Ist sicheres Cloud Computing möglich?

Bezüglich der Nutzung cloudbasierter Dienste zur Kostenreduktion und Verbesserung der Verfügbarkeit haben viele IT-Verantwortliche Sicherheitsbedenken. Dabei erlauben bestimmte technische und organisatorische Massnahmen eine hinreichend sichere Nutzung von Cloud-Diensten.

Hannes Lubich | hannes.lubich@fhnw.ch

Die Auslagerung der Erbringung von ICT-Diensten ist im Zuge der Globalisierung und des stetigen Kostensenkungs-, Optimierungs- und Innovationsdrucks weit fortgeschritten. Während bei bisherigen Outsourcing-Modellen jedoch eher die Übergabe oder die Migration bereits vorhandener Entwicklungs-, Betriebs- und Wartungsleistungen inklusive Personal und ICT-Infrastrukturen an externe Diensterbringer im Zentrum des Servicemodells standen, entsteht durch das Angebot von cloudbasierten Dienstleistungen ein neues Auslagerungsmodell. Dieses neue Modell basiert auf der Nutzung einer technologisch wesentlich stärker standardisierten, dafür jedoch weitgehend dynamischen, orts- und umgebungsunabhängigen Infrastruktur und Diensterbringung.

In diesem Auslagerungsszenario entstehen zwangsläufig neue Fragen nach der Definition, Erbringung und Überprüfbarkeit von Risikomodellen und entsprechenden Sicherheitsleistungen. Das wesentliche Ziel der Risikoanalyse und -bewirtschaftung ist es, das bislang erreichte Schutzniveau auch in einem Cloud-Dienstmodell, das die Grenzen der klassischen Informationssicherheit bezüglich der Kontrolle über die Sicherheitsanforderungen und deren Überwachung und Überprüfung deutlich überschreitet, beibehalten zu können.

Angebot und Nutzung cloudbasierter Dienste

Clouds sind definiert als meist parallele und geografisch breit verteilte Systeme, die aus einer Ansammlung miteinander vernetzter und oft virtualisierter Computersysteme bestehen. Diese Systeme werden dynamisch verwaltet und zugeteilt, erscheinen den Benutzern gegenüber jedoch als einheitlicher Service, dessen Leistungsfähigkeit dynamisch den Benutzeranforderungen angepasst werden kann. Das Nutzungsmodell basiert auf zuvor formell ausgehandelten Service Level Agreements gemäss der vorhandenen Serviceklassen und der zugehörigen, meist nutzungsabhängigen Tarifierung und Abrechnung.

Cloudbasierten Diensten liegt also die Annahme zugrunde, dass die ICT-Infrastruktur – Netzwerke und deren Komponenten, Server und deren Basisdienste (Speicher, Rechenleistung) –, aber ggf. auch standardisierte Dienstleistungen wie E-Mail, webbasierte Anwendungen inklusive der nötigen Datenbewirtschaftung usw. innerhalb einer für den Kunden nicht differenzierbaren „Wolke“ gemäss einem definierten Service Level angeboten werden. Der Wolke hinzugefügt werden dann meist weitere Basisleistungen wie Benutzeridentifikation, -authentisierung und -autorisierung durch geeignete Zugriffsschutzmodelle, einfache Sicherheitsmechanismen wie Firewalls und „Intrusion Detection“-Systeme sowie die Betriebsüberwachung und Alarmierung bzw. Eskalation im Fall erkannter Störungen.

Das Geschäftsmodell eines solchen Cloud-Angebots basiert also einerseits auf einer sehr starken „economy of scale“ mit möglichst vielen Nutzern, welche die Aufbau-, Betriebs-, Erweiterungs- und Erneuerungskosten der Cloud finanzieren, und andererseits auf der starken Standardisierung der Dienste in der Cloud, um die Komplexität der Cloud zu beschränken und damit entsprechende Risiken zu minimieren (im Gegensatz zur Übernahme von „Legacy“-Systemen in vielen klassischen Outsourcing-Ansätzen). Diese Standardisierung erstreckt sich dabei von den applikatorisch verfügbaren Umgebungen (meist webbasierte Services) über die Datenhaltung in standardisierten Datenbankumgebungen bis hin zu standardisierten (ggf. virtualisierten) Servern mit vorkonfigurierten Betriebssystemen. Eine Migration „in die Cloud“ erfordert demzufolge vom Dienstnutzer das vorgängige „Aufräumen“ der eigenen Infrastrukturen und Anwendungen, um „cloudkonform“ zu werden.

