

Sicherheitsaspekte beim Cloud Computing

Leitlinien für Anwender im „global sourcing“

Eberhard von Faber¹

Einordnung: Unternehmen und Institutionen können Dienstleistungen Dritter in Anspruch nehmen, statt Informationstechnologie selbst und unter eigener Verantwortung zu betreiben und zu pflegen. Für Kommunikationsleistungen z.B. über das Internet ist das inzwischen selbstverständlich. Aber auch Systeme und Anwendungen werden zunehmend so genutzt. Natürlich sind damit Unsicherheiten und Risiken verbunden. Anwender benötigen Hilfestellungen, wie sie dies in ihr Risikomanagement integrieren und welche Aufgaben mit welchen Schwerpunkten von ihnen durchzuführen sind.

Schlüsselwörter: Dienstleistungsmodelle; Arbeitsteilung; Outsourcing; Informationstechnologie; IT-Sicherheit; Cloud-Computing; Globalisierung; Risikomanagement; Datensicherheit; Datenschutz

Abstract

Anwender konzentrieren sich auf das Kerngeschäft und lagern IT-Leistungen zunehmend an externe Dienstleister aus. Jedes der angebotenen Modelle ist mit spezifischen Risiken bezüglich der IT-Sicherheit verbunden, mit denen sich die Anwender im Rahmen ihre Risikomanagements auseinandersetzen müssen. Um „Unsicherheiten“ im Sinne von mangelndem Wissen über real vorhandenen Risiken zu beseitigen, müssen Anwender vorab ihre Anbieter, deren Services und die Art der Serviceerbringung evaluieren. Der Beitrag zeigt wichtige Aspekte, Fragestellungen und eventuelle Grenzen bei der Herstellung der benötigten Transparenz speziell am Beispiel Cloud-Computing. Auf dieser Basis müssen dann gegebenenfalls „Unsicherheiten“ im Sinne unakzeptabler Risiken (durch mangelnde IT-Sicherheit) beseitigt werden. Dazu muss der Anwender im Rahmen eines im Beitrag skizzierten Vorgehensmodells seine Anforderungen genau spezifizieren. Dies kann gesetzliche Datenschutzerfordernungen (BDSG) einschließen. Erst dann kann die Umsetzung auf operativer Ebene bewertet werden. Die Arbeitsteilung in modernen Dienstleistungsmodellen schafft aber nicht nur Risiken, sondern senkt die Kosten und kann sogar das Sicherheitsniveau anheben. In jedem Falle hat der Anwender eine geschäftliche Entscheidung zu treffen. Der Beitrag bietet Hilfestellungen dazu.

¹ Eberhard.Faber@t-systems.com, T-Systems, Rabinstraße 8, D-53111 Bonn



Eberhard von Faber

arbeitet bei T-Systems im Aufgabenbereich Security Strategy und Executive Consulting; studierte Theoretische Elektrotechnik und promovierte auf dem Gebiet der Halbleiterphysik; verfügt über mehr als 17 Jahre Industrieerfahrung auf dem Gebiet der IT-Sicherheit; ist Professor für IT-Sicherheit an der Fachhochschule Brandenburg im Master-Studiengang Security-Management.

Einleitung

Mit fortschreitender Reife und Industrialisierung der Informationstechnologie (IT) kann der Anwender zunehmend unter mehreren Dienstleistungsmodellen wählen, deren Unterschiede wesentlich in der Arbeitsteilung zwischen Leistungserbringer und Anwender liegen. Sie reichen von Support, Überwachung oder aktiver Pflege von Inhouse- oder Campussystemen (im RZ des Anwenders) durch den Dienstleister über klassisches Hosting dedizierter Kundensysteme (im RZ des Dienstleisters) und dem Übergang auf die Verwendung von gemeinsam genutzten („shared“) Plattformen oder Anwendungen bis hin zur flexiblen Bereitstellung von IT-Ressourcen (meist „Services“) auch über das Internet. Zu dem letztgenannten „as-a-Service“-Modell gehört auch das Cloud-Computing. Zu den bereitgestellten IT-Ressourcen gehören Software (Software-as-a-Service, SaaS), Speicher und Rechenleistung („utility computing“), komplette Systeme („platform-as-a-Service“) oder Anwendungen bzw. Dienste von speziellen Anwendungen („managed services“).

Mit der Übertragung von IT-Services an einen Anbieter und der damit einhergehenden weiteren Dezentralisierung und Verteilung von IT entstehen neue Angriffsvektoren und damit mögliche Risiken. Im folgenden werden am Beispiel „Cloud-Computing“ Fragestellungen hinsichtlich der Datensicherheit und des Datenschutzes erläutert sowie ein Modell vorgestellt, wie Anwender vorgehen können, um adäquate Dienstleistungsmodelle und Anbieter zu finden, bei denen die Risiken durch Vorteile aufgewogen werden. Die meisten dieser Risiken resultieren nicht direkt aus der IT, sondern (wie so oft) der Art und Weise, wie sie eingesetzt wird.

