcen eines Hosts konsumieren und die Auslastung des Hosts beeinflussen.

In kommerziellen Cloud-Serviceangeboten ist es in der Vergangenheit vor allem bei übermäßiger Nutzung von Ressourcen zu Engpässen gekommen, die ein Verhungern von Anwendungen zur Folge hatten [9]. Auslöser waren beispielsweise verteilte Denial-of-Service Angriffe, die darauf abzielten, die Zuverlässigkeit und Verfügbarkeit der Ressourcen eines Anbieters negativ zu beeinflussen. Um das Risiko eines Verhungerns eines Anwendung zu vermeiden, sollten Ressourcenservices mit einer konstant hohen Performanz ausgewählt – dies kann beispielsweise durch Abfrage von Überwachungsdiensten und Analyse der Performanzhistorie festgestellt werden – und/oder Strafen bei der Verletzung von

Dienstgütekriterien wie beispielsweise Verfügbarkeit vertraglich festgeschrieben werden.

Checkliste der Sicherheit des Hosts

- Werden Verfahren zur Verhinderung des Verhungern von Anwendungen angewandt?
- Wie werden die Prozesse unterschiedlicher Benutzeranwendungen voneinander isoliert?
- Welche Verfahren zur Abschottung der Hosts werden eingesetzt?
- Wer hat Zugriff auf die Hosts im Rechenzentrum des Anbieters?

5.2.3 Virtualisierung

Wie bereits im vorangegangenen Abschnitt erwähnt, wird vor allem Virtualisierung in Cloud-Computing-Systemen eingesetzt, um eine Isolierung von Benutzerumgebungen zu erreichen, und ist dadurch ein wichtiger Grundbaustein der Cloud-Computing-Systeme. Virtualisierung wird aktuell hauptsächlich in Rechenzentren eingesetzt, um Rechner zu konsolidieren und die Auslastung des Rechenzentrums zu erhöhen. Die Fähigkeit eine sichere Umgebung durch Isolierung zu schaffen, ist ein Nebenprodukt der Virtualisierungslösungen und eine Grundvoraussetzung für die Trennung von Benutzerumgebungen und für die Einhaltung der in Kapitel 3 definierten Schutzziele.

Bedrohungen auf Ebene der Virtualisierung haben häufig ihren Ursprung in der Verwaltung von Zugriffsberechtigungen und der dynamischen Natur der Cloud-Computing-Systeme. Es sollte vor dem Einsatz von Cloud-Computing-Systemen genau festgelegt werden, welcher Benutzer Berechtigungen für die Verwaltung der virtuellen Maschinen hat, wie die Dateiberechtigungen der virtuellen Maschine definiert sind und welche Berechtigungen das Gastbetriebssystem besitzt. Zusätzlich zu den Berechtigungen, die auf den Host bezogen sind, sind auch Berechtigungen auf Netzwerkebene, wie die Konfiguration einer Host-basierten Firewall oder der Zugriff zu weiteren Internet- bzw. Cloud-Ressourcen, zu setzen.

Aktuelle Virtualisierungslösungen wie beispielsweise Xen[1], KVM[2], VMWare ESX[3] oder Microsofts Hyper-V[4] bieten das Verschieben von virtuellen Maschinen zwischen Hosts an, was eine Verletzung eines oder mehrerer Schutzziele wie

[1] http://xen.org/
[2] http://www.linux-kvm.org/page/Main_Page
[3] http://www.vmware.com/de/
[4] http://www.microsoft.com/hyper-v-server/en/us/default.aspx

beispielsweise den Schutz der Privatsphäre zur Folge haben kann. In diesem Zusammenhang ist zu überprüfen, ob ein Anbieter von Cloud-Services diese Funktion nutzt und welche Folgen sich daraus ergeben können. Zusätzlich sollte der Anbieter Angaben zum geographischen Ort der virtuellen Maschine machen oder ein Testat darüber vorweisen, da dieser beispielsweise durch gesetzliche Vorschriften festgelegt sein kann.

Checkliste der Virtualisierungsicherheit

- Welche Virtualisierungstechnologie wird von dem Cloud-Anbieter verwendet?
- Wie stellt der Cloud-Anbieter sicher, dass die Isolierung der virtuellen Maschinen eingehalten wird und eine virtuelle Maschine beispielsweise nicht auf den Speicherbereich der jeweils anderen zugreifen kann?
- Mit welchen Maßnahmen werden die virtuellen Maschinen geschützt?
- Wie wird verhindert, dass fehlerhafte virtuelle Maschinen einen Speicherangriff durch z. B. Ausnutzung einer Sicherheitslücke verursachen?
- Was wird unternommen, wenn ein Virtual Machine Monitor (VMM) kompromittiert wird?
- Wie sicher ist der Kommunikationskanal zwischen den virtuellen Maschinen und dem VMM?

5.2.4 Netzwerk

Das Netzwerk und seine Komponenten wie Kommunikationsprotokolle und Filtertechnologien ist ein weiterer wichtiger Teil der Infrastruktur, der Einfluss auf die Sicherheit des Cloud-Computing-Systems haben kann. Kommunikationsprotokolle zielen darauf ab, eine einheitliche Nutzung der Cloud-Services durch Benutzer und zwischen den Rechnern eines oder mehrerer Cloud-Computing-Systeme zu ermöglichen, während Filtertechnologien wie Firewall, Intrusion-Detection-Systeme (IDS) oder Intrusion-Prevention-Systeme (IPS) eingesetzt werden, um nur bestimmte Netzwerkverbindungen zuzulassen und somit böswilliges Eindringen in das System zu verhindern.

Im Folgenden wird eine kurze Übersicht über Sicherheitsaspekte des Netzwerks eines Cloud-Computing-Systems gegeben, da eine umfassende Betrachtung den Rahmen dieser Studie sprengen würde. Cloud-Computing-Systeme benötigen üblicherweise eine zuverlässige Netzinfrastruktur zu ihrem Funktionieren, so dass ein umfassendes Verständnis der Netzsicherheit sowohl auf der Seite der Cloud-Benutzer wie auch auf der Seite der Cloud-Anbieter notwendig ist. Die Herausforderungen aus Sicht der Netzsicherheit für Cloud-Computing-Systeme beruhen auf der Einhaltung der in Kapitel 3 eingeführten Schutzziele und den typischen Anforderungen der Cloud-Services, die einen geografisch

und Endgeräte-unabhängigen Zugriff unter Einbezug heterogener Netzinfrastrukturen ermöglichen sollen. Des Weiteren sollten nicht nur Cloud-spezifische Sicherheitsaspekte von Netzen, sondern auch das sichere Weiterleiten von Nachrichten und sicheres Multicasting berücksichtigt werden.

Ausgehend vom ISO/OSI-Schichtenmodell [1] kann die Kontrolle des Netzzugangs und wichtige Sicherheitsfunktionen auf verschiedenen Ebenen wie beispielsweise auf der IP-Ebene durch IPSec oder durch TLS/SSL auf der Transportschicht realisiert werden. Dabei kommen Verfahren zur Isolierung des Netzverkehrs durch Virtualisierung, Zugangskontrolle durch Firewalls, Integration von VPN-Technologien in Cloud-Services sowie zum Erkennen und Entfernen verdächtiger Netzwerkpakete durch IDS- bzw. IPS-Systeme zum Einsatz.

Checkliste der Netzsicherheit

- Welche Verfahren und Systeme des Netzsicherheit setzt ein Cloud-Anbieter ein?
- Welche Technologien werden eingesetzt, um Netzangriffe wie z. B. Denial-of-Service-Angriffe, Man-in-the-Middle-Angriffe oder Port-Scanning zu verhindern?
- Wie sind diese Systeme konfiguriert?
- Welche Konfigurationen kann bzw. muss der Cloud-Konsument durchführen?
- Wie wird auf Sicherheitsvorfälle reagiert? Gibt es ein Vorgehensmodell?

5.3 Anwendung und Plattform

Im Fokus des Bereichs Anwendung und Plattform der Cloud-Taxonomie stehen Sicherheitsrisiken, die bei der Entwicklung und Nutzung von Cloud-Services entstehen können und ihren Ursprung sowohl in der Infrastruktur als auch in der als Service bereitgestellten Anwendung und der dazugehörigen Plattform haben können. Dabei spielen Einflüsse aus den Gebieten der Sicherheit von Service-orientierten Architekturen, und der Sicherheit von Webanwendungen eine wichtige Rolle, um die Schutzziele für schützenswerte Daten, Anwendungen und Prozesse in Cloud-Computing-Systemen zu gewährleisten. Im Rahmen der Taxonomie der Sicherheitsaspekte von Cloud-Computing-Systemen wurden die folgenden Bereiche identifiziert, die im weiteren Verlauf dieses Abschnitts näher betrachtet werden: Datensicherheit, Anwendungssicherheit, Plattformsicherheit und Sicherheit als Service.

5.3.1 Datensicherheit

Unter dem Begriff der Datensicherheit wird im Rahmen dieser Studie die Sicherheit aller Daten – inklusive eventuell vorhandener Konfigurations- und Metadaten – verstanden, die in Cloud-Computing-Systemen gespeichert, verarbeitet und zwischen Cloud-Computing-Systemen und deren Services transportiert werden. Dabei stehen die Schutzziele Vertraulichkeit und Integrität im Vordergrund.

Analog zum klassischen Auslagern der IT zu einem Outsourcing-Anbieter, der die Daten eines Unternehmens im Zuge des Auslagerns der IT übernimmt, werden die Daten eines Cloud-Benutzers ebenfalls auf den Rechnern eines Cloud-Anbieters gespeichert. Dies hat zur Folge, dass der Cloud-Serviceanbieter Sicherheitsfunktionen implementieren und bereitstellen muss, die diese Daten schützen, und gegebenenfalls dem Cloud-Benutzer Rechenschaft darüber ablegen muss.

Vor dem Übermitteln von Daten an einen Service eines Cloud-Anbieters sollte ein Cloud-Konsument eine Klassifikation seiner Daten vornehmen und genau festlegen, welche Daten bei einem Cloud-Anbieter gespeichert werden dürfen. In dieser Klassifikation muss genau spezifiziert werden, mit welchen Sicherheitsmaßnahmen die Daten übermittelt und abgespeichert werden müssen. Dies können bestimmte kryptografische Verfahren oder aber auch Richtlinien sein, die ein Anbieter unterstützen muss. Zur Sicherstellung der Schutzziele bieten sich die Festlegung von Sicherheitsrichtlinien an, die vom Anbieter eingehalten werden müssen. In diesen Sicherheitsrichtlinien kann beispielsweise die Verwendung bestimmter Verschlüsselungstechnologien wie beispielsweise Public-Key-Infrastrukturen (PKI) vorgeschrieben werden. Üblicherweise werden mit dem Cloud-Anbieter die Schlüssel für die sichere Übertragung und Speicherung der Daten ausgetauscht und diese auf den Daten angewandt. Die Schlüsselverwaltung wird im Bereich Verwaltung der Taxonomie noch weiter vertieft.

Zusätzlich kann durch einen Cloud-Konsumenten da Prinzip der Datenminimierung angewandt werden, bei dem z. B. Kundendaten aus den Datensätzen, die durch einen Cloud-Service verarbeitet werden, entfernt oder ersetzt werden und nur durch Daten, die unternehmensintern vorgehalten werden, wieder ihre ursprünglich semantisch Bedeutung erlangen. Ein solches Szenario kann beispielsweise bei rechenintensiven Statistikberechnungen angewandt werden, wo beispielsweise nur Zahlen für die Berechnung benötigt werden, die Zuweisung zu einem Kunden aber für die eigentliche Berechnung nicht notwendig ist.

Checkliste der Datensicherheit

- Wo werden die Daten gespeichert und wie sind diese von den Daten anderer Kunden getrennt? Werden die Daten auf den Rechnern des Cloud-Anbieters durch diesen verschlüsselt angelegt?
- Wo werden die Daten zusätzlich z. B. bei der Datensicherung und -archivierung oder durch Redundanz des Cloud-Computing-Systems gespeichert?

- Für wen sind die Daten im gespeicherten Zustand, während der Verarbeitung und bei der Übertragung über ein Netzwerk sichtbar?
- Wer kann auf die Daten zugreifen, wenn diese gespeichert sind oder sich in Verarbeitung oder in der Übertragung befinden?
- Sind die Daten so gesichert, so dass diese nur für den Besitzer der Daten sichtbar und nutzbar sind?
- Werden bei einer Löschung die Daten von allen Instanzen, allen Zwischenspeichern und allen Sicherungskopien gelöscht?
- Welche Verschlüsselungsverfahren bietet der Cloud-Anbieter an? Ist eine Verwendung dieser Verfahren im Vertrag festgeschrieben?
- Können Sicherungskopien verschlüsselt werden?
- Welche Richtlinien und Verfahren für die Erstellung, Verteilung und Verwaltung der Daten und deren Replica wendet der Cloud-Anbieter an?
- Können Daten nach einer Löschung wiederhergestellt werden?
- Ist es möglich die Daten wieder in das Unternehmen zurückzuholen?
- Ist es möglich die gespeicherten Daten mit anderen Cloud-Konsumenten zu teilen?

5.3.2 Anwendungssicherheit

Der Bereich der Anwendungssicherheit umfasst Verfahren und Methoden zur Sicherstellung des authentifizierten Zugangs zu Cloud-Services und des Einbezugs von Sicherheitskriterien bei der Entwicklung von Cloud-Services. Des Weiteren wird neben der Vertraulichkeit eine Einhaltung der Schutzziele Integrität, Verfügbarkeit und Authentizität gefordert. Da eine Anwendung in Cloud-Computing-Systemen als Service über ein meist öffentliches Netzwerk zugänglich gemacht wird, sollten folgende Themen im Rahmen der Anwendungssicherheit betrachtet werden:

- Nachrichten: Die Nachrichten sollten verschlüsselt unter Verwendung von Webservice-Sicherheitsstandards (z. B. WS-Security [2]) übertragen werden und gegen erneutes Verschicken derselben Nachricht (Replay-Angriff) geschützt sein. Zusätzlich sollten Nachrichten signiert und gegen ein Schema – z. B. unter Verwendung des XML-Schema Standards [3] – validiert werden können, um zum einen den Sender identifizieren zu können und zum anderen fehlerhafte Nachrichten vor der eigentlichen Verarbeitung erkennen zu können.

- Sitzung: In Cloud-Computing-Systemen wird häufig seitens des Anbieters die Sitzung mitprotokolliert, da auf deren Basis die Abrechnung erfolgt. Eine Sitzung definiert sich als die Zeitspanne zwischen dem Aufbau und dem Abbau der Verbindung zum Cloud-Anbieter. In diesem Zusammenhang sollte eine böswillige Übernahme einer nicht mehr aktiven Sitzung verhindert werden, um einen Missbrauch zu vermeiden.
- Konfiguration: Ein Cloud-Service sollte gegen böswillige Veränderung der Konfiguration geschützt sein. Dies kann beispielsweise durch eine spezielle Administrationsschnittstelle erfolgen, die nur wenigen Benutzern zugänglich ist.
- Ausnahmen: Ausnahmen in Cloud-Services sollten andere Benutzer bei der Ausführung ihres Services nicht beeinträchtigen.

Weitere Bedrohungen der Anwendungssicherheit können ihren Ursprung in Malware-Infektionen, Medienbrüchen bei der Verarbeitung der Daten durch die Anwendung, Man-In-the-Middle Angriffen oder in der Nachahmung von Cloud-Benutzern haben. Da es sich bei Cloud-Services häufig um Webanwendungen handelt, haben auch die wichtigsten Bedrohungen für Webanwendungen eine hohe Relevanz für Cloud-Computing-Systeme. An dieser Stelle wird auf die Arbeiten der OWASP Foundation verwiesen, die in regelmäßigen Abständen die wichtigsten Bedrohungen von Webanwendungen zusammenstellt [36].

Die Ziele dieser Angriffe sind Schäden durch die Verletzung der Schutzziele, aus denen zusätzlich ein ökonomischer Schaden durch übermäßige Nutzung eines Cloud-Services entstehen kann, der dem Cloud-Benutzer in Rechnung gestellt wird. In diesem Zusammenhang wird häufig von einem ökonomischen Angriff gesprochen im Gegensatz zu verteilten Denial-of-Service-Angriffe, die vor allem auf das Schutzziel Verfügbarkeit abzielen.

Checkliste der Anwendungssicherheit

- Welche Verfahren werden verwendet, um die Anwendung von den Daten, der Plattform und der Infrastruktur zu trennen?
- Wie sieht die Ausführungsumgebung der Cloud-Services aus? Welche weiteren Services sind bei der Ausführung beteiligt? Wie sehen deren Sicherheitsfunktionen aus?
- Finden regelmäßige Sicherheitsüberprüfungen der Cloud-Services durch den Anbieter und externe Dienstleister statt?
- Sind die Ergebnisse von Sicherheitsüberprüfungen dokumentiert?
- Welche Authentifizierungsmechanismen werden angeboten und sind diese Mechanismen angemessen für die Sensitivität der Daten?
- Welche Profil- und Passwortkontrollen werden verwendet, um einen Missbrauch zu vermeiden?

- Werden Überwachungswerkzeuge auf Anwendungsebene angeboten, mit den deren Hilfe sicherheitsrelevante Vorfälle aufgespürt werden können?
- Wie werden Zeitüberschreitungen einer Sitzungen behandelt?

5.3.3 Plattformsicherheit

Die Plattformsicherheit zielt vor allem auf Entwickler von Cloud-Services ab, die eine Cloud-Plattform wie beispielsweise Microsoft Azure, Google App Engine oder Force.com für die Entwicklung eigener Cloud-Anwendungen einsetzen. Cloud-Konsumenten, deren Cloud-Service der Anwendungsschicht auf einer Cloud-Plattform ausgeführt werden, können von den Sicherheitsfunktionen der Plattform profitieren oder im Fall einer Sicherheitsbedrohung davon betroffen sein.

Wichtige Sicherheitsmerkmale der Plattform beziehen sich auf die Entwicklungsprozesse der Cloud-Anwendungen und die Werkzeuge, die dabei zum Einsatz kommen. Des Weiteren ist die Isolierung der Anwendungen und Daten auf einer Cloud-Plattform für die Einhaltung der Schutzziele essentiell. Sichere Entwicklungsprozesse müssen hier zur Anwendung kommen, um dies seitens der Plattform und der Anwendung sicher zu stellen. Vor allem neuartige Angriffsvarianten auf Grundlage von Seitenkanalattacken stellen hier eine Bedrohung dar. Seitenkanalattacken sind eine bekannte Angriffsmethode auf Hardwaresicherheitsmodule, wurden jedoch auch erfolgreich in Cloud-Computing-Systemen zur Überwindung der Isolierung der Benutzerumgebungen angewandt [33].

Checkliste der Plattformsicherheit

- Welche sicheren Entwicklungsverfahren kommen zum Einsatz?
- Werden die Services einer Cloud-Plattform einer kontinuierlichen Sicherheitsüberprüfung unterzogen?
- Sind die Ergebnisse der Sicherheitsüberprüfungen dokumentiert?
- Welche Maßnahmen zur Isolierung der Anwendungen und Daten werden auf der Cloud-Plattform verwendet?
- Wo werden die Benutzerdaten und -anwendungen über die Cloud-Plattform auf der Cloud-Infrastruktur abgelegt?
- Wie werden die Anwendungen auf der Cloud-Plattform bereitgestellt und wieder aus der Plattform entfernt?
- Bietet die Cloud-Plattform Funktionen zur Einhaltung der Schutzziele, wie beispielsweise die Integrität der Informationen, an?

5.3.4 Sicherheit als Service

Der Bereich Sicherheit als Service aus dem Bereich der Architektur der Cloud-Taxonomie umfasst verschiedene Modelle, mit denen Sicherheitsfunktionen als Mehrwertdienst, der meist von einem Cloud-Benutzer zu bezahlen ist, zu bestehenden Sicherheitsfunktionen eines Cloud-Service hinzugefügt werden können. Ziel ist es, ein bestimmtes Sicherheitsniveau zu erreichen, ohne dass Änderungen am eigentlichen Service vorgenommen werden müssen. Die Bereitstellung eines solchen Service kann durch den Cloud-Serviceanbieter selbst oder durch einen vertrauenswürdigen Dritten erfolgen, wobei für die Bereitstellung von Sicherheitsfunktionen als Service auch auf Cloud-Ressourcen zurückgegriffen werden kann.

