Risiko-Betrachtungen in Cloud-basierten Diensten

In diesem Beitrag:

- Die Klassifizierung von Cloud-Diensten
- Typische Problemfelder bei der Auslagerung von IT-Sicherheit in die Cloud
- Exakte Abklärung von Governance- und Compliance-Vorgaben
- Die «Security Guidance for Critical Areas of Focus in Cloud Computing» der Cloud Security Alliance

Dunkle Wolken über der IT-Sicherheit

Der Vormasch von Cloud-basierten Dienstleistungen bringt auch neue Fragestellungen hinsichtlich Definition, Erbringung und Überprüfbarkeit von Risiko- und Sicherheitsleistungen mit sich, um das bislang erreichte Schutzniveau auch in einem Dienstmodell beibehalten zu können.

Infos zum Autor

Prof. Dr. Hannes P. Lubich

Institut für Mobile und Verteilte Systeme
Hochschule für Technik der Fachhochschule Nordwestschweiz, Windisch

Die Auslagerung von ICT-Diensten ist im Zuge der Globalisierung und des stetigen Optimierungs- und Innovationsdrucks weit fortgeschritten. Während jedoch bei bisherigen Outsourcing-Modellen eher die Übergabe oder die Migration von bereits vorhandenen Entwicklungs-, Betriebs- und Wartungsleistungen inklusive Personal und ICT-Infrastrukturen an externe Diensterbringer im Zentrum des Service-Modells stand, entsteht durch das Angebot von Cloud-basierten Dienstleistungen ein neues Auslagerungsmodell, welches auf der Nutzung einer technologisch wesentlich stärker standardisierten, dafür jedoch weitgehend dynamischen, orts- und umgebungsunabhängigen Infrastruktur und Diensterbringung basiert. In diesem Szenario entstehen neue Fragestellungen nach der Definition,

Erbringung und Überprüfbarkeit von Risiko- und Sicherheitsleistungen, um das bislang erreichte Schutzniveau auch in einem Dienstmodell beibehalten zu können, welches die Grenzen der klassischen Informationssicherheit bezüglich Kontrolle über die Sicherheitsanforderungen und deren Überwachung und Überprüfung deutlich überschreitet.

Clouds und Cloud-basierte Dienste

Clouds sind definiert als meist massiv parallele und verteilte Systeme, welche aus einer Ansammlung miteinander vernetzter und oft virtualisierter Computer bestehen. Diese Computer werden dynamisch verwaltet und zugeteilt, erscheinen den Benutzern gegenüber jedoch als vereinheitlichter Service. Die Nutzung basiert auf zuvor ausgehandelten Service Level Agreements und der zugehörigen, meist nutzungsabhängigen Tarifierung und Abrechnung. Cloudbasierte Dienste basieren auf der grundsätzlichen Annahme, dass die ICT-Infrastruktur – Netzwerke und deren Komponenten, Server und deren Basisdienste (Speicher, Rechenleistung) – aber gegebenenfalls auch standardisierte Dienstleistungen wie E-Mail, Web-basierte Anwendungen inklusive der nötigen Datenbewirtschaftung usw. innerhalb einer für den Kunden nicht differenzierbaren «Wolke» gemäss einem definierten Service Level angeboten werden.
Das Geschäftsmodell eines solchen Cloud-Angebots basiert also einerseits auf einer sehr starken «economy of scale» mit möglichst vielen Nutzern, welche die Betriebs-, Ausbau- 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).

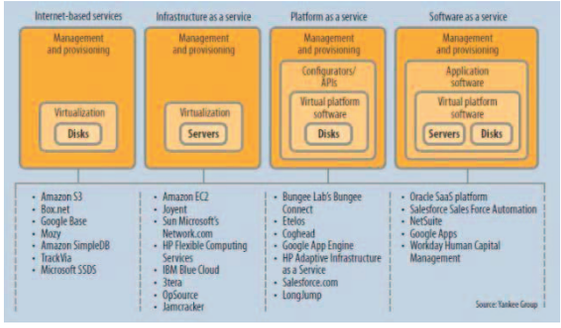
Cloud-Dienste werden heute gemäss einer Hierarchie des Dienstangebots klassifiziert:

1. Infrastructure as a Service (IaaS): Infrastruktur-Anbieter 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 auch kostengünstig, je nach Abrechnung und Tarifierungsmodell, z.B. Sockelbeitrag plus «pay per use») die jeweiligen Benutzerbedürfnisse abdecken zu können – gleichzeitig erlaubt dies dem Anbieter auch ein «Overbooking» 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 dafür ist Amazon EC2.