Cloud-Dienste werden gemäss einer Hierarchie des Dienstangebots klassifiziert:

1. *Infrastructure as a Service (IaaS):* Die Infrastrukturanbieter stellen eine grosse Menge von ICT-Ressourcen zur Verfügung (Sekundärspeicher, Rechenleistung usw.). Durch Virtualisierung können diese Ressourcen dynamisch den Nutzern zugeordnet werden und bieten dadurch die Fähigkeit, zeitnah (und ggf.

kostengünstig, je nach Abrechnung und Tarifierungsmodell, z. B. Sockelbeitrag plus „Pay per Use“) die jeweiligen Benutzerbedürfnisse abzudecken. Gleichzeitig erlaubt dies dem Anbieter auch – analog zur häufigen Praxis von Fluggesellschaften – ein Überbuchen der verfügbaren Ressourcen bzw. die Befriedigung von Benutzerbedürfnissen, deren Summe die Kapazität der Ressourcen eigentlich übersteigt. Jedoch muss der Benutzer „seinen“ Software-Stack selbst erstellen, ausrollen, verwalten und betreiben. Ein typisches Beispiel ist der EC2 Cloud Service von Amazon [1], der die vorhandene Kapazität bzw. Überkapazität der Amazon-eigenen ICT-Infrastruktur als mietbaren Service im offenen Markt platziert.

2. *Platform as a Service (PaaS):* Anstelle einer virtualisierten Infrastruktur wird auch die Softwareplattform (Betriebssystem und zugehörige Middleware-Komponenten) als Service zur Verfügung gestellt. Die darunter liegende optimale Zuteilung der Hardware und sonstigen Betriebsmittel geschieht dabei „unsichtbar“ für den Benutzer. Ein typisches Beispiel für diese Dienstklasse ist die „Google App Engine“ [2], die es Anwendern erlaubt, eigene Webanwendungen in der Infrastruktur von Google auszuführen.
3. *Software as a Service (SaaS):* In diesem Szenario wird auch die Anwendungssoftware als verwalteter und abrechenbarer Dienst zur Verfügung gestellt. Die darunter liegende Plattform und technische Infrastruktur und deren Zuteilung bleiben dabei weiterhin vor dem Benutzer verborgen. Typische Beispiele für diese Serviceklasse sind die „Oracle Platform for SaaS“ [3] oder „salesforce.com“ [4] zur Auslagerung von CRM-orientierten Anwendungen. Einige dieser Plattformen erlauben durch die Bereitstellung entsprechender Entwicklungsumgebungen zusätzlich die Erstellung und Nutzung neuer Softwarekomponenten durch den Anwender in der Cloud.

Eine ähnliche Taxonomie der Yankee Group [5] stellt diesen drei Cloud-Modellen noch ein weiteres Modell voran, in dem einfache Cloud-Services über das Internet bezogen werden (siehe Abb. 1).

Erste Cloud-Ansätze entstanden typischerweise im Umfeld von sehr grossen Technologienutzern und Serviceanbietern, die an einer Zusatzfinanzierung ihrer internen Über- oder Spitzenlastkapazität durch das Angebot einfacher cloudbasierter Dienste (typischerweise Ablage von Dateien, E-Mails oder ähnliche Dienste) interessiert waren. Durch den Sprung zu „Software as a Service“ und die Bereitstellung meist webbasierter Entwicklungs- und Betriebsumgebungen in der Cloud können nun jedoch Geschäftsmodelle für das Angebot komplexer Applikationen entwickelt und umgesetzt werden, die den kommerziellen Aufbau und Betrieb von Cloud-Diensten ohne Querfinanzierung erlauben. Der Marktforscher IDC schätzt, dass Cloud-Services ein stark wachsendes Marktpotenzial haben, da Firmen durch die Nutzung von Clouds ihre Infrastruktur- und Betriebskosten sowie die Kosten für die Sicherung, Pflege, Modernisierung, Leistungssteigerung usw. einsparen bzw. von einem Fixkostenmodell auf ein „Pay per Use“-Modell umstellen können. IDC erwartet weltweit eine Steigerung des Umsatzes von ca. 121.5 Mrd. US-Dollar im Jahr 20010 auf etwa 72 Mrd. US-Dollar im Jahr 2015 [6]. Zudem wird angenommen,