Beispiele hierfür finden sich im Bereich Identitäts- und Zugangsverwaltung durch Single-Sign-On-Services für Cloud-Anbieter oder im Bereich der Verwaltung von Cloud-Services selbst. Die Verwaltung von Cloud-Services bieten beispielsweise Funktionen zur automatisierten Verwaltung der Instanzen eines Service an, um eine gleichbleibend hohe Verfügbarkeit zu gewährleisten. Ist eine Instanz eines Service nicht mehr erreichbar, wird automatisch eine neue Instanz bereitgestellt.

Checkliste der Sicherheit als Service

- Ist eine vollständige Dokumentation der Sicherheitsarchitektur vorhanden?
- Werden spezielle Sicherheitsaspekte wie Anwendungssicherheit und Plattformsicherheit betrachtet, auf der die Sicherheitsfunktionen als Service bereitgestellt werden?
- Gibt es ein Sicherheitstestat für die Cloud-Services?
- Wie lassen sich die Sicherheitsfunktionen als Service integrieren? Gibt es offene Schnittstellen und ein benutzerfreundliches Portal?
- Welche Cloud-Anbieter und Cloud-Services werden unterstützt?
- Wo werden die sicherheitsrelevanten Daten gespeichert?

5.4 Verwaltung

Eine der größten Herausforderungen aus Sicherheitssicht stellt der Bereich der Verwaltung von Cloud-Services dar. Zum einen wird dieser noch unzureichend von Cloud-Anbietern unterstützt und zum anderen stehen Cloud-Benutzer noch keine Werkzeuge zur Verfügung bzw. befinden sich in der Entwicklung, mit denen sie eine integrierte und effiziente Verwaltung ihrer angemieteten Cloud-Services durchführen können. Dieser Bereich ist in seiner Gesamtheit

noch Gegenstand aktueller Forschung und es ist zu erwarten, dass es noch Zeit benötigt, bis die Verwaltung von Cloud-Services das gleiche Qualitätsniveau bestehender Programme und Werkzeuge in Unternehmensnetzen erreicht.

In den folgenden Abschnitten werden die typischen Phasen der Nutzung eines Cloud-Services betrachtet, die Sicherheitsaspekte bei der Prüfung von Cloud-Services beschrieben und die Sicherheitsrisiken der Identitäts-, Rechte- und Schlüsselverwaltung von Cloud-Computing-Systemen vorgestellt.

5.4.1 Phasen der Servicenutzung

Die Phasen der Nutzung eines Cloud-Services werden in der Taxonomie der Sicherheitsaspekte von Cloud-Computing-Systemen analog zu den Schritten einer Transaktion im E-Commerce gesehen, mit dem Ziel, die Transaktionskosten zu senken. Die 5 Phasen einer Transaktion sind: Anbahnung, Vereinbarung, Ausführung, Anpassung und Kontrolle sowie Durchsetzung. Abbildung 5.4 zeigt die Phasen der Servicenutzung, die bei jeder Nutzung von Cloud-Services neu durchlaufen wird.

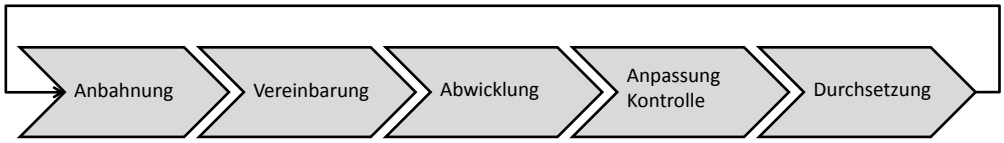

Abbildung 5.4: Phasen der Nutzung eines Cloud-Services

In der Anbahnungsphase veröffentlicht der Cloud-Serviceanbieter die Beschreibung seines Produkts. Ein Cloud-Konsument startet eine Suche nach Cloud-Serviceangeboten mit Hilfe von vorher festgelegten funktionalen und nichtfunktionalen Kriterien. Da es aktuell noch kein standardisiertes Format für die Suche nach Cloud-Services gibt, erfolgt die Suche meist über die Webseiten der jeweiligen Anbieter von Cloud-Services. Vereinzelt sind Kataloge oder Verzeichnisse von Cloud-Services einer Plattform verfügbar, die den Cloud-Benutzer bei der Suche unterstützen können. Eine Beschreibung von unterstützten Sicherheitsfunktionen findet sich jedoch nur sehr selten bei Cloud-Anbietern, so dass es aktuell sehr aufwändig ist, ein umfassendes Bild eines Cloud-Services und seiner Sicherheitsfunktionen zu bekommen. Weiterhin sollten bei der Suche Kriterien, wie z. B. Plattformunabhängigkeit und Interoperabilität, eine wichtige Rolle spielen, damit eine reibungslose Integration in bestehende IT-Systeme erfolgen und der Serviceanbieter ohne hohe Kosten gewechselt werden kann [11][10]. Eine Automatisierung der Suche von Cloud-Services ist aktuell wegen der fehlenden Standardisierung nur eingeschränkt möglich, so dass in dieser Phase mit hohen Kosten bei der Suche und Auswahl von Cloud-Serviceanbietern zu rechnen ist.

Auf die Anbahnungsphase folgt im Lebenszyklus einer Cloud-Transaktion die Phase der Vereinbarung. Die Phase der Vereinbarung wird üblicherweise bei erfolgreicher Einigung zwischen Cloud-Benutzer und Cloud-Anbieter durch den Abschluss eines Vertrags beendet. Ein Vertrag regelt meist die Nutzung eines

Cloud-Services und schreibt alle Regeln und Pflichten der beteiligten Parteien fest. Diese Verträge bzw. Service-Level-Agreements (SLA) werden von den Cloud-Serviceanbietern in einer standardisierten Form angeboten, so dass der Cloud-Konsument nur die Auswahl zwischen der Annahme oder der Ablehnung des Vertrags hat.

Eine individuelle Aushandlung eines Service-Level-Agreements durch den Konsumenten ist meist nicht möglich. Nur bei Großkunden von Serviceanbietern findet häufig eine individuelle Anpassung des Vertrags statt, in dem beispielsweise die rechtlichen Aspekte detaillierter ausgearbeitet werden. Die standardisierten Verträge des Cloud-Serviceanbieters senken die Transaktionskosten und erhöhen gleichzeitig die Geschwindigkeit, mit der ein Cloud-Service genutzt werden kann. Eine Garantie bestimmter Schutzziele findet sich in keinem der bekannten Service-Level-Agreements von Cloud-Anbietern, da diese häufig Garantien ablehnen, die beispielsweise durch den Einsatz von Softwareprodukten entstehen können, die von Dritten hergestellt wurden, und bei denen sie nur geringen bis keinen Einfluss auf die Zuverlässigkeit der Software haben [29]. In der Phase der Vereinbarung sollte bei der Auswahl eines Cloud-Services auch Kriterien wie die Reputation des Produkts, dessen Benutzerfreundlichkeit, bisherige Erfahrungen oder Wissen über die eingesetzten Technologien einfließen, um einen Cloud-Service hoher Qualität von einem zuverlässigen Anbieter auszuwählen.

Die Erfüllung des Vertrags steht im Zentrum der Ausführungsphase. In dieser Phase werden die Ressourcen bereitgestellt, die Anwendung in Betrieb genommen, die Daten zur Anwendung transportiert, die Berechnungen ausgeführt und die Ergebnisse abgespeichert. Die einzelnen Sicherheitsrisiken wurden bereits in den Bereichen der Infrastruktur und Anwendung und Plattform der Taxonomie diskutiert. Im Rahmen der Phasen der Cloud-Servicenutzung müssen während der Ausführung weitere Systeme zur Überwachung und Messung der Dienstgüte sowie der Sicherheitsfunktionen vorhanden sein, so dass im Idealfall eine Prüfung aller Schutzziele durchgeführt werden und auf diesen Daten eine verbrauchsabhängige Abrechnung der benutzten Ressourcen erfolgen kann. Zwar werden von fast allen Anbietern Systeme zum Logging von Benutzeraktionen betrieben, jedoch muss der Benutzer diesen uneingeschränkt vertrauen, da er keine Möglichkeit hat, diese Daten, z. B. von vertrauenswürdigen Dritten, überprüfen zu lassen.

Nach Abschluss der Ausführung des Cloud-Services durch den Anbieter, findet in der Anpassungsphase eine dynamische Anpassung der Cloud-Ressourcen an die Dienstausführung statt, um die vereinbarte Dienstgüte einzuhalten. Es werden zum einen die Ergebnisse der Ausführungsphase überprüft und zum anderen Anpassungen für eine zukünftige Transaktion, abhängig von aktuellen und vergangenen Transaktionen, z. B. der Ressourcenmenge, vorgenommen werden. Weichen zur Laufzeit gemessene Werte von der vereinbarten Performanz ab, so lassen sich dynamisch Gegenmaßnahmen zur Bereitstellung weiterer Rechenleistung oder Bandbreite definieren, die automatisch eingeleitet werden. Dies kann eine Skalierung der Ressourcen nach oben, aber auch eine Skalierung der

Ressourcen nach unten bedeuten.

Die Durchsetzungsphase stellt die letzte Phase der Servicenutzung dar. In dieser Phase werden Abweichungen von den im SLA vereinbarten Performanz- und Sicherheitsmetriken analysiert und durchgesetzt, d. h. Abweichungen von den vereinbarten Metriken werden beispielsweise durch Strafzahlungen kompensiert oder die eine Bewertung über den Serviceanbieter abgegeben, die in seine Reputation mit einfließt. Auslöser aus Sicherheitssicht können der Ausfall bestimmter Sicherheitskontrollen sein, die bestimmte Anforderungen des Cloud-Konsumenten verletzen, oder zuviele offene Sicherheitslücken in den Services des Cloud-Anbieters, die außerhalb des vereinbarten Zeitrahmens geschlossen werden.

Checkliste der Phasen der Servicenutzung

- Wie werden die Anforderungen an die Sicherheit durch den Cloud-Anbieter umgesetzt?
- Können bei Abbruch der Vertragsverhandlungen durch den Cloud-Konsumenten oder Cloud-Anbieter die bereits übermittelten Anwendungen und Daten wieder zurückgeholt werden?
- Sind alle Sicherheitsfunktionen des Anbieters dokumentiert? Sind die Informationen für eine Bewertung ausreichend?
- Welche Garantien werden in den standardisierten Service-Level-Agreements des Anbieters gegeben? Welche Ausnahmen gibt es?
- Bietet der Anbieter die Vereinbarung individueller Service-Level-Agreements an?
- Wo und durch welche Systemkomponenten wird die Ausführung eines Cloud-Services überwacht? Ist es möglich Services Dritter zu integrieren?
- Werden dynamische Anpassungen der Ressourcen zur Laufzeit durch den Cloud-Anbieter vorgenommen oder nur zwischen der Ausführung von zwei Diensten?
- Welche Vertragsstrafen sind in den standardisierten SLAs enthalten? Wann und in welchem Umfang werden diese fällig?
- Welche Möglichkeiten zur Durchsetzung des SLAs bietet der Cloud-Anbieter an? Muss der Cloud-Konsument eine Verletzung des Vertrags selbst melden?

5.4.2 Prüfung

Der Bereich der Prüfung bezieht sich auf die Frage, wie sicherheitsrelevante Ereignisse in Cloud-Computing-Systemen aufgezeichnet, überwacht und überprüft werden können. Diesem Bereich kommt in Cloud-Computing-Systemen eine besondere Bedeutung zu, da für alle Schutzziele eine entsprechende Prüfungsmöglichkeit existieren sollte. Das Ziel der Prüfung ist es, eine Beweissicherung auf Grundlage der aufgezeichneten Daten zu ermöglichen. Hierfür muss die Beweissicherung in alle relevanten Komponenten eines Cloud-Computing-Systems eingebaut werden, um so eine möglichst lückenlose Überprüfung zu ermöglichen.

Wie für die meisten Sicherheitsaspekte der Taxonomie, gibt es auch für den Bereich Prüfung noch keine standardisierten Ansätze. Es kann jedoch ein generischer Ansatz auf Grundlage der Prüfung vertraglich vereinbarter Prüfpfade angewandt werden. Eine Prüfung der Einhaltung von Schutzzielen kann bestehende Prozesse und Verfahren umfassen, die anhand vertraglich vereinbarter Dokumentationspflichten, die beispielsweise einen Cloud-Serviceanbieter zu regelmäßigen Sicherheitsprüfungen verpflichtet, überprüft werden. Dies kann sowohl manuell oder mit IT-Unterstützung erfolgen.

Wegen der hohen Komplexität eines Cloud-Computing-Systems ist eine solche Prüfung jedoch mit hohen Kosten verbunden, so dass sie von Unternehmen wohl nur selten und nur bei Verdachtsfällen zum Einsatz kommen wird. Eine Prüfung der Sicherheit z. B. mit Portscanning ist jedoch mit Schwierigkeiten hinsichtlich ihrer Durchführbarkeit verbunden, da die Anbieter von Cloud-Services meist Abwehrmechanismen gegen solche meist böswilligen Angriffe einsetzen. Aus diesem Grund sollten bei einem Vertragsabschluss die Maßnahmen zur Sicherheitsprüfung detailliert festgehalten werden.

Checkliste der Prüfung

- Welche Prüfungsmöglichkeiten bietet der Anbieter an?
- Werden die Messdaten dem Cloud-Konsumenten zur Verfügung gestellt?
- Werden regelmäßige Sicherheitsprüfungen durch den Anbieter selbst und externe Dienstleister durchgeführt? Sind diese vertraglich festgehalten?
- Nach welchen Standards werden die Prüfungen durchgeführt?
- Besteht die Möglichkeit durch den Cloud-Konsumenten eigene Sicherheitsprüfungen durchzuführen?

5.4.3 Identitäts- und Rechteverwaltung

Einen sehr wichtigen Sicherheitsaspekt des Verwaltungsbereichs der Taxonomie stellt die Identitäts- und Rechteverwaltung dar, die eine zentrale Rolle bei der Integration von Cloud-Services in bestehende IT-Landschaften übernimmt. Dabei stehen zwei Merkmale der Identitäts- und Rechteverwaltungssysteme im Fokus: erstens die Möglichkeit der Anpassung bestehender Systeme auf Cloud-Computing-Systeme zur Erreichung der Sicherheitsziele Authentizität, Integrität und Vertraulichkeit und zweitens die Fähigkeit zum Schutz der Privatsphäre von Cloud-Nutzern.

Die Anpassung bestehender Systeme zur Zugangsverwaltung muss unter Einbezug der Charakteristika von Cloud-Systemen erfolgen. Durch den Bezug von Cloud-Services über ein öffentliches Netzwerk wird der Authentifizierungsvorgang Bedrohungen des Internets ausgesetzt, die bei der Verifikation eines Benutzers berücksichtigt werden müssen und im obigen Abschnitt zur Anwendungssicherheit kurz vorgestellt wurden. Zusätzlich müssen nicht nur Mitarbeiter eines Unternehmens, sondern auch dessen Kunden und Geschäftspartner bei Bedarf gegenüber einem Cloud-Service authentifiziert werden. Verwenden alle Akteure unterschiedliche Technologien zur Identitätsverwaltung, bietet sich der Einsatz föderierter Identitäten an, die Authentifizierung zwischen unterschiedlichen Technologieplattformen ermöglichen und dadurch eine wichtige Rolle bei der Authentifizierung von Benutzern in Cloud-Computing-Systemen übernehmen [31]. Bei einer föderierten Identitätsverwaltung wird die Identität des Benutzers bzw. werden die Attribute der Identität verteilt auf Rechnern im Internet gespeichert. Der Vorteil einer föderierten Identität ist, dass sich der Benutzer nur einmal authentifizieren muss und verschiedene Cloud-Services auch unterschiedlicher Anbieter nutzen kann. Zur Umsetzung eines föderierten Identitätsmanagements stehen standardisierte Technologien wie Security Assertion Markup Language (SAML) oder Open-Source-Rahmenwerke wie OpenID zur Verfügung [40] [32].

In einer föderierten Identitätsverwaltung müssen Attribute einer Identität für den Authentifizierungsvorgang ausgetauscht werden. Dabei sollte möglichst die Privatsphäre des Cloud-Benutzers geschützt werden, um Nutzerdaten und weitere vertrauliche Daten einer Identität nicht an den Kommunikationspartner übermitteln zu müssen. Dies kann durch den Einsatz von Pseudonymen verhindert werden, die eine Zuordnung von Servicenutzung zu einem Cloud-Benutzer nur über eine temporäre Identität, ohne Übermittlung von Identitätsattributen, ermöglichen.

Neben den Funktionen der Identitäts- und Zugangsverwaltung, die einen einfachen Einsatz von Cloud-Services ermöglichen, sind auch neue Ansätze im Bereich der Administration dieser Systeme notwendig, um die komplexen Strukturen mit einer Reihe von Identitätsanbietern und einer Vielzahl unterschiedlicher Berechtigungen effizient handhaben zu können. Im Fokus steht in diesem

Zusammenhang die Verwaltung von Benutzerprofilen, die eine Kommunikation zwischen Benutzer und Maschine – ein Endbenutzer nutzt einen Cloud-Service – und zwischen zwei Maschinen – zwei Cloud-Services kommunizieren weitgehend automatisiert – ermöglichen. Dabei kann es vorkommen, dass die Identitätsdaten ebenfalls auf Cloud-Ressourcen gespeichert werden und deren Informationssicherheit gewährleistet werden muss.

Die Rechteverwaltung wird in Cloud-Computing-Systemen häufig durch eine Zugriffskontrollliste durchgeführt. Die Vorteile des Konzepts der Zugriffskontrolllisten liegen in der einfachen Verwaltung der Zugriffsrechte, insbesondere der einfachen und effizienten Realisierung einer Rechterücknahme. Dazu müssen nur die entsprechenden Einträge in der Zugriffskontrollliste aktualisiert werden. Außerdem ist es sehr einfach, für ein spezifisches Objekt wie beispielsweise eine Datei zu bestimmen, welche Subjekte welche Zugriffsrechte an dem Objekt besitzen. Es ist jedoch für einen Benutzer sehr aufwändig, eine Übersicht über seine aktuellen Rechte zu ermitteln. Problematisch an der Rechteverwaltung mithilfe von Zugriffslisten ist weiterhin, dass die Zugriffskontrolle bei langen Listen aufwendig und ineffizient ist. Alternativen zur Rechteverwaltung in Cloud-Computing-Systemen stellen Systeme zur digitalen Rechteverwaltung dar, wie sie häufig bei multimedialen Inhalten zum Einsatz kommen und auch in Cloud-Computing-Systemen eingesetzt werden, um den Zugriff auf die gespeicherten Daten zu verwalten.

Aktuell gibt es im Bereich der Identitäts- und Rechteverwaltung noch kein standardisiertes Vorgehensmodell. Es ist jedoch zwingend notwendig, den Zugangspfad zu Cloud-Services zu überwachen, ohne Einschränkungen hinsichtlich der Skalierbarkeit oder Dynamik des Cloud-Systems machen zu müssen. Ein erster Ansatz kann, wie bisher bereits praktisch eingesetzt, die Verwendung von Sicherheitsproxies sein, die einen zentralen Zugriffspunkt für Cloud-Services darstellen und dadurch eine Überprüfung der Berechtigungen für den Zugriff erleichtert. Nachteil dieses Vorgehens kann eine eingeschränkte öffentliche Erreichbarkeit des Cloud-Services sein.

- Welche Identitäts- und Rechteverwaltungsstandards werden unterstützt?
- Wie sehen die Prozesse zur Rechtevergabe und dem kontrollierten Rechteentzug aus?
- Welche Standards zur Bereitstellung der Identitäten und Benutzerprofile werden unterstützt?
- Ist die Rechtevergabe transparent?
- Existiert eine Programmierschnittstelle für die Bereitstellung und Löschung von Rechten?