1. Definition „Cloud-Computing“ und Dilemma

Allen diesen „as-a-Service“-Modellen ist gemeinsam, dass IT gemeinsam von mehreren Anwendern genutzt wird. Aus Sicht des Dienstleisters handelt es um einen „1-to-many“-Ansatz. Technisch werden Virtualisierungstechnologien eingesetzt und Plattformen, Systeme oder Anwendungen sind mandantenfähig ausgelegt. „Cloud-Computing“ ist eigentlich kein neues Dienstleistungsmodell, sondern eine Architektur für die Bereitstellung von IT-Leistungen, die durch Verteilung und Lastverteilbarkeit gekennzeichnet ist. Die Haupteigenschaft aus Nutzersicht ist die extrem hohe Skalierbarkeit. In dem Sinne ist „Cloud-Computing“ keine Alternative zu SaaS, sondern eine besondere Form von deren Bereitstellung. Trotzdem wirft „Cloud-Computing“ besondere Fragestellungen hinsichtlich IT-Sicherheit auf, die im folgenden diskutiert werden.

Risiken bezüglich der IT-Sicherheit sind mit jeder Art der Leistungserbringung verbunden. Um eine geschäftliche Entscheidung treffen zu können, ob das Anwenderunternehmen diese zu akzeptieren gewillt ist (oder Verbesserungen nötig sind), benötigt man Wissen über das Sicherheitsniveau. „Unsicherheit“ kann also zweierlei bedeuten:

- das Vorhandensein unakzeptabler Risiken (also mangelnde IT-Sicherheit) oder
- mangelndes Wissen über die real vorhandenen Risiken bzw. die integrierten Sicherheitsmaßnahmen (mangelnde Vertrauenswürdigkeit).

Das Dilemma besteht nun gewissermaßen darin, dass das Konzept „Cloud-Computing“ darin besteht, dem Anwender einen hochgradig standardisierten Service sehr flexibel, d.h. weitgehend autonom durch den Dienstleister bestimmt, bereitzustellen. So wie bei der Versorgung mit Elektroenergie soll sich der Anwender (Verbraucher) nur für Qualität der Leistung interessieren und nicht für deren Produktion. Der Anwender soll also keine detaillierten Kenntnisse über die Hintergründe der Leistungserbringung haben. Und doch sind sie oft sicherheitsrelevant. Beispiel: Der Anbieter transferiert die Daten in ein Land seiner Wahl, um Rechen- und Speicherkapazitäten bestmöglich auszunutzen und den Service kostenoptimal anbieten zu können. Der Produktionsstandort hat aber Auswirkungen auf die Sicherheit.

2. Datensicherheit und Datenschutz

Wenn nicht bekannt ist, auf welchen Systemen, in welchem Rechenzentrum und in welchem Land sich die Daten und Anwendungen befinden, kann dies dazu führen, dass staatliche Gesetze und Anforderungen oder unternehmens- oder branchenspezifische Auflagen nicht erfüllt werden. Oder dem Anwender fehlt ein Nachweis, dass der Anbieter solche Auflagen erfüllt.

Einzelne Länder unterscheiden sich hinsichtlich Gegebenheiten, die auch Einfluss auf die Sicherheit haben. Man vergleiche Produktionsstandorte wie China und Russland, Indien und Brasilien oder Schweiz und Deutschland. Bedingungen bzw. Risiken, die Anwender konkret betrachten müssen sind:

- Datenschutz und Datenschutzgesetzgebung (Vertraulichkeit persönlicher Daten),
- Schutz von geistigem Eigentum und der Gesetzgebung dazu,
- Risiken durch staatliche Eingriffe (unbemerkter Zugriff, Abhören) sowie Verbot oder Einschränkungen hinsichtlich der Nutzung von Sicherheitstechnologien wie z.B. Verschlüsselung,
- Sicherheitskultur (Verständnis der Menschen, Geschichte und Erfahrungen mit IT-Sicherheit, rechtliche Tradition),
- internationale Zusammenarbeit bei der Rechtspflege, Rechtslage und Praxis zum Schutz von Angestellten, allgemeiner Rechtsschutz von Verträgen usw.

Manche Anbieter bieten sogenannte „private clouds“, bei denen der Datenaustausch in vordefinierten Rahmen innerhalb des internen Netzes erfolgt. Dadurch können Risiken von vornherein ausgeschlossen werden. Doch es gibt mehr als die länderspezifische Risiken, die Anwender eventuell betrachten müssen. Auf operativer Ebene sind folgende Bereiche hinsichtlich Relevanz und Erfüllung zu prüfen:

- technische Maßnahmen der IT-Sicherheit,
- Personal und Prozesse,
- bauliche und physische Sicherheitsmaßnahmen (RZ-Sicherheit),
- Architekturen und Lokationen,
- Datenaustausch, Zusammenarbeit- und Zugriffsmodelle,
- Business Continuity and Disaster Recovery,
- Überwachung und Management von Sicherheitsvorfällen.