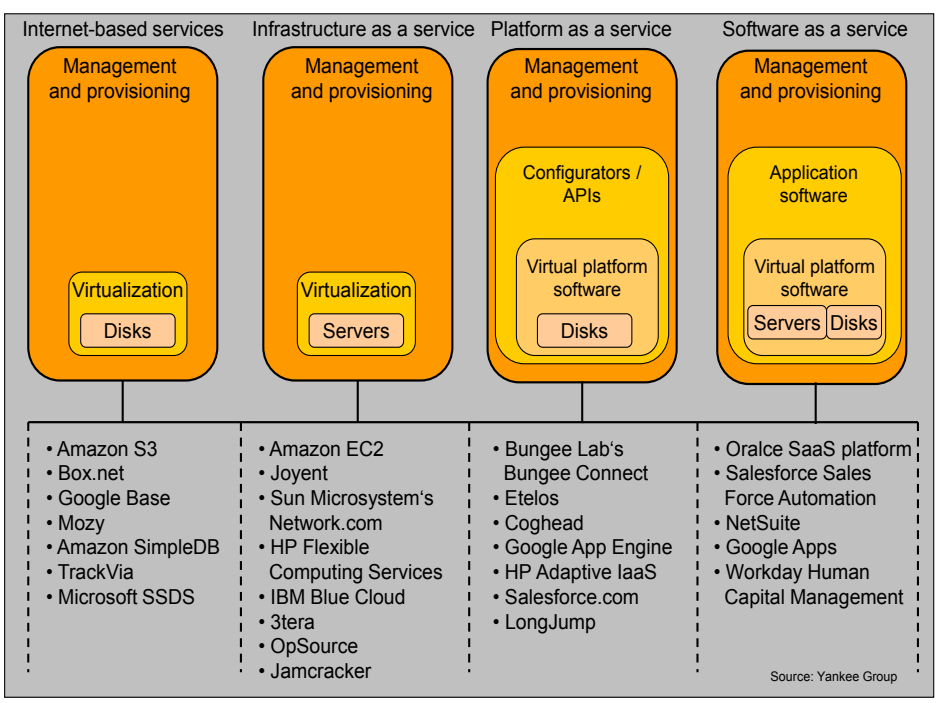

Abb. 1: Cloud-Taxonomie der Yankee Group

dass im Jahr 2012 von den Kosten für die Informatik eines Unternehmens etwa 25% auf die Nutzung von Cloud-Services entfallen werden [7].

Wesentliche Treiber für das Angebot und die Nutzung von Cloud-Diensten sind also die Reduktion von Komplexität, Fixkosten und Infrastrukturrisiken für den Kunden bzw. die Nutzung von Skaleneffekten homogenisierter Infrastrukturen und Dienste für den Anbieter. Mögliche bremsende Faktoren für den Transfer von ICT-Systemen und -Services in die Cloud sind:

- die Abhängigkeit von Fremdanbietern, deren Besitzverhältnisse und finanziellen Hintergründe oft nur ungenau überprüfbar sind oder sich stark verändern können;
- die mangelnde Kontrolle über den Ort der Diensterbringung (z. B. in Ländern mit nicht hinreichendem Datenschutz oder pauschalen Regelungen bezüglich des staatlichen Zugriffs auf Kundendaten);
- die Kontrolle der Einhaltung von Dienst- und Qualitätsgarantien;
- die Aufrechterhaltung der IT-Sicherheit und der nötigen Rechtssicherheit (z. B. bezüglich der Einhaltung des Datenschutzes oder des Geschäftsgeheimnisses);
- die Verfügbarkeit, Qualität und Bezahlbarkeit der nötigen Kapazität;
- die ggf. mangelnde Transparenz der Leistungserbringung und kundenspezifischen Dienstabrechnung.