5.4.4 Schlüsselverwaltung

Die Schlüsselverwaltung ist ein wichtiger Bestandteil der Sicherheitsimplementierung eines Cloud-Computing-Systems. Dabei muss der vollständige Lebenszyklus der Schlüsselverwaltung mit den Phasen Schlüsselerzeugung, Schlüsselaustausch, Schlüsselspeicherung, Schlüsselverifikation und Schlüsselvernichtung in Cloud-Computing-Systemen abgebildet werden, um Vertrauen zwischen den beteiligten Akteuren in einem Cloud-Computing-System nachprüfbar zu gestalten.

Die grundlegenden Probleme sind dabei die Verwaltung einer großen Anzahl an Schlüsseln für unterschiedliche, kryptografische Verfahren und die Verteilung der Schlüssel an Akteure, die bei der Planung der Schlüsselverwaltung nicht berücksichtigt wurden. Der Aufbau eines Vertrauensverhältnisses durch den Austausch von Schlüsseln zwischen Cloud-Konsument und Cloud-Anbieter wird zusätzlich noch weiter dadurch erschwert, dass durch die Möglichkeit, kurzfristig den Bedarf an Ressourcen in einem Cloud-Computing-System decken zu können, diese dynamisch von unterschiedlichen Anbietern und unterschiedlichen Plattformen bezogen werden können. Die Schlüsselverwaltung muss also mit einer Reihe von Schlüsselspeichern und Schlüsselarten umgehen können.

Akteuren eines Cloud-Computing-Systems, die bei der Planung der Schlüsselverwaltung nicht berücksichtigt wurden, kann beispielsweise über einen Intermediär ein Schlüssel zur Verfügung gestellt werden. Dabei sollten die Rollen der Akteure, die verschlüsseln und die die Schlüssel speichern, strikt getrennt sein, um einen nicht-autorisierten Zugriff auf weitere Schlüssel zu verhindern. Desweiteren ist zu verhindern, dass die Daten nicht in „Geiselhaft“ genommen werden, indem mit einem unbekannten Schlüssel die Daten auf einem Cloud-Computing-System verschlüsselt werden und damit der Zugriff auf die Daten im Klartext nicht mehr möglich ist.

Die Speicherung der Schlüssel muss analog zu besonders schützenswerten Daten in Cloud-Computing-Systemen erfolgen und stets redundant gesichert und wiederherstellbar sein, um einen Verlust eines Schlüssels zu vermeiden. Dies kann im schlimmsten Fall zu einem Szenario führen, bei dem die Daten nicht mehr entschlüsselt und wiederhergestellt werden können. Eine Möglichkeit kann in diesem Zusammenhang die verteilte Speicherung der Schlüssel sein, bei nur ein Teil eines Schlüssels in einem Schlüsselspeicher abgelegt ist und ein weiterer Teil des Schlüssels in einem anderen Schlüsselspeicher. Nur das Zusammenfügen der einzelnen Schlüsselteile ermöglicht den Zugriff auf die Daten.

Checkliste für die Schlüsselverwaltung

- Werden Services seitens eines Cloud-Anbieters für die Speicherung von Schlüsseln und deren Verwaltung bereitgestellt?
- Wie werden die Schlüssel für die Cloud-Services erzeugt, verwaltet und geschützt?

- Liegt die Verantwortung für die Schlüsselverwaltung beim Cloud-Konsumenten oder beim Cloud-Anbieter?
- Gibt es einen Schutz gegen den Verlust eines Schlüssels?
- Wie viele Schlüssel gibt es für einen Benutzer? Einen oder mehrere? Wem gehören die Schlüssel?
- Wo werden die Daten ver- und entschlüsselt?

5.4.5 Interoperabilität und Portabilität

Die beiden letzten Sicherheitsaspekte im Bereich der Verwaltung der Taxonomie sind die Interoperabilität und Portabilität von Daten und Anwendungen in Cloud-Computing-Systemen. Die Interoperabilität von Cloud-Computing-Systemen bezeichnet dabei die Fähigkeit zweier oder mehr unabhängiger Cloud-Computing-Systeme nahtlos zusammen zu arbeiten, ohne dass gesonderte Absprachen zwischen den Systemen notwendig sind. Die Interoperabilität ist dabei ein Kriterium, das die Unterstützung von Standards z. B. auf Schnittstellen oder Protokollebene beschreibt. Die Plattformunabhängigkeit oder Portabilität eines Cloud-Computing-Systems hingegen ist die Eigenschaft eines Cloud-Services, auf verschiedenen Cloud-Computing-Systemen mit unterschiedlichen Dienstprogrammen auf unterschiedlichen Schichten lauffähig zu sein.

Unternehmen sollten bei der Auswahl der Cloud-Services sowohl auf die Interoperabilität als auch die Portabilität achten, um Lock-in-Effekte zu vermeiden und die Kosten bei einem Wechsel des Cloud-Anbieters möglichst gering zu halten. Gründe für einen Wechsel können eine Erhöhung der Mietkosten, die Rückholung der Daten und Anwendungen in das Unternehmen, die Einstellung eines Cloud-Services durch den Anbieter oder die Verringerung der Servicequalität sein.

Drei Szenarien können bei der Interoperabilität und Portabilität unterschieden werden, abhängig davon, ob der Cloud-Service auf Anwendungsschicht, auf Plattformschicht oder auf der Infrastrukturschicht durch den Cloud-Konsumenten angemietet wurde. Im Fall eines Cloud-Services auf der Anwendungsschicht gehört der Cloud-Service dem jeweiligen Anbieter, der die Daten eines Cloud-Konsumenten verarbeitet. Ein Cloud-Konsument muss die Möglichkeit haben, die Daten in eine neue Anwendung zu migrieren. Aus diesem Grund sollte darauf geachtet werden, dass ein Cloud-Konsument immer Zugriff auf seine Daten besitzt und diese Daten in einem Datenformat sind, das vom Cloud-Konsumenten auch weiterverarbeitet bzw. in ein anderes Datenformat transformiert werden kann.

Auf der Plattformschicht kann eine fehlende Abstraktionsschicht zwischen Anwendung und Plattformservices dazu führen, dass signifikante Teile des Quellcodes bei einer Migration umgeschrieben werden müssen. So können beispielsweise fehlende Sicherheitsfunktionen oder kontinuierlich auftretende Sicher-

heitsrisiken der Plattform dazu führen, dass die Plattform gewechselt werden muss. Die Daten sollten in jedem Fall an einem zweiten Ort gesichert werden, da Sicherheitslücken der Plattform diese kompromittieren können.

Anwendungen, die Services auf der Infrastrukturschicht verwenden, werden meist innerhalb einer virtuellen Maschine ausgeführt, die es ermöglicht, von einem System in ein anders kopiert zu werden, wenn es sich um die gleiche Virtualisierungslösung handelt. Erste Standardisierungsvorschläge wie das Open Virtualization Format[5] unterstützen die einfache Migration von virtuellen Maschinen zwischen unterschiedlichen Systemen. Sicherungskopien der virtuellen Maschinen sollten in einem Cloud-unabhängigen Format abgespeichert werden und regelmäßig außerhalb der Cloud gesichert werden.

In allen drei Szenarien sollte ein Cloud-Konsument einen Risikomanagementprozess etablieren, um die Risiken, die bei einer möglichen Migration auftreten können, zu behandeln. Er hat beispielsweise die Möglichkeit über Redundanz die Abhängigkeit von einem Anbieter zu reduzieren oder Cloud-Services verschiedener Anbieter einzusetzen und damit sein Risiko zu diversifizieren. Details hierzu werden im Bereich Compliance näher betrachtet.

Checkliste für Interoperabilität und Redundanz

- Welche Standards werden durch den Cloud-Anbieter unterstützt, so dass Interoperabilität und Protabilität sichergestellt werden können?
- Ist ein Zugriff auf die Daten möglich? In welchem Datenformat werden die Daten gespeichert?
- Können die gespeicherten Daten in ein anderes Format überführt werden?
- Unterstützt die Plattform des Cloud-Anbieters eine Abstraktionsschicht, die die Portierung einer Anwendung unterstützt? Muss der Cloud-Konsument dies bei dem Entwurf der Anwendung berücksichtigen?
- Ist die Plattform eines Anbieters kompatibel mit der eines anderen Anbieters? Welche Standards werden hier unterstützt?
- Welche Migrationsmöglichkeiten bietet der Cloud-Anbieter an?
- Werden Standards und Technologien z. B. bei der Langzeitarchivierung auch in Zukunft unterstützt?
- Werden Sicherungskopien der Daten durch den Anbieter in einem anbieterunabhängigen Format gespeichert?

[5] http://www.vmware.com/appliances/learn/ovf.html

5.5 Compliance

Unter dem Bereich der Compliance werden alle regulatorischen Themen zusammengefasst, die eine Auswirkung auf die Schutzziele haben können. In den folgenden Abschnitten werden kurz der gesetzliche Rahmen in Form von Datenschutzgesetzen, sowie gesetzlichen Vorgaben für Unternehmen bezüglich Datenhaltung und Datenverarbeitung in Cloud-Computing-Systemen vorgestellt. Des Weiteren wird ein Risikomanagementprozess vorgestellt, mit den Cloud-Konsumenten ihre Risiken beim Einsatz von Cloud-Services behandeln können. Ebenfalls werden im Rahmen der Governance wichtige Sicherheitsrichtlinien, Zertifikate und Normen vorgestellt, die ein Cloud-Anbieter haben sollte. Allgemein gilt, dass die Verfahren zur Überwachung der Compliance auf Internet-basierte Dienstleistungen wie Cloud-Services erweitert werden müssen, um Anwendungen, Benutzer und Aktivitäten in Cloud-Computing-Systemen effizient erfassen zu können.

5.5.1 Datenschutz

In einer Cloud können alle Informationen, wie beispielsweise Textverarbeitungsdokumente, Videos, Kundendaten oder Finanzdaten, die bisher lokal oder im Unternehmensnetzwerk gespeichert wurden, abgelegt werden. Dies kann sogar soweit gehen, dass die vollständigen Daten eines Cloud-Benutzers in dem Cloud-Computing-System gespeichert sind. Jedes Mal, wenn ein Cloud-Benutzer Informationen in der Cloud ablegt und mit anderen Akteuren der Cloud teilt, können Fragen hinsichtlich des Schutzes der Privatsphäre auftreten. Die zentrale Frage, die in diesem Zusammenhang beantwortet werden muss, ist: Dürfen die Informationen, die durch die Benutzung eines Cloud-Services mit dem Serviceanbieter geteilt werden, konform zu den aktuell geltenden Datenschutzgesetzen in einem Cloud-Computing-System abgelegt und weiterverarbeitet werden?

Cloud-Services können nach dem Bundesdatenschutzgesetz (BDSG)[6] als Datenverarbeitung im Auftrag gesehen werden, bei der die Verantwortung der Verarbeitung der Daten beim Cloud-Benutzer als Auftraggeber liegt[7]. Voraussetzung ist, dass der Cloud-Serviceanbieter als Auftragnehmer bei Verstößen zur Verantwortung gezogen werden kann. Dies ist innerhalb von Europa durch die EU-Datenschutzrichtlinien gewährleistet [15].

Ziel ist es, Technologien für die Cloud bereitzustellen, die es Unternehmen zum einen ermöglichen, ihre Geschäfte unter Verwendung von Cloud-Services und

[6] http://bundesrecht.juris.de/bdsg_1990/index.html

[7] http://microsite.computerzeitung.de/article.html?art=/articles/2009020/31942144_ha_CZ.html&page=1&ms=/cloud-computing/index.html&pos=4&tpid=ee54f3c7-0de1-40f5-bb23-2cfdf022aee5&pid=ee54f3c7-0de1-40f5-bb23-2cfdf022aee5

Cloud-Ressourcen durchführen zu können und zum anderen die Privatsphäre der Endbenutzer zu schützen. Dazu muss der Cloud-Benutzer dem Cloud-Serviceanbieter die Anforderungen an die Privatsphäre übermitteln und die Einhaltung überprüfen können. Werden beispielsweise Mitarbeiterdaten eines Unternehmens an einen Cloud-Service – wie im aktuellen Fall Siemens an den SaaS-Anbieter SuccessFactors[8] – ausgelagert, so muss das auslagernde Unternehmen in der Rolle als Cloud-Nutzer für eine Einhaltung der Privatsphäre sorgen.

Nach dem deutschen Bundesdatenschutzgesetz spielt der geographische Standort der Datenspeicherung eine wichtige Rolle. Im Bundesdatenschutzgesetz wird unterschieden zwischen EU-Staaten, vertrauenswürdigen Staaten und nichtvertrauenswürdigen Drittländern. In EU-Staaten und vertrauenswürdigen Staaten ist die Speicherung und Verarbeitung auch von personenbezogenen Daten erlaubt, während eine Übertragung und Verarbeitung von Daten in ein nicht vertrauenswürdiges Drittland durch das Bundesdatenschutzgesetz verboten ist. Cloud-Services, die ihre Anwendungen und Ressourcen aus Rechenzentren aus vertrauenswürdigen Staaten beziehen, können also nach Bundesdatenschutzgesetz verwendet werden. Dabei ist zu beachten, dass es abweichende Datenschutzrichtlinien in den einzelnen Staaten geben kann.

Jedoch gibt es auch Ausnahmen für nicht vertrauenswürdige Staaten wie die Vereinigten Staaten von Amerika, Japan oder China, wenn beispielsweise der Betroffene einwilligt oder die Datenverarbeitung zwingend erforderlich ist, um vertraglichen Verpflichtungen nachzukommen.

Diese Ausnahmen kommen beispielsweise bei Cloud-Services von Cloud-Anbietern zur Anwendung, die beispielsweise nur Rechenzentren in den USA betreiben. Unternehmen können sich beispielsweise auf die zwingende Erfordernis der Datenverarbeitung zur Erfüllung vertraglicher Pflichten berufen, um Kundendaten auf den Rechnern von Salesforce zu speichern und zu verarbeiten. Zusätzlich verschärft sich das Problem der entfernten Datenspeicherung, da es aktuell für Cloud-Computing-Systeme noch keine ausreichende Unterstützung technischer Systeme zur kontinuierlichen Überprüfung des Schutzes der Privatsphäre gibt. Cloud-Benutzern bleibt nur die Möglichkeit, die entsprechenden Anforderungen bei der Auswahl eines vertrauenswürdigen Anbieters im Rahmen der Anbahnungsphase zu berücksichtigen, die Anforderungen an die Privatsphäre bei der Vertragsgestaltung festzuschreiben und im Rahmen der IT-Governance zu überprüfen. Im Fall Salesforce werden die Daten auf Basis der im Safe-Harbor-Abkommen festgelegten Kriterien zum Schutz der Privatsphäre behandelt, was eine lokal gültige Datenschutzrichtlinie darstellt [19].

Das deutsche und europäische Datenschutzrecht geht im Prinzip davon aus, dass man jederzeit feststellen kann, wo sich die Daten physisch auf den Rechnern in einem Rechenzentrum befinden. Dies ist bei Cloud-Computing-Systemen,

[8] http://www.successfactors.de/press-releases/detail/?releaseid=36

je nach eingesetzten Verfahren, teilweise nicht mehr gewährleistet. Wird beispielsweise ein Speicherdienst ausgewählt, der die Daten nach dem Map-Reduce-Verfahren speichert, so sind die aufgespaltenen Daten auf verschiedene Server verteilt. Als Einzelteile kann es sein, dass diese keine persönlichen Daten darstellen, wohl aber im zusammengesetzten Zustand. Dies macht eine Überwachung schwierig, wenn nicht gar unmöglich.

Checkliste des Datenschutzes

- Wie sehen die Datenschutzbestimmungen des Cloud-Anbieters aus? Kann eine Kopie der Richtlinien als Dokument zur Verfügung gestellt werden?
- An welche Orte und Komponenten im Cloud-Computing-System können die Daten transferiert werden?
- Gibt es Zweitverwertungrechte an den Daten durch den Cloud-Anbieter?
- Werden Statistiken über die Daten zum Zweck der Systemoptimierung oder der Marktforschung durch den Cloud-Anbieter durchgeführt?
- Wer kann auf die Daten im unverschlüsselten Zustand z. B. während der Verarbeitung zugreifen?
- Wer hat Zugriff zu den Hosts des Cloud-Computing-Systems?

5.5.2 Gesetzliche Rahmenbedingungen

Neben den Datenschutzgesetzen, die auf die Schutzziele Schutz der Privatsphäre und Vertraulichkeit abzielen, können weitere gesetzliche Rahmenbedingungen den Einsatz von Cloud-Computing-Systemen einschränken. Alle Daten, die durch eigene Gesetze in ihrer Verwendung eingeschränkt sind, wie beispielsweise Gesundheitsdaten, Daten bestimmter Berufsgruppen wie Anwälten oder Priestern, Steuerdaten und weitere Daten im Umfeld von Unternehmen oder staatlichen Organisationen, die die Grenzen eines geographischen Ortes nicht verlassen oder von Dritten eingesehen werden dürfen, können auf Cloud-Computing-Systemen unter Umständen nicht gespeichert oder verarbeitet werden [13].

Vor allem, wenn der Anbieter eines Cloud-Services Rechte besitzt, die Daten zu lesen, offenzulegen oder zu transferieren, kann das Sicherheitsziel der Vertraulichkeit sehr schnell verletzt sein und gegen geltendes Recht verstoßen. In diesem Zusammenhang kann die Gesetzeslage in den einzelnen Staaten sehr stark voneinander abweichen, so dass hier die jeweils gültigen Gesetze zu untersuchen sind. Insgesamt stecken die rechtlichen Ansätze noch in den Kinderschuhen und bedürfen noch weiterer Untersuchung.

Ein weiterer Aspekt, der in diesen Bereich der Taxonomie des sicheren Cloud-Computings fällt, ist das Problem des Zugangs und der Verarbeitung der Daten, wenn der Cloud-Serviceprovider seinen Service einstellt oder der Serviceanbieter von einem anderen Anbieter übernommen wird und die Geschäfte des ursprünglichen Serviceanbieters fortführt. Ein solches Szenario sollte auch in das oben diskutierte Risikomanagement miteinbezogen werden, da es in der Zukunft eine Konsolidierung der Cloud-Serviceangebote geben wird. Es könnte beispielsweise ein Treuhändermodell angewandt werden, in dem die Daten und Rechner an einen Treuhänder übergeben werden, der dem Kunden die Möglichkeit bietet, die Daten weiterhin abrufen zu können und geordnet in die Systeme des neuen Besitzers zu überführen.

Checkliste für die gesetzlichen Rahmenbedingungen

- Gibt es Angebote eines Cloud-Anbieters, die auf spezielle gesetzliche Anforderungen zugeschnitten sind?
- Ist der Cloud-Anbieter berechtigt, bestimmte schützenswerte Daten z. B. aus dem Gesundheitsbereich zu verwalten? Besitzt er die notwendigen Zertifikate?
- Kann der geografische Ort so eingeschränkt werden, dass bestimmte gesetzliche Auflagen erfüllt sind?
- Wie sehen die Haftungsfragen bei Verletzung der gesetzlichen Bestimmungen aus? Bei welchen Ereignissen haftet der Cloud-Anbieter?

5.5.3 Risikomanagement

Die Benutzer von Cloud-Services müssen einen Prozess zum Management ihrer Cloud-Anbieter einsetzen, der die Risiken der genutzten Cloud-Services behandeln kann. Durch den Einsatz von Cloud-Services lagern Cloud-Konsumenten nicht nur einen Geschäftsprozess oder eine Anwendung aus, sondern auch das Risiko, das mit dem Betrieb dieser Prozesse oder Anwendungen einhergeht. Cloud-Konsumenten müssen beim Einsatz von Cloud-Services mit Ausfällen und Sicherheitsrisiken rechnen, wie Vorfälle in der Vergangenheit gezeigt haben [9]. Die Identifikation der Risiken und die Festlegung einer Risikomanagementstrategie sind aus diesem Grund wichtige Bestandteile bei der Nutzung von Cloud-Services.