2. Platform as a Service (PaaS): Anstelle einer virtualisierten Infrastruktur wird auch die Software-Plattform (Betriebssystem und zugehörige Middleware-Komponenten) als Service zur Verfügung gestellt. Die darunterliegende optimale Zuteilung der Hardware und sonstigen Betriebsmittel geschieht dabei für den Benutzer transparent. Typisches Beispiel: Google Apps Engine, Salesforce.com.

3. Software as a Service (SaaS): In diesem Szenario wird auch die Anwendungssoftware als verwalteter und abrechenbarer Dienst zur Verfügung gestellt. Die darunterliegende Plattform und technische Infrastruktur und deren Zuteilung bleiben vor dem Benutzer verborgen.
   Typisches Beispiel: Oracle SaaS Platform.

Eine ähnliche Taxonomie der Yankee Group stellt diesen drei Cloud-Modellen noch ein weiteres Modell voran, in dem einfache Cloud Services über das Internet bezogen werden.



Erste Cloud-Ansätze entstanden typischerweise im Umfeld von sehr grossen Technologie-Nutzern und Service-Anbietern, welche an einer Zusatzfinanzierung ihrer internen Über- oder «Peak»-Kapazität durch das Angebot einfacher Cloud-basierter Dienste (typischerweise Ablage von Dateien, E-Mail oder ähnliche Dienste) interessiert waren. Durch den Sprung zu «Software as a Service» und die Bereitstellung meist Web-basierter Entwicklungs- und Betriebsumgebungen in der Cloud können jedoch nun Geschäftsmodelle für das Angebot von komplexen Applikationen entwickelt und umgesetzt werden, welche 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, Moder-

nisierung, Leistungssteigerung usw. einsparen bzw. von einem Fixkosten-Modell auf ein «pay per use»-Modell umstellen können. IDC erwartet weltweit eine Steigerung von ca. 16 Mrd. USD im Jahr 2008 auf etwa 42 Mrd. USD im Jahr 2012. Zudem wird angenommen, dass im Jahr 2012 innerhalb der Kosten für die Informatik einer Unternehmung etwa 25 Prozent auf die Nutzung von Cloud Services entfallen werden.
Treiber für Clouds sind also die Reduktion von Komplexität und Fixkosten für den Kunden, mögliche bremsende Faktoren sind die Kontrolle/Abhängigkeit von Fremdanbietern (ggf. im Ausland oder mit variablem Ort der Diensterbringung), die Kontrolle der Einhaltung von Dienst- und Qualitätsgarantien, die Aufrechterhaltung der IT-Sicherheit und des Datenschutzes, die Verfügbarkeit, Qualität und Bezahlbarkeit der nötigen Kapazität sowie die mangelnde Transparenz der Leistungserbringung und kundenspezifischen Dienstabrechnung.

Implikationen für Informationssicherheit und Risiko-Management

Viele etablierte Elemente der Informationssicherheit und des ICT-Risiko-Managements bei der Auslagerung von Diensten basieren auf der Annahme, dass die relevanten Betriebs- und Kontrollparameter bzw. deren Governance unter der Kontrolle des Auftraggebers verbleiben, während die Umsetzung durchaus auf dem Einsatz von Fremdleistungen basieren kann. War die Einhaltung der Vorgaben für Informationssicherheit und Datenschutz bereits in traditionellen Auslagerungsmodellen komplex und mit substantiellem Aufwand verbunden, so bietet die Kontrolle der Einhaltung entsprechender Vorgaben in Cloud-basierten Modellen zusätzliche Schwierigkeiten, welche in die Gesamt-Risikobetrachtung bei der Nutzung von Cloud-Diensten prominent einfliessen müssen. Im Folgenden werden typische Problemfelder exemplarisch und ohne Anspruch auf Vollständigkeit diskutiert.