Auswirkungen auf Informationssicherheit und Risikomanagement

Viele etablierte Elemente der Informationssicherheit und des ICT-Risikomanagements bei der Auslagerung von Diensten basieren auf der Annahme, dass die relevanten Betriebs- und Kontrollparameter bzw. deren Governance in der Kontrolle des Auftraggebers verbleiben, während die Umsetzung auf dem Einsatz von Fremdleistungen basieren kann.

War die Einhaltung der Vorgaben für Informationssicherheit und Datenschutz bereits in traditionellen Auslagerungsmodellen komplex und mit substanziellem Aufwand verbunden, so bietet die Kontrolle der Einhaltung entsprechender Vorgaben in cloudbasierten Modellen zusätzliche Schwierigkeiten. Diese Aspekte müssen zwingend in die Gesamtrisikobetrachtung bei der Nutzung von Cloud-Diensten prominent einfliessen.

Im Folgenden werden typische Problemfelder exemplarisch und ohne Anspruch auf fallspezifische Vollständigkeit diskutiert.

1. Es gibt keine Kontrolle über den Ort der Diensterbringung (inkl. Transitorte und Netze) und deren Sicherheitsdispositive (von physischem Schutz und Zugangskontrollen bis hin zu den jeweils geltenden betrieblichen IT-Sicherheitskonzepten, Zertifikaten etc.). Eine eigentliche „Due Diligence“ pro betrieblichem Standort und Land ist in einer breit verteilten, dynamischen Cloud also nicht mehr möglich.
2. Die Frage der dynamisch grenzüberschreitenden Funktionalität gegenüber einer immer noch stark nationalen oder regionalen Gesetzgebung hat direkte Konsequenzen auf die Selektion eines Cloud-Angebots. In der Schweiz sind z. B. im Gegensatz zu anderen Ländern nicht nur Personen-, sondern auch Unternehmensdaten geschützt. Auch E-Mails sind in diesem Sinne Personendaten, die dem Datenschutz unterstehen – eine Bekanntgabe ins Ausland kann nur dann erfolgen, wenn am Speicher- oder Aufbewahrungsort ein äquivalentes Datenschutzrecht gilt. Bei einer jederzeit ortsveränderlichen Diensterbringung ist diese Überprüfung aufwendig, wenn nicht unmöglich.
3. Die Kontrolle über das in einen Cloud-Service eingebrachte geistige Eigentum (z. B. Kundendaten, Herstellungs- oder Berechnungsverfahren etc.) erfordert in gemeinsam von mehreren Kunden genutzten Plattformen und Applikationen besondere Aufmerksamkeit. Insbesondere müssen die Betriebsprozesse in der Cloud gewährleisten, dass keine Verwechslung, keine Durchmischung und kein ungeplanter Abgleich von Daten (z. B. in nicht strikt mandantenfähig ausgelegten Applikationen) erfolgt.
4. Eine auf allgemeine Nutzung ausgelegte Cloud wird in aller Regel nur allgemein definierte und implementierte Sicherheitseinrichtungen aufweisen – die zugehörigen Service Agreements sind im gleichen Sinne stark standardisiert und decken die Bereiche Informationssicherheit, Risikomanagement, Betrieb im Krisenfall etc. nur in sehr generischer Form ab. Dementsprechend entstehen für spezifische zusätzliche Sicherheitsanforderungen hohe Zusatzkosten, die in der Regel nicht auf alle anderen Nutzer der Cloud umgelegt werden können, sofern der Cloud-Betreiber überhaupt zur Implementation zusätzlicher, kundenspezifischer Sicherheitsmerkmale bereit ist.
5. Die Überwachung des Zustands der Informationssicherheit und der operationellen Risiken in kundeneigenen Security-Information-Management-Umgebungen ist meist nicht Bestandteil der Dienstleistung. Entsprechende Reportingschnittstellen müssen daher spezifisch definiert und bewirtschaftet werden, sofern die der Cloud unterliegende Infrastruktur diese Daten mandantenfähig und kundenspezifisch trennen und aufbereiten bzw. liefern kann. Das bisher eher feinkörnige Sicherheits- und Risikomanagement, basierend auf kundenspezifischen „Key Performance Indicators“, steht in dieser Form als Führungs-

und Entscheidungsunterstützungswerkzeug nicht mehr zur Verfügung.