Das operationelle Risikomanagement beschäftigt sich mit allen Risiken, die bei dem laufenden Betrieb von Cloud-Computing-Systemen bzw. deren Bezug auftreten können. Es umfasst die Gebiete der traditionellen Sicherheit, der Verfahren zur Fortführung des Geschäftsbetriebs und Mechanismen zur Wiederherstellung nach einem katastrophalen Fehler. Mit dem Betrieb von Cloud-Services sind Risiken verbunden, die beispielsweise Auswirkungen auf die Schutzziele Vertraulichkeit, Integrität oder Verfügbarkeit haben können. Das operationelle

Risikomanagement umfasst alle Verfahren, die dazu beitragen, die Risiken aus Sicht des Cloud-Konsumenten zu behandeln.

Dabei können Cloud-Konsumenten beispielsweise auf eigene Erfahrungswerte, Vorgaben durch Richtlinien oder auf externe Services zurückgreifen, die sie bei ihrer Entscheidung unterstützen. Das Risiko sollte aus dem vereinbarten Service-Level-Agreement ableitbar sein und durch entsprechende Systeme bei der Behandlung unterstützt werden. Einem Cloud-Benutzer sollte bewusst sein, dass er bei der Benutzung eines Cloud-Services immer ein Risiko eingeht, da ein Serviceanbieter wegen der Komplexität von Cloud-Computing-Systemen keine Garantie einer fehlerfreien Erfüllung des Service-Level-Agreements abgeben kann.

Für die Beschreibung eines systematischen Umgangs mit Cloud-Risiken im Rahmen des operationellen Risikomanagements wird im Folgenden ein Risikomanagementzyklus eingeführt und hinsichtlich der Anwendung auf Cloud-Computing-Systeme untersucht. Der Risikomanagementzyklus baut auf dem Risikomanagement-Standard der Federation of European Risk Management Associations (FERMA) auf[9] und wird in Abbildung 5.5 gezeigt:

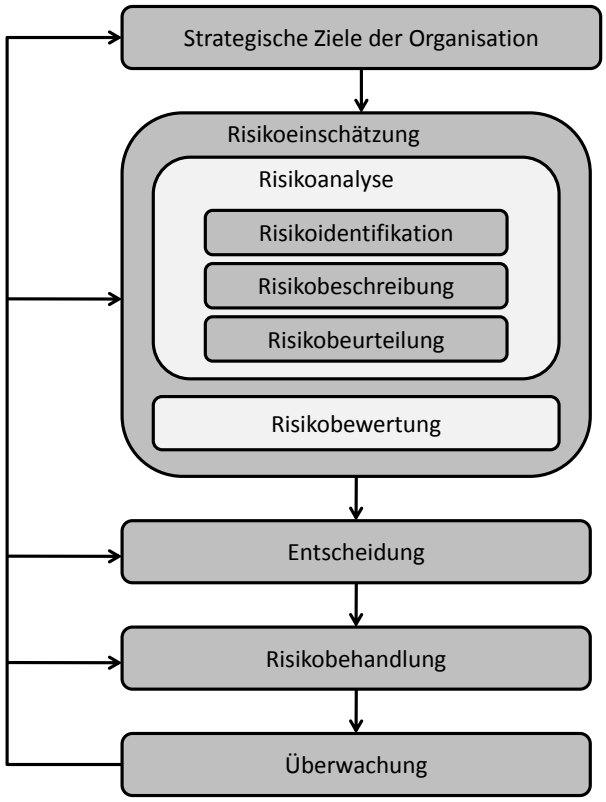

Abbildung 5.5: Risikomanagementzyklus für die Nutzung von Cloud-Services

- Strategische Ziele der Organisation: Die Ziele der Cloud-Service-Nutzung sollten sich aus der Strategie der Organisation ableiten. Sowohl ein Cloud-Konsument als auch ein Cloud-Anbieter können zur Erfüllung der Ziele

[9] Die deutsche Beschreibung des Risikomanagementstandards findet sich unter folgender Webadresse: `http://www.ferma.eu/tabid/195/Default.aspx`

der Organisation entscheiden, ob sie eine Kooperation eingehen oder ablehnen. Dabei sollten dem Nutzen, der sich durch den Einsatz von Cloud-Services ergibt, die damit verbundenen möglichen Risiken gegenübergestellt werden.

- Risikoeinschätzung: Die Risikoeinschätzung umfasst die Risikoanalyse und die Risikobewertung. Am Ende der Risikoeinschätzung steht eine Entscheidung über eine Akzeptanz des Risikos oder die Anwendung eines Verfahrens zur Behandlung des Risikos.
- Risikoanalyse: Die Identifikation eines Risikos stellt den Ausgangspunkt der Risikobetrachtung dar. In diesem Schritt werden die Risiken durch Unsicherheit über die tatsächliche Dienstgüte und Sicherheitsbedrohungen identifiziert.
- Risikobewertung: Nach Abschluss des Risikoanalyseschritts werden die Risiken hinsichtlich der ökonomischen Auswirkungen untersucht. Die Grundlage hierfür bilden quantitative Kennzahlen, die sowohl die Varianz als Streuungsmaß der zu untersuchenden Größen als auch das Ausfallrisiko als Maß des Verlustes bei Nichterfüllung eines Service-Level-Agreements mit einbeziehen. Das Ausfallrisiko sollte dabei die Tatsache berücksichtigen, dass die Cloud-Benutzer eher risikoavers handeln. Dadurch kommt dem Ausfallrisiko gegenüber der Varianz eine größere Bedeutung zu. Die Risikobewertung erfolgt durch den Cloud-Konsumenten. Dieser trifft abhängig von den Risikokennzahlen eine Entscheidung über die Behandlung der Risiken. Dabei wird die Annahme getroffen, dass die Kennzahlen wahrheitsgemäß vom Anbieter übermittelt werden.
- Risikobehandlung: Eine Risikobehandlung betrachtet den Prozess zur Auswahl und Durchführung von Maßnahmen, die zu einer Risikoänderung führen. Zu den 4 wichtigsten Verfahren zur Risikobehandlung gehören Risikoakzeptanz, Risikotransfer, Risikovermeidung, und Risikoreduktion.

  Die Strategie der Risikoakzeptanz bei dem Bezug von Cloud-Services würde bedeuten, dass alle Risiken vom Cloud-Konsumenten getragen und keine weiteren Anstrengungen unternommen werden, die bestehenden Risiken einer Vertragsbeziehung zwischen Cloud-Benutzer und Cloud-Anbieter in irgendeiner Art und Weise zu verändern. Der Cloud-Benutzer trifft in diesem Fall meist unternehmensintern Vorkehrungen zur Behandlung der Risiken, indem er beispielsweise Ressourcen vorhält, die beim Ausfall eines Cloud-Anbieters die Services temporär erbringen. Die Strategie der Risikoakzeptanz kann im Zusammenhang von Testsystemen und Proof-of-Concept-Prototypen angewandt werden, für die bestehende (Sicherheits-)Risiken meist eine untergeordnete Rolle spielen und diese Risiken einen eher geringen Schaden für den Cloud-Benutzer erwarten lassen.

  Eine Anwendung der Strategie Risikovermeidung würde einen Einsatz von Cloud-Services für bestimmte Daten und Prozesse ausschließen, da

alternative Konzepte wie Managed Services oder interne Serviceerbringung weniger Risiken aufweisen. Vor allem bei wichtigen, vertraulichen Unternehmensdaten bietet sich die Strategie der Risikovermeidung an.

Mit der Risikobehandlungsstrategie Risikoreduktion würde ein Cloud-Benutzer Anstrengungen unternehmen, um Sicherheitsrisiken beispielsweise durch zusätzlichen Einsatz von Sicherheitsverfahren zu verringern oder bestehende Verfahren durch Verfahren mit einem höheren Schutzniveau ersetzen. Das Ziel der Risikoreduktion ist es, die Risiken der Cloud-Services soweit zu verringern, dass der Cloud-Benutzer diese akzeptieren und gleichzeitig noch einen Nutzen aus deren Verwendung ziehen kann. Die Anwendung und der Einsatz von Verschlüsselungsverfahren, Zugangsverwaltungssystemen, Überwachungswerkzeugen oder vertrauenswürdiger Systemkomponenten würden in den Bereich der Risikoreduktion fallen und damit wohl die am häufigsten angewandte Strategie im Rahmen der Nutzung von Cloud-Services darstellen.

Als letzte Strategie der Risikobehandlung wird der Risikotransfer untersucht. Diese Strategie zielt darauf ab, dass der Cloud-Benutzer ein bestimmtes (Sicherheits-)Risiko durch das Bezahlen einer Prämie auf den Cloud-Serviceanbieter oder eine dritte Instanz, wie beispielsweise eine Versicherung, übertragen kann. Die Strategie des Risikotransfers ist im Zusammenhang mit Cloud-Computing-Systemen bisher noch sehr wenig diskutiert worden. Sie hat jedoch das Potential, vor allem auf Ebene der Infrastrukturservices eingesetzt zu werden. Ein Risikotransfer kann in diesem Zusammenhang als eine Alternative zu der häufig eingesetzten Methode der Redundanz zur Verringerung des Risikos gesehen zu werden und dazu beitragen, Kosten bei der Cloud-Nutzung zu sparen.

Ein Beispiel für die Anwendung der Risikobehandlungsstrategie Risikotransfer stellt das Produkt "Reserved Instances" des Amazon EC2 Cloud-Services dar. Ist eine aktuell im Betrieb befindliche Instanz nicht mehr verfügbar, kann durch die Bezahlung einer Prämie eine weitere Instanz, die Reserved Instance, vorreserviert werden, die den Service der ausgefallenen Instanz übernimmt. Der Cloud-Benutzer kann in diesem Fall das Risiko eines Ausfalls durch Bezahlung einer Prämie verhindern, indem er Ressourcen vorreserviert, die ihm bei Eintritt eines Schadens zur Verfügung stehen. Die Kompensation seines Schadens erfolgt in obigem Beispiel durch nicht-monetäre Kompensation, wodurch sich der Risikotransfer in Cloud-Computing-Szenarien von der in der Finanzwirtschaft üblichen monetären Kompensation unterscheidet. Analog zu dem Beispiel zur Einhaltung des Sicherheitsziels Verfügbarkeit lassen sich weitere Szenarien definieren, die den Einsatz der Strategie des Risikotransfers als sinnvoll erscheinen lassen.

- Überwachung: Eng mit der Risikobehandlung verknüpft ist die Überwachung der vertraglich vereinbarten Dienstgüte. Sie bildet die Grundlage

einer Prüfung der erbrachten Leistungen des Cloud-Anbieters. Die Dienstgüte bzw. der Service-Level sollte neben zeit-, mengen-, und nutzenbasierten Werten auch Sicherheitsmetriken, sofern messbar, überwachen. In den zu Cloud-Computing-Systemen verwandten Grid-Systemen sind einige leistungsfähige Systeme zur Überwachung bereits im Einsatz, während aktuelle Überwachungssysteme für Cloud-Services bisher nur sehr wenige Werte messen.

Wichtig in Cloud-Computing-Systemen ist auch die Zuverlässigkeit der Überwachungssysteme, da die Rechenzentren der Cloud-Anbieter eine große Anzahl an Rechenknoten umfassen und dadurch auch mit einer erhöhten Anzahl an Rechnerausfällen sowie weiterer Fehlerarten zu rechnen ist. Ziel ist es, die Überwachungssysteme robust gegen Ausfälle oder Veränderungen des Cloud-Computing-Systems zu machen. Aus diesem Grund kommen in Cloud-Computing-Systeme keine zentralen Monitoring-Systeme zum Einsatz, da diese an ihre Leistungsgrenzen stoßen würden. Aktuelle Implementierungen der Überwachungssysteme verfolgen einen verteilten Ansatz, indem sie unterschiedliche Hierarchieebenen definieren, die eine Aggregation der Überwachungsdaten zulassen.

Der Risikomanagementzyklus für Cloud-Computing-Systeme sollte begleitend zu der Auswahl eines Cloud-Services angewandt werden, um frühzeitig mögliche Gefahren erkennen und eine Risikobehandlungsstrategie umsetzen zu können, die beim Erreichen der geforderten Schutzziele unterstützt. Ausgehend von den individuellen Schutzzielen eines Cloud-Benutzers müssen Anpassungen des Risikomanagementzyklus vorgenommen werden, um den Prozess vollständig zu unterstützen. Dabei sollte darauf geachtet werden, dass eine spätere Überwachung der ausgewählten Risikomanagementstrategie durch IT-Systeme oder manuelle Prüfungen gegeben ist, die im nächsten Abschnitt näher erläutert werden.

Checkliste des Risikomanagements

- Was sind die Risikoindikatoren des Cloud-Anbieters? Welche Ziele verfolgt der Anbieter?
- Welche Auswirkungen können die bestehenden Risiken auf das Geschäft des Cloud-Konsumenten haben? Welche Restrisiken bestehen?
- Wie lassen sich die bestehenden Risiken behandeln? Gibt es Services des Cloud-Anbieters, die z. B. eine Reduzierung des Risikos unterstützen?
- Wie sieht der Risikomanagementprozess des Cloud-Anbieters aus? Wird dieser durch eine dritte Partei überprüft? Sind die Dokumente für den Cloud-Konsumenten einsehbar?
- Kann dieser Prozess aus Sicht des Cloud-Konsumenten überprüft werden?

5.5.4 Governance

Die Governance für Cloud-Computing-Systeme definiert einen Ansatz zur Informationssicherheit, indem auf Prozessebene Steuerungs- und Regelungssysteme etabliert werden. Dazu gehört die Definition der Verantwortlichkeiten für Strukturen und Prozesse, deren Compliance bezüglich vorher definierter Metriken, die Festlegung von Informationssicherheitszielen, sowie dazugehörige Richtlinien und Kriterien zur Messung der Effektivität der Informationssicherheitsprozesse.

Die Herausforderung, die die Governance für Cloud-Konsumenten mit sich bringt, besteht darin, einen Kompromiss zu finden, zwischen dem Aufwand, die Prozesse zu erstellen, die Daten zu erheben, die Prozesse durchzusetzen und den Kosten, die hierfür entstehen. Aus funktionaler Sicht besteht die Herausforderung der Governance, einen gesamtheitlichen Rahmen zur Informationssicherheit über die Bezugs- und Nutzungsmodelle der Cloud-Computing-Systeme zu definieren. Dabei sollte zum einen eine Kollaboration auf Ebene der Informationssicherheit mit einem Cloud-Anbieter berücksichtigt werden und zum anderen die Verantwortlichkeiten für die Implementierung und Verwaltung von Sicherheitsprozessen und die dazugehörigen Kontrollen zwischen Cloud-Benutzer und Cloud-Anbieter festgelegt werden.

Die Richtlinien zur Informationssicherheit können auf allgemein akzeptierten Standard basieren. Dazu gehören beispielsweise das IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Veröffentlichungen der European Network and Information Security Agency (ENISA) oder verschiedene Sicherheitsrichtlinien des amerikanischen National Institute of Standards and Technology (NIST). Aufbauend darauf werden verschiedene Zertifizierungen und Normen angeboten, die Regeln zum Umgang mit Daten, Administratorrechten, gesetzlichen Bestimmungen und weiteren IT-Sicherheitsprozessen festlegen. Diese Zertifikate werden meist durch externe Organisationen erteilt und durch eine regelmäßig wiederholte Überprüfung sichergestellt.

Beispiele hierfür sind das Statement on Auditing Standards (SAS) Nummer 70 Typ II Zertifikat und das ISO/IEC 27001:2005 Zertifikat. Durch einen externen Prüfer werden im SAS 70-Zertifikat die Überwachungsaktivitäten und Objekte einer Serviceorganisation, die auch die Überwachungsaktivitäten bezüglich der eingesetzten Informationstechnologien miteinbezieht, dokumentiert und bestätigt. Cloud-Serviceanbieter als eine Ausprägung einer Serviceorganisation können mit dem SAS 70-Zertifikat potentiellen Cloud-Konsumenten signalisieren, dass sie angemessene Überwachungssysteme für ihre IT-bezogenen Technologien und Prozesse installiert haben.

ISO/IEC 27001 spezifiziert Anforderungen für die Einrichtung, Implementierung, Überwachung, Pflege und Verbesserung eines Systems zum Verwalten der Sicherheitsrisiken eines Unternehmens. Es ordnet keine bestimmten Sicherheitsmechanismen an, sondern beschränkt sich nur auf eine Managementebene. Ein

ISO/IEC 27001-System umfasst verschiedene Plan-Do-Check-Act-Zyklen, die dazu führen, dass die Sicherheitsmechanismen einem kontinuierlichen Prozess der Begutachtung und Anpassung unterworfen sind und Schritt halten mit den Veränderungen der Bedrohungen und Schwachstellen der IT-Systeme sowie dem Einfluss der Bedrohungen auf den IT-Betrieb. Mit Bezug auf Cloud-Computing-Systeme sollten die Managementzyklen auf die Sicherheitsbedrohungen durch den Einsatz von Cloud-Computing-Systemen angepasst werden und die in der Taxonomie beschriebenen Sicherheitsfelder berücksichtigen werden.

Checkliste der Governance

- Wer haftet bei Verlust oder Missbrauch der Daten?
- Wer besitzt welchen Teil der Daten und Anwendungen?
- Wie sehen die Verantwortlichkeiten im Bereich Netzzugriffsverwaltung, Berichtswesen, Änderungsverwaltung, Entwicklung und Wartung aus?
- Welche Kontrollen sind auf der Anwendungs-, Plattform- und Infrastrukturschicht vorhanden?
- Welche Zertifikate sind beim Cloud-Anbieter vorhanden? Was bescheinigen Sie aus Sicherheitssicht?
- Werden die Prüfungen der Zertifikate nur intern oder auch extern durchgeführt?
- Werden Kopien der durchgeführten Zertifizierungen ausgehändigt?
- Wie häufig werden Zertifizierungen durchgeführt?
- Wie sehen die Verantwortlichkeiten bei einem Sicherheitsvorfall aus? Wer ist verantwortlich für welche Aktion?
- Welche Prozesse wendet der Cloud-Anbieter bei seinen Lieferanten an? Ist Sicherheit ein Kriterium bei der Auswahl der Lieferanten?
- Welche Sicherheitskontrollen werden bei dem Einsatz von Software Dritter angewandt?
- Was passiert, wenn die Services eines Cloud-Anbieters nicht mehr verfügbar durch z. B. Geschäftsaufgabe sind? Hängt der Cloud-Anbieter von Auswirkungen externer Services ab, die einen Einfluss auf den Cloud-Konsumenten haben können?
- Sind die Prozesse des Anbieters konsistent und vollständig?

5.6 Zusammenfassung

Die Taxonomie der Sicherheitsaspekte von Cloud-Computing-Systemen definiert aus Sicht eines Cloud-Konsumenten einen umfassenden Rahmen für die Bewertung der Sicherheitsrisiken beim Einsatz von Cloud-Services. Sie gliedert sich in die vier Bereiche Infrastruktur, Anwendung und Plattform, Verwaltung und Compliance. Für jeden dieser Bereiche wurden wichtige Sicherheitsaspekte definiert, die Auswirkungen auf die Sicherheit von Cloud-Services haben können.

Der Bereich Infrastruktur konzentriert sich auf die Sicherheit des Rechenzentrumbetriebs und die Sicherheit der Cloud-Services, die auf Infrastrukturschicht (z. B. Rechenleistung) angeboten werden. Im Bereich Anwendung und Plattform steht die Sicherheit der Anwendungs- und Plattformschicht im Vordergrund, sowie Services, die Sicherheitsfunktionen für Cloud-Computing-Systeme anbieten. Diese werden üblicherweise von Dritten bereitgestellt. Verwaltungsaufgaben, die essentiell für die sichere Nutzung von Cloud-Services sind, werden im Bereich Verwaltung betrachtet. Der letzte Bereich der Taxonomie ist der Bereich Compliance, der wichtige Sicherheitsaspekte aus Prozesssicht präsentiert.

Durch die Abhängigkeiten der Bereiche ist es wichtig, eine gesamtheitliche Betrachtung der Sicherheitsrisiken durchzuführen. Aus diesem Grund wurden für jeden Sicherheitsaspekt der Taxonomie Checklisten mit Fragen erarbeitet, die ein Cloud-Konsument einem Anbieter eines Cloud-Services stellen sollte. Die Anwendung der Checklisten wird im folgenden Kapitel exemplarisch am Beispiels des Amazon EC2 Cloud-Services durchgeführt und die Ergebnisse vorgestellt.