1. Es gibt keine Kontrolle über den Ort der Diensterbringung (inkl. Transit-Orte 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 Personendaten, 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 aufwändig, wenn nicht unmöglich.

3. Die Kontrolle über das in einen Cloud Service eingebrachte geistige Eigentum (z.B. Kundendaten, Herstellungs- oder Berechnungsverfahren etc.) benötigt in gemeinsam von mehreren Kunden genutzten Plattformen und Applikationen besondere Aufmerksamkeit. Insbesondere müssen die Betriebsprozesse in der Cloud gewährleisten, dass keine Verwechslung, Durchmischung oder ein nicht intendierter Abgleich von Daten (z.B. in nicht strikt mandantenfähig ausgelegten Applikationen) erfolgt.

4. Eine auf allgemeine Nutzung ausgelegte Cloud wird in aller Regel auch nur allgemein definierte und implementierte Sicherheitseinrichtungen aufweisen – die zugehörigen Service Agreements sind im gleichem Sinne stark standardisiert und decken die Bereiche Informationssicherheit, Risiko-Management, 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 zusätzli-

cher, 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 Reporting-Schnittstellen 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 Risiko-Management, basierend auf kundenspezifischen «Key Performance Indicators», steht in dieser Form als Führungs- und Entscheidungsunterstützungswerkzeug nicht mehr zur Verfügung.

6. Die Abhängigkeitskette bezüglich End-zu-End-Verfügbarkeit wird nicht nur länger, sondern für den Kunden durch die starke Dynamik der Dienstserbringung (Virtualisierung, Ortsveränderlichkeit usw.) auch intransparenter. Dies muss insbesondere in der Szenarienplanung für die Betriebsweiterführung im Not- und Krisenfall berücksichtigt werden. Da jedoch die Cloud Services durch ihre Ausrichtung auf ein standardisiertes Dienstangebot und standardisierte Technologiekomponenten weniger komplex sind als die klassischen Outsourcing-Modelle inklusive dem Betrieb bestehender Legacy-Umgebungen, 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 Wirtschaftsstandortes ...) oder der informationellen Kriegsführung reicht. Ein zusätzliches Problem entsteht hierbei 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.

Schlussfolgerungen

Die vorgängig aufgeführte Liste von Sicherheits- und Risiko-Management-Aspekten kann zu dem Schluss führen, dass die Nutzung Cloud-basierter Angebote generell nicht angezeigt ist – dieser Haltung stehen jedoch die möglichen Einsparungen und Skaleneffekte gegenüber, die in einer Risiko-Gewinn- und Verlustrechnung zu berücksichtigen sind. Jedoch müssen die Aspekte der rechtlichen und regulatorischen Rahmenbedingungen und der korrekten Ausübung von Governance- und Compliance-Vorgaben bei Cloud-basierten Services sehr sorgfältig und unter Beizug aller betroffenen Instanzen vor einem allfälligen Service-Bezug abgeklärt werden.
Ein möglicher Startpunkt für diese Abklärung aus Sicht der IT kann die «Security Guidance for Critical Areas of Focus in Cloud Computing» der «Cloud Security Alliance» sein, welche seit Dezember 2009 in der aktualisierten Fassung 2.1. vorliegt. Dieses Dokument spezifiziert die Sicherheitsanforderungen an Cloud-Computing-Umgebungen anhand von zwölf Arbeitsbereichen: (siehe Tabelle).
Für jeden dieser Arbeitsbereiche werden generische Empfehlungen bezüglich Umsetzung in cloud-basierten Umgebungen gemacht, welche die Grundlage für die Spezifikation von Kundenanforderungen bezüglich Informationssicherheit bilden können – eine 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 Risiko-Profil zu entscheiden haben, ob sie bezüglich Cloud-basierten Diensten als «early adaptor» oder doch eher als «late follower» agieren wollen. □

Aufsicht	Betrieb
Governance & Enterprise Risk Management	Traditional Security, Business Continuity and Disaster Recovery
Legal and Electronic Discovery	Data Center Operations
Compliance and Audit	Incident Response, Notification and Remediation
Information Lifecycle Management	Application Security
Portability and Interoperability	Encryption and Key Management Identity and Access Management Virtualization