6. Die Abhängigkeitskette bezüglich der End-zu-End-Verfügbarkeit wird nicht nur länger, sondern für den Kunden durch die starke Dynamik der Diensterbringung (Virtualisierung, Ortsveränderlichkeit usw.) auch intransparenter. Dies muss insbesondere in der Szenarienplanung für die Betriebsweiterführung im Not- und Krisenfall berücksichtigt werden. Cloud-Services sind jedoch durch ihre Ausrichtung auf ein standardisiertes Dienstangebot und standardisierte Technologiekomponenten weniger komplex als die klassischen Outsourcing-Modelle inklusive des Betriebs bestehender „Legacy"-Umgebungen. Daher ist es denkbar, dass sich diese beiden Effekte bezüglich Gesamtrisiko und Aufwand beim Kunden gegenseitig neutralisieren.
7. Grosse kommerzielle Cloud-Services sind ein Primärziel für Angreifer, wobei die Palette der Motivationen von der Erpressung des Serviceanbieters durch „Denial of Service"-Angriffe bis hin zum „Mitlesen" und zum Datendiebstahl, ggf. schon in der Grauzone der Nachrichtendienste (Terrorismusbekämpfung, Geldwäscherei, Stärkung des eigenen Wirtschaftsstandorts etc.) oder der informationellen Kriegsführung reicht. Ein zusätzliches Problem entsteht durch den grossen Kreis der Betroffenen: In einer zwischen allen Kunden gemeinsam genutzten Infrastruktur und Applikationslandschaft leiden alle Kunden unter einem Angriff, auch wenn nur ein einzelner Kunde angegriffen werden sollte.

Katalog angemessener Sicherheitsmassnahmen

Im Spannungsfeld zwischen Kosten- und Effizienzdruck einerseits und den dargelegten Sicherheitsüberlegungen andererseits kann die Frage nicht lauten, ob man Cloud-Services verwendet oder nicht, sondern unter welchen Bedingungen und mit welchen flankierenden Massnahmen eine Nutzung von Cloud-Diensten möglich und ökonomisch sinnvoll ist.

Ein möglicher Startpunkt für diese Abklärung aus Sicht der IT kann die „Security Guidance for Critical Areas of Cloud Computing" der „Cloud Security Alliance" [8] sein, die seit November 2011 in der aktualisierten Fassung 3.0 vorliegt. Dieses Dokument spezifiziert die Sicherheitsanforderungen an Cloud-Computing-Umgebungen anhand von 13 Arbeitsbereichen, aufgeteilt nach aufsichtsbezogenen (siehe Tabelle 1) und eher betrieblich orientierten Themen (siehe Tabelle 2).

Für jeden dieser Arbeitsbereiche werden in der „Security Guidance for Critical Areas of Cloud Computing" generische Empfehlungen bezüglich Umsetzung in cloudbasierten Umgebungen gemacht, welche die Grundlage für die Spezifikation von Kundenanforderungen bezüglich Informationssicherheit bilden können.

Eine breit abgestützte Abbildung auf die bislang dominierenden Standards und „Best Practices" für Informationssicherheit (insbesondere ISO2700x und CoBIT) steht jedoch noch aus, ebenso fehlen konkrete Nutzungs- und Umsetzungserfahrungen aus dem Betrieb, sodass potenzielle Kunden gemäss ihrem jeweiligen Risikoprofil selbst zu beurteilen und zu entscheiden haben, ob sie bezüglich cloudbasierter Dienste als „Early Adaptor" oder doch eher als „Late Follower" agieren wollen.