6 Cloud-Services und deren Sicherheitsfunktionen

Es existiert eine Vielzahl an Cloud-Services, die sich in verschiedene Servicegruppen eingliedern lassen, wie Infrastruktur-, Plattform-, Anwendungs-, Verwaltungsservices und Sicherheit als Service. Täglich ändert sich das Angebot an Cloud-Computing-Anbietern und -Services, da neue Anbieter und Services hinzukommen bzw. wegfallen. Zunächst wird eine Auswahl von Cloud-Services der unterschiedlichen Servicegruppen und deren Kosten[1] gegeben und in Abschnitt 6.2 werden Anbieter bzgl. ihrer Sicherheitsfunktionen untersucht. Hierbei wird auf die Architektur, Infrastruktur, Verwaltung und Compliance eingegangen. In Abschnitt 6.3 wird die Taxonomie auf den Cloud-Anbieter Amazon angewandt und Abschnitt 6.4 zieht abschließend ein Fazit. Als Informationsquellen werden die Webseiten der Cloud-Anbieter und ihre Whitepaper verwendet.

6.1 Marktübersicht wichtiger Anbieter

Die Angebote der Cloud-Anbieter sind sehr unterschiedlich. So unterscheiden sich die Angebote sowohl in ihrer Funktionalität als auch bei der verwendeten Hardware und dem verwendeten Bezahlmodell. Die Hardware der unterschiedlichen Anbieter weichen beispielsweise bezüglich der Größe der CPU und des RAMs ab. Die Bezahlmodelle der Cloud-Anbieter unterscheiden sich ebenfalls. So bieten Anbieter z. B. ihre Services im pay-as-you-go-Modell an, verlangen eine einmalige Gebühr und zusätzlich ein Nutzungsentgelt, welches pro Nutzungsdauer berechnet wird, oder verlangen einen Festpreis für den Service.

Im Folgenden wird eine Auswahl von Cloud-Services aus den Bereichen Infrastruktur-, Plattform-, Anwendungs-, Verwaltungsservices und Sicherheit als Service vorgestellt. Für diese Auswahl werden Cloud-Anbieter betrachtet, die bereits lange auf dem Markt sind und/oder einen großen Kundenstamm besitzen.

6.1.1 Infrastrukturservices

Zu den Infrastrukturservices gehört z. B. die Bereitstellung von Rechenkapazität, Datenspeicher und auch Datenbanken. In diesem Abschnitt werden die

[1] Stand: Juli 2009

fünf Infrastruktur-Anbieter Amazon[2], Microsoft[3], GoGrid[4], FlexiScale[5] und Rackspace[6] für die Bereitstellung der Rechenkapazität und des Datenspeichers betrachtet. Für die Bereitstellung von Datenbanken werden die Preise der Anbieter Amazon und Microsoft betrachtet. Die Preise für den Datentransfer zu den Datenzentren (eingehend) bzw. aus den Datenzentren heraus (ausgehend) werden getrennt betrachtet, da einige Provider hierfür unterschiedliche Preise verlangen.

Die Infrastrukturservices werden im Folgenden nach der Anmietung der Rechenkapazität, des Datenspeichers und der Datenbank unterteilt.

Rechenkapazität

Amazon hat als einziger aufgeführter Anbieter unterschiedliche Preise für Europa und die Vereinigten Staaten und zusätzlich zwei unterschiedliche Preismodelle. Zum einen kann die Infrastruktur nach dem pay-as-you-go-Modell und zum anderen als reservierte Instanzen bezogen werden. Bei dem Bezug der Infrastruktur über die Variante der reservierten Instanzen wird eine einmalige Gebühr bezahlt, die für ein oder drei Jahre gilt. Dadurch werden die einzelnen angemieteten Instanzen günstiger als bei dem reinen pay-as-you-go-Modell. Die einzeln angemieteten Instanzen der reservierten Instanzen werden zusätzlich nach der Nutzungsdauer abgerechnet.

Da die unterschiedlichen Preismodelle schwer miteinander zu vergleichen sind, wird im Folgenden nur die Rechenkapazität von Anbietern mit dem pay-as-you-go-Modell betrachtet. Die Cloud-Anbieter bieten unterschiedliche Größen der CPUs und des RAMs an und auch innerhalb eines Anbieters können unterschiedliche Instanztypen angemietet werden. Da eine komplette Auflistung aller Instanzen jedes Anbieters den Rahmen der Studie sprengen würde, werden die Preise für die meisten Anbieter mit einer Preisspanne für die verschiedenen Instanztypen angegeben. Die geringeren Preise der Preisspanne sind für die kleineren Instanzen mit kleinen CPUs und wenig RAM, und die höheren Preise sind für die Instanzen mit größeren CPUs und mehr RAM. Microsoft ist der einzige Anbieter, der einen festen Preis für eine Instanz angibt.

Die Preise für die Serverinstanzen der Anbieter werden in Tabelle 6.1 gezeigt und die dazugehörigen Preise für den eingehenden und ausgehenden Datentransfer in Tabelle 6.2. Die Preise für den Datentransfer werden zum Teil als Preisspanne angegeben, da der Preis abhängig ist von der Menge der übertragenen Daten.

[2] http://aws.amazon.com/
[3] http://aws.amazon.com/
[4] http://www.gogrid.com/
[5] http://www.flexiscale.com/
[6] http://www.rackspacecloud.com/?RCMP=cleanEntry

Tabelle 6.1: Preise für Serverinstanzen

Anbieter	Serverinstanzen
Amazon EC2	$0,11 - $1,28 /Stunde
Microsoft Windows Azure	$0,12 /Stunde
GoGrid	$0,095 - $1,32 /Stunde
FlexiScale	$0,04 - $0,64 /Stunde
Rackspace Cloud Server	$0,015 - $0,96 /Stunde

Tabelle 6.2: Preise für den Datentransfer

Anbieter	Datentransfer eingehend	Datentransfer ausgehend
Amazon EC2	$0,10/GB	$0,10 - $0,17/GB
Microsoft Windows Azure	$0,10/GB	$0,15/GB
GoGrid	$0/GB	$0,50/GB
FlexiScale	$0,12/GB	$0,13 - $0,17/GB
Rackspace Cloud Server	$0,08/GB	$0,22/GB

Wird nur der günstigste Preis der Preisspanne betrachtet, so lässt sich erkennen, dass FlexiScale und Racspace Cloud Server die günstigsten Instanzen vermieten. Die teuersten Preise haben Amazon EC2 und GoGrid. Jedoch muss hier beachtet werden, dass sich diese Preise auf unterschiedliche Instanzen mit unterschiedlichen CPUs und RAMs beziehen. Die Preise des eingehenden Datentransfers können sehr gut miteinander verglichen werden, da dort keine Preisspannen existieren. Jedoch gibt es für den ausgehenden Datentransfer bei den Anbietern Amazon und FlexiScale wiederum eine Preisspanne, da diese sich auf die Menge des Datentransfers beziehen. Die Preise des eingehenden und ausgehenden Datentransfers sind allerdings sehr ähnlich bis auf den Anbieter GoGrid, bei dem der eingehende Datentransfer kostenlos ist und der ausgehende ein Vielfaches mehr kostet als bei den restlichen Anbietern.

Bei der Auswahl eines Anbieters muss eine Einzelfallbetrachtung durchgeführt werden und der Cloud-Anbieter und die Ressourcen nach den eigenen Anforderungen ausgewählt werden, da hier keine allgemeine Aussage getroffen werden kann.

Im Folgenden werden die bisher gezeigten Cloud-Anbieter für eine Beispielrechnung herangezogen, in der die Anforderungen zum Hosten einer kleinen, mittleren und großen Webseite betrachtet werden. Die Preise setzen sich aus den Preisen für die Rechenkapazität sowie dem ein- und ausgehenden Datentransfer zusammen. Es werden jeweils die Preise pro Monat berechnet und für die Nutzung der Rechenkapazität wird von 732 Stunden pro Monat ausgegangen. Das verwendete Datenvolumen ist in Tabelle 6.3, aufgeteilt nach ein- und ausgehenden Datentransfer, gezeigt. Die Preise für das Hosten der kleinen Webseite befinden sich in Tabelle 6.4, der mittleren Webseite in Tabelle 6.5 und der großen Webseite in Tabelle 6.6.

Anhand der Tabellen zeigt sich, dass kein Anbieter existiert, der für die verschie-

Tabelle 6.3: Menge des ein- und ausgehenden Datentransfers

Webseite	Datentransfer eingehend	Datentransfer ausgehend
Klein	1 GB	2 GB
Mittel	12 GB	120 GB
Groß	90 GB	900 GB

Tabelle 6.4: Beispiel für das Hosten einer kleinen Webseite

Anbieter	Rechenkapazität	Datentransfer eingehend	Datentransfer ausgehend	Preis
Amazon	$80,52	$0,10	$0,34	$80,96
Microsoft	$87,84	$0,10	$0,30	$88,24
GoGrid	$69,54	$0	$1,00	$70,54
FlexiScale	$29,28	$0,12	$0,34	$29,74
Rackspace	$10,98	$0,08	$0,44	$11,50

denen Anforderungen immer die günstigsten Ressourcen bereitstellt. In diesem Beispiel bietet Rackspace die günstigsten Ressourcen für eine kleine und mittlere Webseite an, während FlexiScale die günstigsten Ressourcen für eine große Webseite bereitstellt. Damit zeigt sich, dass die Cloud-Anbieter immer bezüglich den Anforderungen des Cloud-Nutzers betrachtet werden müssen. Wird für die Webseite beispielsweise noch zusätzlicher Datenspeicher benötigt, so kann wiederum ein ganz anderer Cloud-Anbieter die günstigsten Ressourcen bereitstellen.

Datenspeicher

Die Preise für den Datenspeicher von Amazon und FlexiScale sind gestaffelt nach der Menge der gespeicherten Daten, daher wird hier wieder die Preisspanne angegeben. Bei Microsoft, Rackspace und GoGrid sind die Kosten für jedes GB gleich, jedoch sind bei GoGrid die ersten 10 GB/Monat frei. Der ausgehende Datentransfer ist ebenso wie der Datentransfer im Abschnitt Rechenkapazität mit einer Preisspanne angegeben, da hier der Preis ebenfalls abhängig ist von der Menge der Daten. Tabelle 6.7 zeigt die Preise für die Nutzung des Datenspeichers der einzelnen Anbieter und die Preise für die Abfragen, wie bspw. PUT, POST und LIST. Die Preise für die Abfragen hängen bei Rackspace Cloud Files von der Größe der Abfragedatei ab, bei einer Größe kleiner 250 KB kostet die Abfrage nichts, bei einer Abfragedateigröße von mehr als 250 KB kosten 500 Abfragen $0,01/Monat. Tabelle 6.2 zeigt die Preise für den Datentransfer, welche die gleichen Preise sind wie für den Datentransfer der Rechenkapazität.

In Tabelle 6.7 zeigt sich, dass die Preise für die Anmietung des Speichers sehr ähnlich sind, mit der Ausnahme des Cloud-Anbieters FlexiScale, der wesentlich teurer ist als die anderen Cloud-Anbieter. Bei Amazon und FlexiScale hängen die Preise von der Menge der zu speichernden Daten ab, während Microsoft, GoGrid und Rackspace feste Preise anbieten, unabhängig der Menge der zu

Tabelle 6.5: Beispiel für das Hosten einer mittleren Webseite

Anbieter	Rechenkapazität	Datentransfer eingehend	Datentransfer ausgehend	Preis
Amazon	$80,52	$1,20	$20,40	$102,12
Microsoft	$87,84	$1,20	$18,00	$107,04
GoGrid	$69,54	$0	$60,00	$129,54
FlexiScale	$29,28	$1,44	$20,40	$51,12
Rackspace	$10,98	$0,96	$26,40	$38,34

Tabelle 6.6: Beispiel für das Hosten einer großen Webseite

Anbieter	Rechenkapazität	Datentransfer eingehend	Datentransfer ausgehend	Preis
Amazon	$80,52	$9,00	$153,00	$242,52
Microsoft	$87,84	$9,00	$135,00	$231,84
GoGrid	$69,54	$0	$450,00	$519,54
FlexiScale	$29,28	$10,800	$153,00	$193,08
Rackspace	$10,98	$7,200	$198,00	$216,18

speichernden Daten. GoGrid stellt seinen Service, als einziger der betrachteten Anbieter, für die ersten 10 GB/Monat kostenlos zu Verfügung.

GoGrid ist für die Anmietung von Speicher der günstigste betrachtete Infrastrukturanbieter, da bei diesem auch keine Kosten für die Abfragen entstehen. Jedoch muss, genauso wie bei der Anmietung der Rechenkapazität, eine Einzelfallbetrachtung gemacht werden bzgl. den Anforderungen des Cloud-Benutzers und den Leistungen, die der Anbieter zur Verfügung stellt.

Datenbank

Es werden zwei Datenbankservices betrachtet. Zum einen SimpleDB von Amazon und zum anderen der Service SQL Azure von Microsoft. Diese beiden Services besitzen unterschiedliche Bezahlmodelle. Während bei SimpleDB von Amazon die gemietete Datenbank pro GB und Monat bezahlt wird und die Maschinenstunden extra gezahlt werden, kann bei SQL Azure von Microsoft zwischen zwei Editionen gewählt werden, bei denen jeweils eine feste Größe der Datenbank gemietet und ein Festpreis gezahlt wird. Die Web Edition von SQL Azure bietet eine Datenbank bis zu einer Größe von 1 GB und die Business Edition bis zu einer Größe von 10 GB. Die Preise für den Datenbankspeicher und die benötigten Maschinenstunden pro Abfrage finden sich in Tabelle 6.8. Die Preise für den Datentransfer in Tabelle 6.9. Der Preis des ausgehenden Datentransfers von Amazon hängt wiederum von der Menge der übertragenen Daten ab und wird deshalb als Preisspanne angegeben.

Die zwei Datenbank-Services besitzen unterschiedliche Bezahlmodelle der Service SimpleDB von Amazon wird als Pay-as-you-go-Modell angeboten und bei Microsoft wird die Datenbank in Paketen mit fester Speichergröße angeboten.

Tabelle 6.7: Preise für den Datenspeicher

Anbieter	Speicher	Abfragen
Amazon S3	$0,15 - $0,18/GB/Monat	$0,12 pro 1000 Abfragen
Microsoft Windows Azure	$0,15/GB/Monat	$0,01 pro 10000 Abfragen
GoGrid	10 GB/Monat frei, dann $0,15/GB/Monat	$0/GB
FlexiScale	$0,43-$0,49/GB/Monat	$0/GB
Rackspace Cloud Files	$0,15/GB/Monat	$0 - $0,01 pro 500 Abfragen pro Monat

Tabelle 6.8: Preise für Datenbanken

Anbieter	Speicher	Maschinenstunden
Amazon SimpleDB	1 GB/Monat frei, dann $0,25/GB	25 Maschinenstunden frei, dann $0,14/Stunde
Microsoft SQL Azure	Web Edition bis 1 GB $9,99/Monat Business Edition bis 10 GB $99,99/Monat	$0/Stunde $0/Stunde

Zusätzlich werden bei Amazon die Maschinenstunden für eine Abfrage berechnet, bei Microsoft ist dies bereits in dem Paketpreis inbegriffen. Der Datenbank-Benutzer muss den Service nach dem bevorzugten Bezahlmodell und seinen Anforderungen an die Datenbank auswählen.

6.1.2 Plattformservices

Plattformservices stellen plattformorientierte Ressourcen und IT-Infrastruktur zur Entwicklung und Bereitstellung von Cloud-Anwendungen bereit. Es werden die Anbieter Google[7], LongJump[8] und Force.com[9] betrachtet. Diese drei Anbieter stellen alle eine Anwendungsentwicklungs- und Hostingplattform bereit, womit eigene Webanwendungen erstellt und gehostet werden können. Google bietet die Programmiersprachen Python und Java zur Erstellung von Anwendungen an. Mit LongJump können Anwendungen mit Java und Javascript erstellt werden. Außerdem können die Anwendungen über ein Plugin direkt in Eclipse entwickelt werden. Bei Force.com können sowohl bereits erstellte Anwendungen durch die sogenannte Zeigen-und-Klick-Funktionalität verwendet werden, als auch eigene Anwendungen mit der Java-ähnlichen Programmiersprache Apex entwickelt werden.

[7] http://code.google.com/intl/de-DE/appengine/
[8] http://longjump.com/index.htm
[9] http://www.salesforce.com/platform/cloud-platform/

Tabelle 6.9: Preise für den Datentransfer

Anbieter	Datentransfer eingehend	Datentransfer ausgehend
Amazon SimpleDB	1 GB/Monat frei, dann $0,10/GB	$0,10 - $0,17/GB
Microsoft SQL Azure	$0,10/GB	$0,15/GB

Die Anbieter Force.com und LongJump bieten bei der Abrechnung ihrer Services komplette Pakete an, die sich u.a. in der Anzahl der benutzerdefinierten Objekte und im verfügbaren Speicher unterscheiden. Die Höhe des Nutzungsentgelts, die Anzahl der benutzerdefinierten Objekte und die Größe des zur Verfügung stehenden Speichers der beiden Anbieter Force.com und LongJump sind in Tabelle 6.10 gezeigt. Der Anbieter LongJump unterteilt den Speicher in Daten- und Dokumentenspeicher. In der tabellarischen Ansicht sind die zwei Speichertypen addiert aufgelistet, wobei der Datenspeicher immer $\frac{1}{5}$ des Dokumentenspeichers beträgt. D. h. für die Bronze-Edition, dass der Datenspeicher eine Größe von 5 MB und der Dokumentenspeicher eine Größe von 25MB besitzt, in der Silber-Edition hat der Datenspeicher eine Größe von 10MB und der Dokumentenspeicher von 50 MB und bei der Gold-Edition sind es 20 MB bei dem Datenspeicher und 100MB bei dem Dokumentenspeicher. Bei LongJump kann zusätzlich extra Speicher mit angemietet werden, wenn der verfügbare Speicher nicht ausreicht. Zusätzlicher Datenspeicher von 50 MB kostet $49/Monat und 250MB Dokumentenspeicher kostet $49/Monat.

Tabelle 6.10: Preise für die Plattform-Services von Force.com und LongJump

Anbieter	Nutzungsentgelt	Objekte	Speicher
Force.com			
Free	frei	10	10 MB/Benutzer
Enterprise	$50/User/Monat	200	20 MB/Benutzer
Unlimited	$75/User/Monat	2000	120 MB/Benutzer
LongJump			
Bronze	$30/User/Monat	10	30 MB
Silber	$60/User/Monat	200	60 MB
Gold	$90/User/Monat	2000	120 MB

Google App Engine hingegen bietet seinen Service kostenfrei an, so lange eine bestimmte Quote nicht überschritten wird. Die Quote und die Preise für den Mehrverbrauch für den Speicher und die Maschinenbelegung von Google App Engine sind in Tabelle 6.11 und der Datentransfer in Tabelle 6.12 gezeigt.

Tabelle 6.11: Preise für Google App Engine

Anbieter	Speicher	Maschinenbelegung
Google App Engine	1 GB/Tag frei, dann $0,15/GB	6,5 CPU-Stunden/Tag frei, dann $0,10/CPUStunde

Tabelle 6.12: Preise für den Datentransfer von Google App Engine

Anbieter	Datentransfer eingehend	Datentransfer ausgehend
Google App Engine	1 GB/Tag frei, dann $0,10/GB	1 GB/Tag frei, dann $0,12/GB

Welcher der betrachteten Plattformservices der richtige für einen Cloud-Benutzer ist, kann nicht allgemein gesagt werden. Sie bieten alle eine Anwendungsentwicklungs- und Hostingplattform an, aber bereits bei der Bereitstellung der Programmiersprache unterscheiden sich die betrachteten Anbieter, wobei meist Java, .Net oder Python als Programmiersprachen zum Einsatz kommen und unterstützt werden. Während Google seinen Dienst bis zu einer bestimmten Quote kostenlos zur Verfügung stellt und dann das pay-as-you-go-Modell verwendet, bieten Force.com und LongJump Paketpreise an, wobei sich die Pakete u.a. durch die Größe des verfügbaren Speichers und der Anzahl der benutzerdefinierten Objekte unterscheiden.