Zusammenfassung

Die zuvor aufgeführte Liste von Sicherheits- und Risikomanagementaspekten kann zu dem Schluss führen, dass die Nutzung cloudbasierter Angebote generell nicht angezeigt ist. Dieser Haltung stehen jedoch die möglichen Einsparungen und Skaleneffekte gegenüber, die in einer Risiko-Gewinn- und Verlustrechnung zu berücksichtigen

Aufsichtsthema	Inhalt
Governance and Enterprise Risk Management	Fähigkeit eines Unternehmens, das Risiko durch die Nutzung von cloudbasierten Diensten zu beurteilen und zu steuern bzw. die Risiken und die nötigen Gegenmassnahmen in das unternehmensweite Risikomanagement einzubetten.
Legal Issues, Contracts and Electronic Discovery	Feststellung der rechtlichen und regulatorischen Rahmenbedingungen für die Nutzung cloudbasierter Dienste. Diesem Punkt kommt insbesondere bei der Nutzung grenz- und rechtsüberschreitender Angebote eine besondere Bedeutung zu (allgemeiner Datenschutz, Offenlegung von Daten gegenüber Behörden, Behandlung besonders schützenswerter Daten, Melde- und Berichtspflichten etc., aber auch Überprüfung und Management der Nutzungsbedingungen der Cloud).
Compliance and Audit Management	Regelmässige Überprüfung des ordnungsgemässen Betriebs der cloudbasierten Dienste und Aufbewahrung bzw. Rapportierung ausreichender Beweismittel aus der Überprüfung in Koordination mit den entsprechenden internen und externen Aufsichtsstellen; zudem Festlegung nötiger Korrekturmassnahmen und Überwachung der Umsetzung.
Information Management and Data Security	Management von Daten in der Cloud, Festlegung von Schutzbedarf, Rollen, Rechten und Verantwortlichkeit bezüglich dieser Daten (Data Ownership) und Umsetzung von Kontrollen zum Schutz der Daten vor nicht zulässiger Weitergabe, Nutzung, Verfälschung oder Löschung.
Interoperability and Portability	Aufrechterhaltung der Fähigkeit, Daten und Dienste von einem Dienstanbieter zu einem anderen zu verlagern (Interoperabilität) und Daten/Dienste bei Bedarf wieder in die eigene IT zu integrieren.

Tabelle 1: Die aufsichtsbezogenen Themen der „Security Guidance for Critical Areas of Cloud Computing"