Welcher Anbieter der richtige ist, muss in einer Einzelfallbetrachtung entschieden werden.

6.1.3 Anwendungsservices

Mittlerweile gibt es eine große Auswahl von Anwendungsservices im Internet. Sowohl Email-Anwendungen, als auch Tabellenkalkulations- oder CRM (Customer Relationship Management)-Anwendungen können über das Internet angemietet werden. In diesem Abschnitt wird ein Überblick über die Anwendungsservices Google Apps[10], IBM Lotus Live[11], Microsoft Office Live[12] und Salesforce CRM[13] gegeben.

Google Apps

Google Apps ist eine Anwendungssuite die folgende Anwendungen zur Verfügung stellt:

- Google Mail,
- Google Kalender,
- Google Talk (Instant Messaging und Voice-over-IP),
- Google Text & Tabellen (Text-, Tabellen- und Präsentationsanwendungen),
- Google Sites (Erstellung und Veröffentlichung von Websites),

[10] http://www.google.com/apps/intl/en/business/index.html
[11] https://www.lotuslive.com/
[12] http://www.officelive.com/de-DE/
[13] http://www.salesforce.com/de/crm/service.jsp

- Google Video (Videohosting und -streaming).

Es stehen drei Editionen von Google Apps zur Verfügung, eine kostenlose werbefinanzierte Standard-Edition für den Privatanwender, eine Education-Edition für Schulen und Universitäten und eine Professional-Edition für Unternehmen. Die Standard- und Education-Editionen sind kostenlos. Die Professional-Edition kostet $50/Benutzer/Jahr.

IBM LotusLive

LotusLive bietet u.a. Emailanwendungen, Web Meeting-Anwendungen und Social Networking-Anwendungen an. Die Preise der Services variieren zwischen der monatlichen und jährlichen Bereitstellung, wobei sie bei der jährlichen Bereitstellung günstiger sind. Im Folgenden wird ein kurzer Überblick über die Services LotusLive Notes, LotusLive Meetings, LotusLive Events und LotusLive Connections gegeben, wobei die Preise für die monatliche Zahlung angegeben werden.

LotusLive Notes ist eine Emailanwendung, die u.a. einen Kalender und eine Kontaktverwaltung bereitstellt. LotusLive Notes kostet $9,00/Monat.

LotusLive Meetings ist eine Web Meeting-Anwendung mit vollem Funktionsumfang, mit der Informationen verteilt werden, Präsentationen gegeben und Software demonstriert werden kann. Der Service kostet $48,00/Monat.

LotusLive Events enthält die gleichen Services wie LotusLive Meetings und zusätzlich ein Eventmanagementservice, mit dem bspw. automatische Erinnerungsmails verschickt werden können und auf die Gastregistrierungsinformationen zugegriffen werden kann. LotusLive Events kostet $99/Monat.

LotusLive Connections ist ein Social Networking- und Kollaborationsservice und kostet $12,20/Monat.

Microsoft Office Live

Microsoft bietet mit Office Live zwei Editionen an, Office Live Workspace und Office Live Small Business. Office Live Workspace bietet eine kostenfreie Onlinespeicherung und -dokumentenfreigabe sowie die Office-Programme Word, Excel und PowerPoint an. Die Größe des Speichers ist jedoch auf 5 GB begrenzt.

Office Live Small Business stellt Webpräsenz, Verwaltungstools, Email-Konten und die Office-Programme Word, Excel und Powerpoint kostenlos zur Verfügung. Die folgenden Dienste sind in der Office Live Small Business-Edition jedoch kostenpflichtig:

- Domainnamenregistrierung kostet 9,99€/Jahr für .de und .eu Adresse, bzw. 11,99€/Jahr für .com, .org und .net Adressen

- Premium-Email (werbefreie Emailkonten) für 19,03€/Jahr
- Zusätzlicher Speicher, je nach Größe zwischen 4,75€/Jahr - 14,27€/Jahr
- Zusätzliche Benutzer, je nach Anzahl der Benutzer zwischen 14,27€/Monat - 124,94/€Monat

Salesforce

Salesforce.com stellt vier Editionen für Customer Relationship Management Lösungen mit unterschiedlichem Funktionsumfang bereit. Die Group Edition ist die Edition mit dem kleinsten Funktionsumfang. Es werden Vertriebs- und Marketing-Anwendungen bereitgestellt, wie z. B. Accountmanagement, Kontaktmanagement, Einrichtung von Email-Vorlagen, Verschickung von Massen-Emails oder Datenvalidierung. Zusätzlich zu diesen Funktionalitäten bietet die Professional-Edition Lösungen für Callcenter-Mitarbeiter, wie Kundenvorgangswarteschlangen und automatische Zuweisung, und anpassbare Dashboards an. Anwendungen, wie z. B. Regionsmanagement, Umsatz- und Planungsmanagement und Datenbankspiegelungen in Echtzeit, bietet die Enterpise-Edition an. Die Unlimited-Edition, mit dem größten Funktionsumfang, enthält zusätzlich zu der Enterprise-Edition eine automatische Synchronisation der Daten mit einem bevorzugten mobilen Gerät und den Zugriff auf Salesforce-Anwendungen über ein mobiles Gerät. Weitere Unterschiede zwischen den einzelnen Editionen werden in den Tabellen 6.13 und 6.14 gezeigt, wie der Preis, Anzahl an benutzerdefinierten Anwendungen, maximale Anzahl unterstützter Abonnenten pro Edition und der verfügbare Speicher.

Tabelle 6.13: Preise und Anzahl an benutzerdefinierten Anwendungen bei Salesforce

Edition	Preis	Benutzerdefinierte Anwendungen
Group Edition	75€/Benutzer/Jahr	1
Professional Edition	840€/Benutzer/Jahr	5
Enterprise Edition	1620€/Benutzer/Jahr	10
Unlimited Edition	3240€/Benutzer/Jahr	Unbegrenzt

Tabelle 6.14: Maximale Anzahl unterstützter Abonnenten und Speichergröße bei Salesforce

Edition	Maximale Anzahl unterstützter Abonnenten pro Edition	Speicher
Group Edition	5	1 GB insgesamt
Professional Edition	Unbegrenzt	20 MB/Benutzer
Enterprise Edition	Unbegrenzt	20 MB/Benutzer
Unlimited Edition	Unbegrenzt	120 MB/Benutzer

Hier wurde eine Auswahl von Anwendungsservices vorgestellt, die angemietet werden können. Welcher Anbieter der richtige ist, muss individuell, für die speziellen Anforderungen des Benutzers, entschieden werden.

6.1.4 Verwaltungsservices

Zur Verwaltung der Infrastruktur oder von Anwendungen können Verwaltungsservices von Drittanbietern verwendet werden. In diesem Abschnitt werden die Verwaltungsservices Scalr[14] und RightScale[15] kurz vorgestellt. Scalr kann nur die Infrastruktur von Amazon EC2 verwalten. RightScale kann verschiedene Cloud-Infrastrukturen von verschiedenen Anbietern verwalten, wie bspw. Amazon und GoGrid.

Scalr

Scalr ist ein redundanter und skalierender Verwaltungsservice für Amazon EC2. Mit diesem Service können Serverfarmen, bestehend aus EC2 Instanzen vordefiniert werden. Bei steigendem Ressourcenbedarf oder bei dem Ausfall einer oder mehrerer Instanzen werden automatisch neue Instanzen zugeschaltet und bei weniger Ressourcenbedarf werden die Instanzen abgeschaltet. Zur Einrichtung der Serverfarmen stehen eine Reihe von vorgefertigten Images zur Verfügung, wie Load-Balancer, Application-Server oder Datenbanken. Die Kosten für den Verwaltungsservice von Scalr betragen $50/Jahr und die Kosten für die Instanzen von EC2 müssen separat bei Amazon gezahlt werden.

RightScale

RightScale ist ebenfalls ein Verwaltungsservice, der Anwendungen und Infrastrukturen in der Cloud ausführt und verwaltet. Dieser Anbieter hat den Vorteil, dass mehrere Cloud-Infrastrukturen von verschiedenen Anbietern verwaltet werden können, wie bspw. Amazon, FlexiScale, GoGrid oder Rackspace. Die Kosten für die Infrastrukturen von diesen Anbietern müssen separat gezahlt werden und sind nicht in den Gebühren von RightScale enthalten. RightScale stellt mehrere Editionen bereit, die von skalierbaren Webseiten bis hin zu skalierbaren Batchverarbeitung reichen. Die Website Edition bietet alles an, was benötigt wird, um eine skalierbare Webseite in der Cloud laufen zu lassen. Zum Kontrollieren und Verwalten von Grid-Computing und Batchanwendungen in einer skalierbaren, fehlertoleranten Umgebung wird die Grid Edition angeboten. Die Enterprise Edition besitzt alle Funktionen, die auch die Editionen Website und Grid bereitstellen. Die Premium Edition bietet zusätzlich zur Enterprise Edition Administrationsfunktionen, multi-cloud Support und einen erweiterten Support an. Darüber hinaus bietet RightScale eine Developer Edition an, mit der einige Funktionen kostenlos getestet werden können. In Tabelle 6.15 sind die verschiedenen Editionen und die dazugehörigen Preise gezeigt, welche sich in eine einmalige Nutzungsgebühr und einen Mindestumsatz pro Monat unterteilen.

[14] `https://scalr.net/login.php`
[15] `http://www.rightscale.com/`

Tabelle 6.15: Preise für Editionen von RightScale

Edition	Einmalige Nutzungsgebühr	Mindestumsatz
Developer	kostenfrei	kostenfrei
Website	$2500	$500/Monat
Grid	$2500	$500/Monat
Enterprise	$4000	$1000/Monat
Premium	$10000	$4000/Monat

In diesem Abschnitt wurden nur die zwei Verwaltungsservices von Scalr und RightScale betrachtet. Der große Vorteil von RightScale ist die Verwaltung von mehreren Infrastrukturen im Vergleich zu Scalr, der nur die Verwaltung der Infrastrukturen von Amazon EC2 anbietet. Die Preise bei RightScale sind deutlich höher als bei Scalr, dafür stellt RightScale unterschiedliche Funktionen in den Editionen bereit. Welcher dieser Services für den Benutzer der richtige ist, muss individuell entschieden werden.

6.1.5 Sicherheit als Service

Sicherheitsservices von Drittanbietern existieren für die unterschiedlichsten Anwendungen und Anbieter. In diesem Abschnitt werden die folgenden drei Services kurz vorgestellt: Google Message Security[16] zur Überwachung des Emailverkehrs, Benutzerverwaltungs- und Single Sign-On-Service von PingIdentity[17] und VPN-Cubed für EC2[18] von CohesiveFT, welches ein Overlay-Netzwerk für Amazon EC2 anbietet.

Google Message Security

Google Message Security von Postini, ist ein Softwareservice, der die eingehenden und ausgehenden Emails überwacht. Spam-Nachrichten, Viren und anderen Emailbedrohungen werden geblockt und erreichen somit nicht das Unternehmen. Der Benutzer kann die Spamschutz-Einstellungen selber konfigurieren. Zur Verschlüsselung der Emailkommunikation unterstützt Google Message Security TLS (Transport Layer Security). Zusätzlich kann die Verschlüsselung für alle Kommunikationen zwischen den gewünschten Emaildomainen eingestellt werden. Der Google Message Security Service kostet $12/Benutzer/Jahr. Postini bietet zusätzlich den Archivierungsservice Google Message Discovery an, der die gleichen Funktionen wie Google Message Security enthält und zusätzlich die Emails archiviert. Dieser Service kostet für ein Jahr Emailarchivierung $25/Benutzer/Jahr und für 10 Jahre Emailarchivierung $45/Benutzer/Jahr.

[16] http://www.google.com/postini/email.html#archive
[17] http://www.pingidentity.com/
[18] http://www.cohesiveft.com/vpncubed/

PingIdentity

PingIdentity bietet mit PingConnect einen On-Demand Single Sign-On (SSO) und Benutzerwaltungsdienst an. PingConnect unterstützt mehr als 60 Softwareservices, wie Google Apps, Salesforce CRM, Postini (Google) oder SuccessFactors. Der Service kostet 1€/Benutzer für eine Anwendung im Monat.

VPN-Cubed für EC2

CohesiveFT bietet mit seinem Produkt VPN-Cubed für EC2 ein Overlay-Netzwerk für Amazon EC2 an, mit welchem innerhalb der Umgebung in Amazon eine gesicherte Verbindung etabliert werden kann.

Es existieren zwei Varianten des VPN-Cubed für EC2, eine kostenfreie Variante und nicht kostenfreie Variante. Die kostenfreie Variante beinhaltet zwei VPN-Cubed Manager. Die VPN-Cubed Manager können zwei Server wahlweise innerhalb einer Region (EU- oder US-Region) oder zwischen den beiden Regionen miteinander verbinden. Die zweite Variante kostet $0,05/Stunde und beinhaltet 4 VPN-Cubed Manager mit denen bspw. vier Server innerhalb und/oder außerhalb einer Region verwendet werden können.

Es exisitieren Sicherheitsservices von Dritten, die bereits gemietete Services absichern, jedoch ist hier die Auswahl noch nicht so groß wie bspw. bei den Anwendungen oder Infrastrukturen. Welche zusätzlichen Sicherheitsservices von Dritten Service-Anbietern benötigt werden, muss jeder Benutzer individuell entscheiden.

6.2 Sicherheitsfunktionen aktueller Cloud-Anbieter

Die Taxonomie aus Kapitel 5 wird exemplarisch auf einige Anbieter bzw. Services angewandt und die aktuellen Sicherheitsfunktionen betrachtet. An dieser Stelle wird keine vollständige Auflistung aller Services und deren aktuellen Sicherheitsfunktionen gegeben.

Zunächst wird in Abschnitt 6.2.2 auf die Sicherung der Daten und die Verschlüsselung der Daten in der Cloud eingegangen. Im Anschluss daran wird in Abschnitt 6.2.1 die physikalische Sicherheit von Rechenzentrumsbetrieben und die Netzwerksicherheit der Cloud-Anbieter kurz erläutert. Abschnitt 6.2.3 gibt einen Einblick in die Service-Level-Agreements der Cloud-Anbieter und Abschnitt 6.2.4 zeigt auf, welche Zertifikate die Cloud-Anbieter besitzen.

6.2.1 Infrastruktur

In diesem Abschnitt wird sowohl auf die physikalische Sicherheit von Rechenzentrumsbetrieben, als auch auf die Netzwerksicherheit eingegangen, die bereits in Kapitel 5.2 identifiziert wurde. Es wird auf Maßnahmen zur Sicherung der Rechenzentrumsbetriebe und des Netzwerks der folgenden Cloud-Anbieter eingegangen: Amazon [5], Google [4], GoGrid[19] und Microsoft [6].

Zur Sicherung eines Rechenzentrums gibt es mehrere Aspekte die betrachtet werden müssen. Von der Wahl des Grundstücks über die Sicherheitssysteme bis zur Zugangskontrolle müssen Maßnahmen ergriffen werden, um das Rechenzentrum zu schützen. Das Grundstück sollte so gewählt werden, dass es sich nicht in Hochwasser- oder Erdbebengebieten befindet. Die Rechenzentren von Google sind z. B. in Gebieten gelegen, die soweit wie möglich vor Katastrophen geschützt sind.

Sowohl die Außenanlage des Rechenzentrums, als auch Rechnerräume und kritische Infrastrukturräume sollten überwacht werden. Amazon kontrolliert durch Sicherheitspersonal die Außenanlage des Rechenzentrums und den Gebäudezugang mit Hilfe von Videoüberwachung, Einbruchsmeldeanlagen und anderen elektronischen Mitteln. Bei Google wird sowohl lokal als auch zentral, in Googles *Security Operations Center*, das Rechenzentrum überwacht. Das Rechenzentrum von GoGrid wird mit modernen Audio- und Videoanlagen überwacht und zusätzliche durch Wachpersonal vor Ort. Microsoft kombiniert eine Reihe von Technologien um die physikalische Sicherheit des Rechenzentrums zu sichern. Es werden sowohl Kameras und Alarme, als auch traditionelle Sicherheitsmechanismen, wie Schloss und Schlüssel verwendet.

Um Zugang zu den Rechenzentren von Amazon zu erhalten, müssen Mitarbeiter eine Zwei-Faktor-Authentifizierung durchführen. Besucher müssen sich identifizieren und werden kontinuierlich von autorisiertem Personal begleitet. Alle physikalischen Zugänge bei Amazon werden geloggt und routinemäßig überprüft. Bei Google haben nur ausgewählte Google Mitarbeiter Zugang zu den Rechenzentren und auch hier werden die Zugänge kontrolliert und überprüft. Besucher haben keinen Zugang zu den Google Rechenzentren. Bei dem Zugang ins Gebäude von GoGrid müssen sich alle Personen registrieren und eine gültige ID hinterlassen, während sie sich im Gebäude befinden.

Amazon, GoGrid und auch Microsoft verwenden Virtualisierungslösungen in der Cloud-Infrastruktur. Jedoch verwenden die Cloud-Anbieter nicht alle die gleichen Lösungen. Amazon und GoGrid setzen beispielsweise die Virtualisierungslösung von Xen ein, wobei Amazon Paravirtualisierung und GoGrid Hardware-Virtualisierung verwendet. Microsoft hingegen verwendet eine eigene Virtualisierungslösung namens Windows Azure Hypervisor.

Cloud-Anbieter haben täglich mit einer Menge an Netzwerkangriffen zu kämpfen, wie z. B. verteilte Denial-of-Service, Man-in-the-Middle oder Port Scanning

[19] `http://www.gogrid.com/legal/sla.php`

Angriffen. Um diese Angriffe abzuwehren, werden eine Reihe von Anwendungen und Standardtechnologien eingesetzt. Im Folgenden wird ein Einblick in die Maßnahmen von Cloud-Anbietern, zur Verhinderung dieser Angriffe, gegeben.

Zur Verhinderung von verteilten Denial-of-Service Angriffen verwendet Amazon eigene Maßnahmen um die Angriffe abzuwehren, die jedoch nicht weiter beschrieben sind. Microsoft verwendet zur Verhinderung von verteilten Denial-of-Service Angriffen Techniken, wie Load-Balancer, zur Lastverteilung auf mehreren Servern, Firewalls und Intrusion Prevention Systeme.

Alle APIs von Amazon sind über SSL geschützte Endpunkte verfügbar, welche eine Serverauthentifizierung benötigen. Dadurch werden Man-in-the-Middle Angriffe verhindert, bei denen ein Angreifer versucht, die volle Kontrolle über den Datenverkehr zu erhalten und beliebige Informationen einzuspielen und zu manipulieren.

Standardmäßig sind bei Amazon EC2 alle eingehende Ports gesperrt und somit vor Port Scanning Angriffen geschützt. Jedoch kann jeder Benutzer beliebige Ports öffnen. Sobald bei Amazon ein Port Scanning entdeckt wird, wird es gestoppt und blockiert.

Auch Google wird mit diesen Angriffen konfrontiert und versucht sie, durch eine Vielzahl von kommerziellen und proprietären Anwendungen zum Scannen von Netzwerken und Anwendungen zu verhindern. Zusätzlich arbeitet Google mit Dritten zusammen, um die Google Infrastruktur und Anwendungssicherheit zu testen und zu verbessern.

Zur Verschlüsselung der Netzwerkverbindung wird von den meisten Anbietern SSL und HTTPS eingesetzt. Der Zugang zu Google Apps und den meisten Endanwenderprogrammen von Google wird über eine SSL-Verbindung gesichert. Zusätzlich wird für die meisten Services innerhalb von Google Apps ein HTTPS-Zugang angeboten. Der Zugang zu Kalender und Email kann standardmäßig auf HTTPS eingestellt werden, so dass nur noch über eine verschlüsselte Verbindung darauf zugegriffen werden kann. Auch Microsoft Office Live bietet eine SSL-Verbindung an, jedoch ist diese nicht standardmäßig eingestellt, kann aber jederzeit aktiviert werden. GoGrid bietet ebenfalls eine SSL-Verschlüsselung zu ihrem Portal und für die API an. Die Services von Amazon Web Services sind über eine gesicherte SSL-Verbindung sowohl über das Internet als auch innerhalb von EC2 erreichbar.