Betriebliches Thema	Inhalt
Traditional Security, Business Continuity and Disaster Recovery	Beurteilung und Management des Einflusses der Nutzung cloudbasierter Dienste auf die vorhandenen Prozesse für Security Management und die Geschäftsweiterführung im Krisenfall. In diesem Bereich ist insbesondere zu beachten, dass die in der Cloud genutzten Dienste und Infrastrukturen nicht mehr dem eigenen Zugriff und der eigenen Kontrolle unterstehen. Die entsprechenden Prozesse des Dienstnehmers müssen also sehr genau spezifizierte Schnittstellen zu den entsprechenden Diensten und Prozessen des Dienstanbieters aufweisen und bewirtschaften.
Data Center Operations	Beurteilung der Architektur des Rechenzentrums des Dienstanbieters sowie der entsprechenden betrieblichen Prozesse. Dieser Aspekt ist insbesondere bei der Auswahl von Dienstanbietern, bei der Umgestaltung des Betriebs durch den Anbieter während der Vertragslaufzeit oder bei beobachteten betrieblichen Mängeln von Interesse.
Incident Response, Notification and Remediation	Angemessen zeitnahe und vollständige Erkennung von Störungen im Betrieb der cloudbasierten Dienste, stufengerechte Information der Dienstnutzer und rasche Störungsbehebung. Dieser Aspekt umfasst technische Schnittstellen (z. B. zwischen Helpdesks oder Trouble-Ticket-Systemen) sowie organisatorische Anpassungen (Informations- und Eskalationspfade, gemeinschaftliches Problemmanagement, nachgelagerte Ursachenanalyse, Forensik usw.).
Application Security	Sicherungsmassnahmen für Anwendungssoftware, die in einer Cloud entwickelt und/oder betrieben wird. Dieser Aspekt beinhaltet Fragen, ob eine Anwendung für die Cloud-Nutzung umgestaltet oder in die Cloud migriert werden kann und welche Plattform (SaaS, PaaS oder IaaS) dafür geeignet ist.
Encryption and Key Management	Identifikation und Gestaltung ausreichend starker Chiffrierung und ausreichend skalierbarer Schlüsselverwaltung in cloudbasierten Umgebungen mit verteilter betrieblicher Verantwortung. In diesem Bereich müssen auch Themen wie die Einbettung in oder bewusste Trennung von Verschlüsselungsinfrastrukturen zwischen internem Betrieb und der Cloud-Umgebung sowie die treuhänderische Hinterlegung von Schlüsselmaterial zwischen den Vertragspartnern diskutiert und bearbeitet werden.
Identity, Entitlement, and Access Management	Management von Identitäten, Rechten und Rollen, basierend auf Benutzerverwaltungs- und Verzeichnisdiensten, die entweder spezifisch für die Cloud-Umgebung aufgebaut und betrieben oder mittels geeigneter Schnittstellen an das interne Identitätsmanagement angeschlossen und durch entsprechende Bearbeitungsprozesse betrieben werden. In diesen Bereich fallen zudem Anlage und Auswertung von Protokollinformationen bezüglich Vergabe, Nutzung und Modifikation von Zugriffsrechten, um Missbräuche oder Fehlkonfigurationen rasch erkennen und beseitigen zu können.
Virtualization	Beurteilung und Kontrolle der Nutzung von hard- oder softwarebasierten Virtualisierungstechnologien in der Cloud-Umgebung bezüglich Aufrechterhaltung der Sicherheitsvorgaben (z. B. bei unkontrollierter Redundanz von Datenhaltungen oder paralleler Nutzung von Infrastrukturen durch unterschiedliche Kunden).
Security as a Service	Angebot von Sicherheitsüberprüfungen, Fallbehandlung und/oder Betriebsüberwachung sicherheitsrelevanter Einrichtungen durch spezialisierte Drittanbieter (ggf. mit der Delegation von Handlungsrechten im Schadenfall).

Tabelle 2: Die betrieblichen Themen der „Security Guidance for Critical Areas of Cloud Computing“

sind. Bei sorgfältiger Vorbereitung und Durchführung entsprechender Migrationsprojekte „in die Cloud“ und bei angemessener Berücksichtigung der „Security Guidance for Critical Areas of Cloud Computing“ ist ein ausreichend sicherer Betrieb basierend auf Cloud-Angeboten jedoch durchaus realistisch.

Neben den technischen Abklärungen und Transitionen müssen insbesondere die rechtlichen und regulatorischen Rahmenbedingungen und die korrekte Ausübung von Governance- und Compliance-Vorgaben bei cloudbasierten Services sehr sorgfältig und unter Einbeziehung aller betroffenen Instanzen vor einem Servicebezug abgeklärt werden. Zudem sind die Überprüfungen des gewählten Dienstanbieters im Betrieb zyklisch zu wiederholen und mit den vereinbarten Dienstgüteparametern und vertraglichen Vereinbarungen zu vergleichen, um eine „schleichende“ Dienstgefährdung zu vermeiden.

Referenzen

[1] Amazon Elastic Compute Cloud (Amazon EC2): http://aws.amazon.com/de/ec2/

[2] Google App Engine: https://developers.google.com/appengine/

[3] Oracle SaaS Platform: Building On-Demand Applications – An Oracle White Paper, Sep 2008: http://www.oracle.com/us/technologies/cloud/026989.pdf

[4] http://www.salesforce.com

[5] Yankee Group Cloud Comuting Survey, July 2011: http://waimingmok.files.wordpress.com/2009/01/yankeegroupcloudservices.jpg

[6] IDC Cloud Research: http://www.idc.com/prodserv/idc_cloud.jsp

[7] Cap Gemini Studie IT-Trends 2012: http://www.ch.capgemini.com/insights/publikationen/it-trends-2012/

[8] Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud Computing Version 3.0: https://cloudsecurityalliance.org/research/security-guidance/