6.2.2 Architektur

Strategien zur Datensicherheit, die bereits in Kapitel 5.3 beschrieben wurden, werden hier am Beispiel der Cloud-Anbieter Amazon [5], Google [4] und FlexiScale[20] betrachtet. Die Strategie der Datenverschlüsselung wird anhand des Cloud-Anbieters Amazon gezeigt.

[20] `http://www.flexiscale.com/faqs.php`

Amazon sichert die gespeicherten Daten von Amazon S3, SimpleDB und Elastic Book Store redundant an mehreren physikalischen Orten ab. Die Kopien von Amazon Elastic Book Store werden in der gleichen Verfügbarkeitszone gesichert und nicht über mehrere Zonen hinaus. Google sichert ebenfalls die gespeicherten Daten redundant über eine Vielzahl an physikalischen und logischen Speicherkapazitäten ab, um bei einer unbeabsichtigten Löschung der Daten diese wieder herstellen zu können. Auch FlexiScale macht eine Sicherung der Daten, allerdings erlaubt es den Kunden nicht die Wiederherstellung virtueller Platten oder einzelner Dateien. Für die Sicherung der eigenen Daten muss jeder Benutzer selber sorgen.

Innerhalb der Services von Amazon Web Services werden die Daten nicht verschlüsselt. Es existiert zwar die Möglichkeit der verschlüsselten Datenübertragung, aber die Speicherung der Daten geschieht unverschlüsselt. Jedoch können die Benutzer der Services die Daten vor dem Hochladen auf die entsprechenden Server selbst verschlüsseln und die verschlüsselten Daten abspeichern.

6.2.3 Verwaltung

In Kapitel 5.4 wurden bereits die Service-Level-Agreements beschrieben, welche die Nutzung eines Cloud-Services regeln. Jeder Cloud-Anbieter hat seine eigenen Service-Level-Agreements für die unterschiedlichen Dienste, die er anbietet. Meist sind sich diese jedoch sehr ähnlich. Unterschiede gibt es z. B. in der Bereitstellung der Service-Gutschrift für eine Nichteinhaltung der Verfügbarkeit der Services. Es gibt Anbieter, die eine Servicebereitstellung anbieten, d. h. die Vertragsdauer für den Service wird um eine Anzahl an Tagen verlängert. Andere Anbieter gewähren eine Gutschrift, die für zukünftige Gebühren verwendet werden können. Ein Beispiel von Service-Level-Agreements wird anhand der beiden Services Google Apps[21] und Amazon S3[22] gegeben.

Google stellt bei Google Apps eine Verfügbarkeit von 99,9% pro Kalendermonat sicher. Wird diese Verfügbarkeit nicht von Google erbracht, so muss der Benutzer innerhalb von 30 Tagen eine Service-Gutschrift anfordern, da sonst das Recht auf eine Gutschrift verfällt. Die Service-Gutschrift kann bei Google nicht geldlich eingetauscht oder ausbezahlt werden, sondern wird in Form einer Servicebereitstellung für maximal 15 Tage erbracht. Die Ausfallzeit wird basierend auf einer serverseitigen Fehlerrate gemessen und wird bis zu maximal 12 Stunden pro Kalenderjahr nicht als Ausfallzeit gemessen. Wie viele Tage zusätzlicher Service bereitgestellt wird, ist in Tabelle 6.16 gezeigt. Der monatliche Betriebszeitprozentsatz lässt sich - vereinfacht - folgendermaßen berechnen:

$$\frac{\text{Gesamtzahl der Minuten in einem Kalendermonat - Ausfallzeit in Minuten}}{\text{Gesamtzahl der Minuten in einem Kalendermonat}}.$$

[21] http://www.google.com/apps/intl/en/terms/sla.html
[22] http://aws.amazon.com/s3-sla/

Tabelle 6.16: Service-Gutschrift für nicht erbrachte Verfügbarkeit von Google

Monatlicher Betriebszeitprozentsatz	Zusätzliche Servicebereitstellung
99,0% < x < 99,9%	3 Tage
95,0% < x < 99,0%	5 Tage
x < 95,0%	15 Tage

Amazon S3 stellt ebenso wie Google eine Verfügbarkeit von 99,9% pro Kalendermonat sicher. Wird diese Verfügbarkeit unterschritten, so kann der Benutzer eine Service-Gutschrift anfordern. Liegt die Verfügbarkeit zwischen 99,0% und 99,9%, so wird die Rechnung um 10% gekürzt und bei einer Verfügbarkeit von weniger als 99% wird die Rechnung um 25% gekürzt.

Die bekannten Service-Level-Agreements von Cloud-Anbietern beinhalten auch Ausschlüsse, die sich zum Teil sehr ähnlich sind. Drei Ausschlusskriterien von den Cloud-Anbietern Amazon und Google, die bei beiden Anbietern ähnlich sind, werden kurz aufgeführt. Die Ausfallzeit wird nicht berechnet, wenn

1. sich die Probleme außerhalb der Kontrolle des jeweiligen Betreibers befinden,
2. aufgrund von Aktivitäten oder Untätigkeiten des Kunden oder eines Dritten,
3. aufgrund von Problemen der Gerätschaften des Kunden und/oder der Gerätschaften eines Dritten, die nicht innerhalb der primären Kontrolle der Anbieter liegen.

6.2.4 Compliance

In Kapitel 5.5 wurde bereits auf die Notwendigkeit von Datenschutzgesetzen, Gesetzen zum Schutz der Privatsphäre und Sicherheitsrichtlinien in Cloud-Systemen eingegangen. Im Folgenden werden Cloud-Anbieter aufgezeigt, die Zertifizierungen bzgl. der Sicherheitsrichtlinien besitzen, und Cloud-Anbieter, die sich mit Datenschutzbestimmungen nach dem Safe Harbor[23] Abkommen und dem TRUSTe-Programm[24] auseinandersetzen.

Die meisten Cloud Computing Anbieter sind mit dem SAS (Statement on Auditing Standard) 70 Type II Report zertifiziert. Dieser Report ist für alle ausgelagerten Dienstleistungen zu erstellen, die einen Einfluss auf Unternehmensaktionen haben und bestätigt, dass ein Unternehmen über ein funktionierendes Kontrollsystem verfügt. Obwohl SAS 70 ein US-Standard ist, ist dieser auch für viele deutsche und europäische Unternehmen wichtig, wenn diese bspw. für Auftraggeber in den USA tätig sind. SAS 70 zertifizierte Cloud-Anbieter sind bspw. Amazon, Google, Microsoft, Salesforce oder GoGrid.

[23] http://www.export.gov/safeharbor/
[24] www.truste.org

Microsoft und Salesforce besitzen neben der SAS 70 Type II Zertifizierung ein ISO/IEC 27001 Zertifikat, welches die internationale Norm für Informationssicherheits-Managementsysteme (ISMS) ist. Diese Norm spezifiziert die Anforderungen an Implementierung, Überwachung, Wartung und Verbesserung eines dokumentierten ISMS, das nach diesem Standard zertifiziert werden kann. Das Zertifikat bestätigt, dass Microsoft und Salesforce die Sicherheitsmechanismen nach diesem Standard implementiert haben.

Safe Harbor ist eine Datenschutzbestimmung, die es erlaubt personenbezogene Daten aus der Europäischen Union in die Vereinigten Staaten zu übermitteln. Mit der Registrierung in dem US-Handelsministerium verpflichten sich US-Unternehmen, einige europäische Datenschutzanforderungen einzuhalten. Cloud-Anbieter die dem Safe-Harbor-System beigetreten sind, bieten einen ausreichenden Schutz bzgl. Benachrichtigungen, Weiterleitung, Sicherheit, Datenintegriät und Zugriffsrechten. In das US-Handelsministerium eingetragene Cloud-Anbieter sind beispielsweise Amazon, Google, Microsoft, IBM, Salesforce und Rackspace.

Neben den Safe Habor Datenschutzbestimmungen existiert das TRUSTe-Programm. TRUSTe ist eine unabhängige, gemeinnützige amerikanische Initiative, die dafür eintritt, dass Benutzer ihre Zustimmung zur Verwendung der Daten geben müssen und über die folgenden Punkte im Privacy Statement informiert sind:

- Welche persönlichen Daten werden gespeichert?
- Wie werden die Daten verwendet?
- Werden die Daten an Dritte weitergegeben?
- Welche Sicherheitsmaßnahmen bestehen, um Verlust, Missbrauch oder Veränderungen zu verhindern?
- Wie kann der Kunde seine Daten einsehen oder verändern?

Cloud-Anbieter die das TRUSTe-Siegel besitzen sind z. B. Microsoft, IBM und Salesforce.

In Tabelle 6.17 befindet sich eine komplette Auflistung der betrachteten Anbieter und ihrer Zertifizierungen.

Die Sicherheitstechnologien in den Bereichen Infrastruktur, Architektur, Verwaltung und Compliance sind noch nicht genügend dokumentiert, um die Cloud-Anbieter möglichst genau auf ihre Sicherheitsmaßnahmen überprüfen zu können. Im Bereich der Verwaltung werden die Informationen der Service-Level-Agreements den Cloud-Benutzern zur Verfügung gestellt, jedoch wird bei diesen nicht detailliert auf die Sicherheit eingegangen, sondern hauptsächlich auf die Verfügbarkeit der Services. Cloud-Anbieter deren Sicherheitsrichtlinien zertifiziert wurden, dem Safe-Harbor-System beigetreten sind und/oder sich dem TRUSTe-Programm angeschlossen haben, geben diese Informationen auf ihren Webseiten bekannt. Es ist jedoch nicht immer nachvollziehbar wie Cloud-Anbieter vorgehen, die nicht im Besitz dieser Zertifikate sind oder diesen

Tabelle 6.17: Zertifikate der betrachteten Anbieter

Anbieter	TRUSTe	Safe Harbor	SAS 70 Type II	ISO/IEC 27001
Microsoft	x	x	x	x
Google	x		x	
Amazon	x		x	
Salesforce	x	x	x	x
PingIdentity			x	
Postini		x	x	
CohesiveFT				
Scalr				
RightScale				
IBM	x	x	x	x
GoGrid	x		x	
FlexiScale				
Rackspace	x			
LongJump				

Programmen beigetreten sind. Im Bereich der Infrastruktur werden bereits eine Reihe von Sicherheitstechnologien beschrieben, jedoch fehlen auch hier noch ausreichend dokumentierte Informationen.

6.3 Anwendung der Taxonomie auf Amazon Cloud Services

Die Taxonomie aus Kapitel 5 wird beispielhaft auf den Cloud-Anbieter Amazon angewandt. Die Beantwortung der Checklisten basiert auf öffentlichen Informationsquellen, wie Webseiten, Whitepaper [5] und dem Forum[25] von Amazon. Im Folgenden sind nur die Fragen aufgeführt, die anhand der Informationsquellen beantwortet werden konnten. Die Anwendung der Taxonomie ist hierbei in die Abschnitte Infrastruktur, Anwendung und Plattform, Verwaltung und Compliance unterteilt.

6.3.1 Infrastruktur

Physikalische Sicherheit

F: Verwenden alle Rechenzentren des Cloud-Anbieters die gleichen Standards bezüglich der physikalischen Sicherheit?

A: Alle Rechenzentren des Cloud-Anbieters verwenden die gleichen Standards bezüglich der physikalischen Sicherheit.

[25] http://developer.amazonwebservices.com/connect/forumindex.jspa

F: Welche Maßnahmen zur Sicherstellung der physikalischen Sicherheit besitzt das Rechenzentrum, in dem die Daten des Cloud-Konsumenten liegen?
A: Amazon verwendet u.a. folgende Maßnahmen zur Sicherstellung der physikalischen Sicherheit des Rechenzentrums: Sicherheitspersonal für Außenanlagen und den Gebäudezugang, Videoüberwachung, Einbruchsmeldeanlagen und andere elektronische Mittel.
F: Wie ist das Rechenzentrumsgebäude gesichert?
A: Das Rechenzentrumsgebäude ist durch Sicherheitspersonal, Videoüberwachung und Einbruchsmeldeanlagen gesichert.

F: Wie sind die Zugänge zum Gebäude gesichert?
A: Der Zugang zum Gebäude ist durch Zwei-Faktor-Authentifizierung für Mitarbeiter gesichert. Besucher müssen sich identifizieren und werden kontinuierlich von autorisiertem Personal begleitet.

F: Welche Alarmsysteme werden eingesetzt?
A: Es werden Einbruchsmeldeanlangen eingesetzt.

Host

F: Welche Verfahren zur Abschottung der Hosts werden eingesetzt?
A: Der Hypervisor von Xen wird verwendet.

F: Wer hat Zugriff auf die Hosts im Rechenzentrum des Anbieters?
A: Zugriff auf die Hosts im Rechenzentrum haben nur überprüfte Mitarbeiter.

Virtualisierung

F: Welche Virtualisierungstechnologie wird von dem Cloud-Anbieter verwendet?
A: Amazon verwendet die Paravirtualisierung von Xen.

Netzwerk

F: Welche Verfahren und Systeme der Netzsicherheit setzt ein Cloud-Anbieter ein?
A: Amazon setzt z. B. SSL und Firewalls ein.

F: Welche Technologien werden eingesetzt, um Netzangriffe wie z. B. Denial-of-Service-Angriffe, Man-in-the-Middle-Angriffe oder Port-Scanning zu verhindern?
A: Zur Verhinderung der Angriffe werden eigene Maßnahmen, SSL und host-based Firewalls eingesetzt.

F: Wie sind diese Systeme konfiguriert?

A: Die Firewall hat beispielsweise alle Ports standardmäßig geschlossen.

F: Welche Konfigurationen kann bzw. muss der Cloud-Konsument durchführen?

A: Der Cloud-Konsument kann die Ports der Firewall konfigurieren.

6.3.2 Anwendung und Plattform

Datensicherheit

F: Wo werden die Daten gespeichert und wie sind diese von den Daten anderer Kunden getrennt? Werden die Daten auf den Rechnern des Cloud-Anbieters durch diesen verschlüsselt angelegt?

A: Die Daten werden von Amazon nicht verschlüsselt abgelegt, aber der Cloud-Konsument kann sie selber verschlüsseln und dann abspeichern.

F: Wo werden die Daten zusätzlich z. B. bei der Datensicherung und -archivierung oder durch Redundanz des Cloud-Computing-Systems gespeichert?

A: Die Daten werden an mehreren physikalischen Orten in der gleichen Region gespeichert.

F: Werden bei einer Löschung die Daten von allen Instanzen, allen Zwischenspeichern und allen Sicherungskopien gelöscht?

A: Es werden alle Daten und deren Sicherungskopien gelöscht.

F: Welche Verschlüsselungsverfahren bietet der Cloud-Anbieter an? Ist eine Verwendung dieser Verfahren im Vertrag festgeschrieben?

A: Es existieren keine Verschlüsselungsverfahren von Amazon, jedoch kann der Cloud-Konsument die Daten selber verschlüsseln und dann abspeichern.

F: Können Sicherungskopien verschlüsselt werden?

A: Nein, diese sind nur verschlüsselt, wenn die Daten an sich schon verschlüsselt sind.

F: Können Daten nach Löschung wiederhergestellt werden?

A: Die Daten können nach einer Löschung nicht wiederhergestellt werden, da diese komplett gelöscht wurden.

F: Ist es möglich die gespeicherten Daten mit anderen Cloud-Konsumenten zu teilen?

A: Die Daten können sowohl bestimmten Amazon-Nutzern freigegeben werden, als auch allen freigegeben werden.

Anwendungssicherheit

F: Welche Authentifizierungsmechanismen werden angeboten und sind diese Mechanismen angemessen für die Sensitivität der Daten?

A: Amazon bietet eine Multi-Faktor-Authentifizierung an.

Sicherheit als Service

F: Ist eine vollständige Dokumentation der Sicherheitsarchitektur vorhanden?
A: Nein, es ist keine vollständige Dokumentation der Sicherheitsarchitektur vorhanden.

6.3.3 Verwaltung

Phasen der Servicenutzung

F: Sind alle Sicherheitsfunktionen des Anbieters dokumentiert? Sind die Informationen für eine Bewertung ausreichend?
A: Die Informationen sind für eine Bewertung nicht ausreichend, da nicht alle Sicherheitsfunktionen ausreichend dokumentiert sind.

F: Welche Garantien werden in den standardisierten Service-Level-Agreements des Anbieters gegeben? Welche Ausnahmen gibt es?
A: Amazon stellt eine Verfügbarkeit von 99,9% pro Kalendermonat sicher. Ausschlüsse sind bspw. Ausfallzeiten, die nicht berechnet werden, wenn die Probleme außerhalb der Kontrolle von Amazon liegen, aufgrund von Aktivitäten oder Untätigkeiten des Kunden oder eines Dritten und aufgrund von Problemen der Gerätschaften des Kunden und/oder Dritten.

F: Wo und durch welche Systemkomponenten wird die Ausführung eines Cloud-Services überwacht? Ist es möglich Services Dritter zu integrieren?
A: Es können Services Dritter in Amazon integriert werden, wie bspw. VPN-Cubed für EC2.

Identitäts- und Rechteverwaltung

F: Wie sehen die Prozesse zur Rechtevergabe und dem kontrollierten Rechteentzug aus?
A: Für die Rechtevergabe werden Access Control Lists (ACL) verwendet.

F: Existiert eine Programmierschnittstelle für die Bereitstellung und Löschung von Rechten?
A: Über die API können die ACLs angepasst werden.

6.3.4 Compliance

Datenschutz

F: Wie sehen die Datenschutzbestimmungen des Cloud-Anbieters aus? Kann eine Kopie der Richtlinien als Dokument zur Verfügung gestellt werden?
A: Amazon besitzt das TRUSTe-Siegel.

F: Wer hat Zugriff zu den Hosts des Cloud-Computing-Systems?
A: Zugriff auf die Hosts des Cloud-Computing-Systems haben nur Administratoren mit einer betrieblichen Notwendigkeit.

Gesetzliche Rahmenbedingungen

F: Kann der geografische Ort so eingeschränkt werden, dass bestimmte gesetzliche Auflagen erfüllt sind?
A: Die geografischen Orte, an denen die Daten gespeichert werden, können eingeschränkt werden.

Governance

F: Welche Zertifikate sind beim Cloud-Anbieter vorhanden? Was bescheinigen Sie aus Sicherheitssicht?
A: Amazon besitzt das SAS 70 Type II Zertifikat.

F: Werden die Prüfungen der Zertifikate nur intern oder auch extern durchgeführt?
A: Die Prüfungen werden extern durchgeführt.

6.4 Fazit

Eine Bewertung der Sicherheitsimplementierungen von Cloud-Anbietern ist sehr schwierig, da es hierzu seitens der Cloud-Anbieter an Informationen fehlt. Die Verwendung von SSL und HTTPS ist bei vielen Anbietern dokumentiert, jedoch fehlt es an Information zu weiteren Technologien, die verwendet werden. Standardtechnologien für Cloud-Systeme sollten in naher Zukunft definiert und eingeführt werden.

Informationen über die Service-Level-Agreements und die Sicherung der Privatsphäre ist meist bei den Cloud-Anbietern zu finden. Jedoch sind diese zum Teil so ungenau definiert, dass diese ausgelegt werden können, wie sie gebraucht werden. Bei der Bewertung der Sicherung der Privatsphäre muss unterschieden werden zwischen Unternehmen, die die Daten in der Europäischen Union speichern, und Unternehmen, die die Daten in den Vereinigten Staaten speichern, da es hier unterschiedliche Bestimmungen und Regelungen gibt. Abhilfe schafft hier bspw. das Safe-Harbor-Abkommen und das TRUSTe-Programm, jedoch haben sich nicht alle Cloud-Anbieter diesen Datenschutzbestimmungen

unterworfen, wie z. B. CohesiveFT oder RightScale. Auch die Messung von zeit- und mengenbasierten Werten, sowie die Überwachung der vertraglich vereinbarten Dienstgüte ist ein wichtiger Punkt. Die Cloud-Anbieter setzen bereits Messverfahren ein, jedoch sind die gemessenen Werte für den Cloud-Benutzer schwer nachzuvollziehen.

Solange es keine Standards für Cloud-Systeme gibt und diese auch nicht gesetzlich vorgeschrieben sind, sollte jeder Cloud-Anbieter vor der Benutzung eines Services genauestens untersucht werden. Diese Untersuchung sollte die wichtigsten Sicherheitsfelder, die in Kapitel 5 identifiziert wurden, berücksichtigen.

7 Zusammenfassung und Ausblick

Cloud-Computing-Systeme sind in den letzten Jahren ein wichtiges Schlagwort zur Bereitstellung von IT-Services auf entfernten Ressourcen und deren Bezug über ein meist öffentliches Netzwerk. Durch ihre Verbreitung geht eine ständige und schnell wechselnde Veränderung der Serviceangebote einher, die Cloud-Anbieter auf den Markt bringen. Besonders im Fokus stehen dabei die Sicherheitsfunktionen, die von Cloud-Services angeboten werden.

Wie in dem vorangegangenen Kapitel gezeigt, geben die betrachteten Sicherheitsfelder der Cloud-Services ein uneinheitliches Bild ab. Grundlegende Sicherheitsfunktionen bekannter Technologien werden auch in Cloud-Computing-Systemen eingesetzt, um beispielsweise einen Datenkanal zu verschlüsseln. Jedoch unterscheiden sich die Anbieter teilweise deutlich in ihren unterstützten Sicherheitsmerkmalen. Auch der Mangel an einer standardisierten Sicherheitskonfiguration erschwert den Vergleich zwischen verschiedenen Anbietern.

In den folgenden Abschnitten werden die Ergebnisse der Studie kurz zusammengefasst und ein Ausblick auf offene Fragestellungen gegeben, die in Zukunft gelöst werden müssen, damit ein sicheres Cloud-Computing effizient und benutzerfreundlich zu realisieren ist. Abschließend werden die Dienstleistungen des Fraunhofer AISEC im Bereich Cloud-Computing-Sicherheit vorgestellt.

7.1 Ergebnisse der Studie

Die Ergebnisse dieser Studie sind:

- Der Aufbau von Cloud-Computing-Systemen in seine vier Schichten Benutzerschicht, Softwareschicht, Plattformschicht und Infrastrukturschicht und die auf den Schichten agierenden Akteure bilden ein sehr komplexen Rahmen für die IT-Sicherheit. In dieser Studie werden alle wichtigen Schichten und Akteure vorgestellt, die je nach Anwendungsfeld und ausgewähltem Cloud-Service untersucht werden müssen.
- Für Cloud-Computing-Systeme werden zertifizierte Werkzeuge benötigt, die Cloud-Services zu Grunde liegen. Dies erhöht die Portabilität und Interoperabilität einzelner Cloud-Serviceangebote. Hierfür werden Standardisierungsgremien, Referenzimplementierungen und auf Cloud-Computing-Systeme angepasste Entwicklungsumgebungen benötigt.

- Die Cloud-Sicherheitstaxonomie gibt einen übersichtlichen Rahmen der Sicherheitsfelder, die beim Einsatz von Cloud-Services betrachtet werden sollten. Wegen der schnellen Weiterentwicklung der Technologien und der bestehenden Serviceangebote sollte die Anwendung der Cloud-Taxonomie projektbezogen erfolgen und die Gewichtung einzelner Sicherheitsfelder nach der jeweiligen Anforderung angepasst werden.
- Die aktuellen Cloud-Serviceangebote zeigen, dass vor allem im Bereich der Infrastruktur eine Reihe von Sicherheitstechnologien bereits zum Einsatz kommen. In den Bereichen Architektur, Verwaltung und Compliance ist die Unterstützung von Sicherheitstechnologien seitens der Cloud-Anbieter jedoch noch nicht soweit fortgeschritten, um die geforderten Schutzziele zu erreichen. Hier sind weitere, detaillierte Analysen notwendig, welche aktuellen Technologien hier eingesetzt werden können und ob neue Technologien hierfür entwickelt werden müssen. Es zeigt sich ein Trend, bestimmte Sicherheitsfunktionen wie beispielsweise Teile der Identitäts- und Zugangsverwaltung von spezialisierten Anbietern als Service zu beziehen.
- Im Bereich der Verwaltung von Cloud-Services und den dazugehörigen Sicherheitsmechanismen sind Service-Level-Agreements ein wichtiger Bestandteile zur Festschreibung aller Rechte und Pflichten zwischen den Cloud-Benutzern und Cloud-Anbietern. Die bisher angebotenen standardisierten Service-Level-Agreements, die ein Cloud-Benutzer meist nicht frei verhandeln und nur akzeptieren oder ablehnen kann, geben nur minimale Garantien bezüglich der Dienstgüte eines Cloud-Services. Vor allem Sicherheitsgarantien sind nur rudimentär in diesen Service-Level-Agreements vorhanden und müssen ausgebaut werden, um die eingangs vorgestellten Schutzziele zu erreichen. Zusätzlich werden Systeme benötigt, die eine automatisierte Überwachung und Prüfung der vereinbarten Dienstgütekriterien zulassen.
- Aus Sicht der Compliance können Cloud-Services eingesetzt werden. Jedoch bleibt die Verantwortung der Daten meist beim Cloud-Benutzer, so dass dieser genaue Richtlinien definieren sollte, welche Daten wie in einem Cloud-Service abgespeichert und verarbeitet werden dürfen und welche Sicherheitsfunktionen vorhanden sein müssen. Auch aus rechtlicher Sicht sollte im Einzelfall überprüft werden, welche Einschränkungen bei bestimmten Daten gelten und die Verwendung eines Cloud-Services in Betracht gezogen werden kann.
- Die Marktübersicht aus Kapitel 6.1 gibt einen Überblick über ausgewählte Cloud-Serviceangebote, ihre Preise und Funktionen. Des Weiteren wird die Taxonomie des sicheren Cloud-Computing auf diese Cloud-Services angewandt und deren Sicherheitsfunktionen untersucht. Dabei lässt sich festhalten, dass die Informationen zu den implementierten Sicherheitsfunktionen durch die Cloud-Anbieter nur unzureichend dokumentiert sind. Häufig nimmt die Sicherheit bei der Vorstellung ihrer Angebote nur

eine untergeordnete Rolle ein, so dass hier vor der Auswahl und Nutzung eines Cloud-Services beim Anbieter detaillierte Informationen angefordert werden sollten und eventuell ein Proof-of-Concept vor dem eigentlichen Produktiveinsatz eines Cloud-Services realisiert werden sollte.

7.2 Offene Fragestellungen

Offene Fragestellungen beziehen sich vor allem auf die Bereiche Architektur, Verwaltung und Compliance der Taxonomie des sicheren Cloud-Computings, die, wie bereits bei der Vorstellung der Ergebnisse kurz diskutiert, noch einer detaillierteren Analyse unterzogen werden müssen. Viele der bestehenden Cloud-Serviceangebote werden bereits in verschiedenen Bereichen im Normalbetrieb eingesetzt. Es stellt sich jedoch die Frage, nach welchen Kriterien diese ausgewählt und ihre Leistung bewertet werden. Auch ist die Integration in bestehende Systeme noch eine offene Frage, die nicht in ihrer Allgemeinheit gelöst ist.

Des Weiteren sollte eine kontinuierliche Sicherheitsprüfung der Cloud-Services durchgeführt werden, wie es häufig bereits unternehmensintern durchgeführt wird. Hierfür sind Richtlinien und standardisierte Vorgehensweise zu definieren, um dies effizient umsetzen zu können. Dabei können beispielsweise verschiedene Sicherheitsebenen abhängig von den Daten und Prozessen der Cloud-Nutzer festgelegt werden und diese einer separaten Prüfung unterzogen werden.

Mit der fortschreitenden Entwicklung der Sicherheitstechnologien für Cloud-Services wird am Fraunhofer AISEC eine Testumgebung für Cloud-Services aufgebaut werden, in dem verschiedene Sicherheitskonfigurationen sowohl innerhalb des Cloud-Computing-Systems des Fraunhofer AISEC als auch von öffentlichen Cloud-Computing-Systemen durchgeführt werden kann.

7.3 Dienstleistungen des Fraunhofer AISEC

Das Fraunhofer AISEC entwickelt an die Bedürfnisse der Kunden zugeschnittene und direkt einsetzbare Lösungen für alle Branchen, wie den Gesundheitsbereich, Transport, Verkehr und Logistik, die Produktion, aber auch den Handel und für Finanzdienstleister. Neben der kundenorientierten Auftragsforschung bietet das Fraunhofer AISEC Unternehmen und Behörden Beratungsdienste sowie die Entwicklung von Sicherheitskonzepten und die Durchführung von Studien an.

Die Cloud-Computing Aktivitäten des Fraunhofer AISEC, unter der Leitung von Dr. Werner Streitberger, sind gebündelt in der Abteilung „Sichere Services und Qualitätstests“ am neuen Standort in Garching bei München. Diese umfassen die Beratung für den Einsatz von Cloud-Services, die Realisierung von Proof-of-Concepts und das Cloud-Testlabor.

- Konzeptentwicklung und Beratung für den Einsatz von Cloud-Services: In dem Bereich der Konzeptentwicklung und Beratung für den Einsatz von Cloud-Services werden aktuelle Cloud-Serviceangebote hinsichtlich ökonomischer und technischer Kriterien bewertet und den Anforderung entsprechend ausgewählt. Bei Bedarf findet ein Vergleich mit nicht Cloud-basierten Lösungen statt sowie bereits bestehenden Systemen und Services. Dabei liegt der Fokus auf der Sicherheit der Lösung und der Auswahl der Technologien, die im Rahmen von Workshops und Studien präsentiert werden können.
- Realisierung von Proof-of-Concept-Lösung: Neben der Entwicklung von Architekturkonzepten werden auch die Integration in bestehende Prozesse aus Sicherheitssicht betrachtet und in Form von Prototypen implementiert. Des Weiteren erhalten Kunden Unterstützung bei der Inbetriebnahme von Cloud-basierten Lösungen.
- Cloud-Testlabor: Das im Aufbau befindliche Cloud-Testlabor des Fraunhofer AISEC bietet die Prüfung bestehender Cloud-Service-Installationen und die Ausstellung von Sicherheitstestaten an. Dabei kann es auf die langjährige Erfahrung des Sicherheitstestlabors zurückgreifen. Zusätzlich besteht die Möglichkeit, auf eigener Hardware private und hybride Cloud-Konfigurationen zu entwickeln und Sicherheitsüberprüfungen durchzuführen. Im Rahmen der Cloud-Testlaboraktivitäten sind weiterhin die Entwicklung von Demonstratoren und Prototypen möglich, um beispielsweise Compliance und Interoperabilitätstests durchzuführen.

Literaturverzeichnis

[1] *Information technology - open system interconnection - basic reference model: The basic model*, 1994. 48

[2] *Web Services Security*, March 2004. 50

[3] *Xml schema part 0: Primer second edition*, October 2004. 50

[4] *Comprehensive review of security and vulnerability protections for Google Apps*, February 2007. 87, 88

[5] *Amazon Web Services: Overview of Security Processes*, June 2009. 87, 88, 92

[6] *Securing Microsoft's Cloud Infrastructure*, May 2009. 87

[7] Almond, Carl: *A Practical Guide to Cloud Computing Security - What you need to know now about your business and cloud security*. Technischer Bericht, Avanade Inc., August 2009. 44

[8] Amrhein, Dustin, Andrew de Andrade, Joe Armstrong, Ezhil Arasan B, Richard Bruklis, Ken Cameron, Reuven Cohen, Rodrigo Flores, Gaston Fourcade, Thomas Freund, Babak Hosseinzadeh, William Jay Huie, Sam Johnston, Ravi Kulkarni, Anil Kunjunny, Gary Mazzaferro, Andres Monroy-Hernandez, Dirk Nicol, Lisa Noon, Santosh Padhy, Thomas Plunkett, Ling Qian, Balu Ramachandran, Jason Reed, German Retana, Dave Russell, Krishna Sankar, Alfonso Olias Sanz, Wil Sinclair, Erik Sliman, Patrick Stingley, Robert Syputa, Doug Tidwell, Kris Walker, Kurt Williams, John M Willis, Yutaka Sasaki, Eric Windisch und Fred Zappert: *Cloud Computing Use Cases*. Technischer Bericht, Cloud Computing Use Case Discussion Group, July 2009. 12, 14, 28

[9] Armbrust, Michael, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica und Matei Zaharia: *Above the Clouds: A Berkeley View of Cloud Computing*. Technischer Bericht UCB/EECS-2009-28, Electrical Engineering and Computer Sciences, University of California at Berkeley, February 2009. 29, 38, 45, 66

[10] Bardin, Jeff, Jon Callas, Shawn Chaput, Pam Fusco, Francoise Gilbert, Christofer Hoff, , Dennis Hurst, Subra Kumaraswamy, Liam Lynch, Scott Matsumoto, Brian Higgins, Jean Pawluk, George Reese, Jeff Reich, Jeffrey Ritter, Jeff Spivey und John Viega: *Security Guidance for Critical Areas of Focus in*

Cloud Computing. Technischer Bericht, Cloud Security Alliance, April 2009. 41, 44, 54

[11] Bernstein, David, Erik Ludvigson, Krishna Sankar, Steve Diamond und Monique Morrow: *Blueprint for the Intercloud - Protocols and Formats for Cloud Computing Interoperability*. Internet and Web Applications and Services, International Conference on, 0:328–336, 2009. 54

[12] Borthakur, Dhruba: *The Hadoop Distributed File System: Architecture and Design*. The Apache Software Foundation, 2007. 37

[13] Cavoukian, Ann: *Privacy in the Clouds*. Technischer Bericht, Information and Privacy Commissioner of Ontario, 2009. 65

[14] Chakrabarti, Anirban: *Grid Computing Security*. Springer, Berlin, Juni 2007. 45

[15] Comission, European: *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Official Journal of the European Communities, 281:31, 1995. 63

[16] Dean, Jeffrey und Sanjay Ghemawat: *MapReduce: Simplified Data Processing on Large Clusters*. In: *Proceedings of the 6th Symposium on Operating Systems Design and Implementation*, Seiten 137–150, San Francisco, CA, December 2004. `http://www.usenix.org/events/osdi04/tech/dean.html`. 37

[17] Eckert, Claudia: *IT-Sicherheit*. Oldenbourg, 6. Auflage, 2009. 20, 21, 24

[18] Erdogmus, Hakan: *Cloud Computing: Does Nirvana Hide behind the Nebula?* IEEE Software, 26(2):4–6, 2009. 4

[19] Fink, Simon: *Datenschutz zwischen Staat und Markt : die Safe-Harbor-Loesung als Resultat einer strategischen Interaktion zwischen der EU, den USA und der IT-Industrie*. Dissertation, Uni Konstanz, 2003. 64

[20] Gellman, Robert: *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*. Technischer Bericht, World Privacy Forum, February 2009. 21

[21] Greenberg, Albert, James Hamilton, David A. Maltz und Parveen Patel: *The cost of a cloud: research problems in data center networks*. SIGCOMM Comput. Commun. Rev., 39(1):68–73, 2009, ISSN 0146-4833. 44

[22] Grossman, Robert L.: *The Case for Cloud Computing*. IT Professional, 11(2):23–27, 2009, ISSN 1520-9202. 7

[23] Hayes, Brian: *Cloud computing*. Communications of the ACM, 51(7):9–11, 2008, ISSN 0001-0782. 4

[24] Heiser, Jay und Mark Nicolett: *Assessing the Security Risks of Cloud Computing*. Technischer Bericht G00157782, Gartner Research, June 2008. 41

[25] Horrigan, John B.: *Data Memo*. Technischer Bericht, PEW Internet and American Life Project, September 2008. 32

[26] Leavitt, Neal: *Is Cloud Computing Really Ready for Prime Time?* Computer, 42(1):15–20, January 2009. 4, 9

[27] Lin, Geng, David Fu, Jinzy Zhu und Glenn Dasmalchi: *Cloud Computing: IT as a Service*. IT Professional, 11(2):10–13, 2009, ISSN 1520-9202. 4

[28] Mell, Peter und Tim Grance: *Darft NIST Working Definition of Cloud Computing*. Technischer Bericht Version 15, National Institute of Standards and Technology, Information Technology Laboratory, August 2009. 5, 27

[29] Mowbray, Miranda: *The Fog over the Grimpen Mire: Cloud Computing and the Law*. Technischer Bericht HPL-2009-99, HP Laboratories, 2009. 55

[30] Pearson, Siani und Andrew Charlesworth: *Accountability as a Way Forward for Privacy Protection in the Cloud*. Technischer Bericht HPL-2009-178, HP Laboratories, 2009. 26

[31] Pfitzmann, Birgit und Michael Waidner: *Security Protocols*, Band Volume 3364/2005 der Reihe *Lecture Notes in Computer Science*, Kapitel Federated Identity-Management Protocols, Seiten 153–174. Springer Berlin / Heidelberg, 2004. 58

[32] Recordon, David und Drummond Reed: *OpenID 2.0: a platform for user-centric identity management*. In: *DIM '06: Proceedings of the second ACM workshop on Digital identity management*, Seiten 11–16, New York, NY, USA, 2006. ACM, ISBN 1-59593-547-9. 58

[33] Ristenpart, Thomas, Eran Tromer, Hovav Shacham und Stefan Savage: *Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds*. In: *Proceedings of CCS 2009*. ACM Press, November 2009. 52

[34] Smith, Matthew: *Security for Service-Oriented On-Demand Grid Computing*. Dissertation, Fachbereich Mathematik und Informatik, Universität Marburg, 2008. 38

[35] Staten, James, Simon Yates, Frank Gillett, Walid Saleh und Rachel A. Dines: *Is Cloud Computing Ready For The Enterprise?* Technischer Bericht, Forrester Research, Inc., March 2008. 9

[36] Stock, Andrew van der, Jeff Williams und Dave Wichers: *OWASP Top 10: The ten most critical web application security vulnerabilities*. Technischer Bericht, OWASP Foundation, 2007. 51

[37] Streitberger, Werner: *Einsatz von Risikomanagement bei der Steuerung von Grid-Systemen - Eine Analyse von Versicherungen anhand einer simulierten Grid-Ökonomie*. Dissertation, Lehrstuhl für Wirtschaftsinformatik, Fakultät für Rechts- und Wirtschaftswissenschaften, Universität Bayreuth, 2009. 9, 31

[38] Varia, Jinesh: *Cloud Architectures*. Technischer Bericht, Amazon Web Services, 2008. 32

[39] Vishwanath, Kashi Venkatesh, Albert Greenberg und Daniel A. Reed: *Modular data centers: how to design them?* In: *LSAP '09: Proceedings of the 1st ACM workshop on Large-Scale system and application performance*, Seiten 3–10, New York, NY, USA, 2009. ACM, ISBN 978-1-60558-592-5. 44

[40] Wisniewski, Thomas, Tony Nadalin, Scott Cantor, Jeff Hodges und Prateek Mishra: *SAML V2.0 Executive Overview*, April 2005. 58

[41] Zaharia, Matei, Dhruba Borthakur, Joydeep Sen Sarma, Khaled Elmeleegy, Scott Shenker und Ion Stoica: *Job Scheduling for Multi-User MapReduce Clusters*. Technischer Bericht UCB/EECS-2009-55, Electrical Engineering and Computer Sciences, University of California at Berkeley, April 2009. 45

Kontaktdaten

Fraunhofer AISEC
(ehemals Fraunhofer SIT, Institutsteil München)
Parkring 4
D-85748 Garching b. München

Tel.: +49 (0)89-322-9986-0
Fax: +49 (0)89-322-9986-299
http://www.aisec.fraunhofer.de
http://www.cloudsecuritylab.de

Planung und Durchführung der Studie

Dr. Werner Streitberger (Leitung)

Angelika Ruppel
Tel.: +49 (0)89-322-9986-154
angelika.ruppel@aisec.fraunhofer.de

Forschungsbereich "Sichere Services und Qualitätstests"

Mario Hoffmann
Tel.: +49 (0)89 322-9986-177
mario.hoffmann@aisec.fraunhofer.de

Presse und Öffentlichkeitsarbeit

Oliver Küch
Tel.: +49 (0)6151869213
oliver.kuech@sit.fraunhofer.de

Stand der Studie: September 2009