Allem voran sollten Anwender darauf achten, dass der Anbieter notwendige Maßnahmen wie Backup mit Recovery-Fähigkeit anbietet. Eventuell müssen Daten und Software hierfür oder aus anderen Gründen auch auf andere Systeme portiert werden. Dies muss rechtlich und technisch möglich sein und sollte getestet werden. Auch sollten Anwender nicht vergessen, dass ihre Datensicherheit ganz maßgeblich dadurch bestimmt wird, dass der Anbieter sein Geschäft aufrechterhält und aufrechterhalten kann. Große Anbieter, die IT-Outsourcing strategisch mit langem Erfahrungshorizont betreiben, sind sicher kleineren oder solchen vorzuziehen, die das Thema erst zu entwickeln versuchen.

3. Vorgehen

Für Anwender mit Sicherheitsanforderungen ist die Kenntnis des notwendigen Sicherheitsniveaus unerlässlich. Schließlich sind IT-Risiken Geschäftsrisiken. Auch die IT muss daher im Rahmen des Risikomanagements bewertet werden. Das Risikomanagement identifiziert, analysiert und bewertet Risiken. Dann wird eine geschäftliche Entscheidung getroffen, ob diese Risiken akzeptiert oder Maßnahmen ergriffen werden, um diese zu verringern, abzuwälzen oder zu vermeiden. Die Umsetzung und Kontrolle der Maßnahmen ist Teil des Risikomanagements. Dafür ist ein enger Austausch mit dem Anbieter unerlässlich, um die notwendigen Informationen über den Anbieter, über dessen Service und die Serviceerbringung zu beschaffen. Häufig hat der Anwender keine oder nur beschränkte Möglichkeiten, eigene Tests durchzuführen oder individuelle Anforderungen durchzusetzen und zu kontrollieren. Umso wichtiger ist deshalb eine „due diligence“ des Anbieters, um die notwendige Transparenz zu schaffen.

Bei jeder Art von „Outsourcing“ muss der Anwender folgende Phasen durchlaufen: Strategiebildung, Anforderungsdefinition, Marktanalyse und Anbieterauswahl, Verhandlungen und Abschluss, sowie schließlich Betrieb. In jeder dieser Phasen muss die IT-Sicherheit von Anfang an bedacht werden. Der Anwender muss seinen Anbieter genau evaluieren und vertragliche Vereinbarungen als SLA treffen hinsichtlich der Einhaltung definierter Sicherheitsstandards. Dafür ist es häufig notwendig, die eigenen Anforderungen deutlicher und expliziter zu definieren als dies vielleicht für den internen Gebrauch praktiziert wird.

In diesem Zusammenhang sind auch die relevanten Datenschutzgesetze auf Bundes- und Landesebene zu berücksichtigen, die sie die Auftragsverarbeitung personenbezogener Daten an besondere Voraussetzungen knüpfen. So sind Sicherheitsanforderungen und Zweckbestimmung genau zu definieren, und der Anbieter muss zusichern, die Daten nur gemäß der Vorgaben des Auftraggebers zu verarbeiten.

Fragen sie ihren Anbieter (vorher), wer welche Zugriffe auf ihre Daten und Anwendungen haben kann, wie die Zugriffskontrolle organisiert ist und wie das Personal und ihre Zugriffe kontrolliert werden. Fragen sie, welche Schutzmaßnahmen bei der Datenübertragung, für die sichere Speicherung einschließlich Backup und Recovery getroffen wurden und wie die Separation von Anwendungen und Daten (durch Virtualisierungstechnologien) der einzelnen Anwender erreicht und sichergestellt wird. Betrachten sie Compliance und andere Aspekte. Auch geht es darum zu prüfen, welche generellen Anforderungen der Anbieter erfüllt und in welcher Form er dies nachweisen kann. Als Nachweis gelten regelmäßig erneuerte Zertifizierungen durch anerkannten Institutionen. Darüber hinaus können regelmäßige Überprüfungen durch den Anwender oder beauftragte Dritte erforderlich bzw. hilfreich sein.

Allgemein ist zu bedenken, dass die Sicherheit meistens höher eingeschätzt wird, wenn der Anwender selbst die Kontrolle ausübt, als wenn dies ein Dienstleister tut und dass jede Art von Dezentralisierung und Verteilung weitere Angriffsvektoren und damit mögliche Risiken hervorbringt. Dezentralisierung und Verteilung sind aber gerade mit Cloud-Computing untrennbar verbunden.

Jede extern erbrachte IT-Leistung entzieht sich dem gewohnten und selbstverständlich erscheinenden Schutz durch die selbst implementierten internen Maßnahmen des Anwenderunternehmens. Eigene Mitarbeiter erscheinen vertrauenswürdiger als die eines fremden Unternehmens. Doch Arbeitsteilung geht mit einer Spezialisierung einher, die nicht nur Kosten senkt. Spezialisten können in der Regel mehr, sie sind besser ausgebildet und verfügen über mehr Erfahrung, was sich in unserem Beispiel direkt positiv auf die Sicherheit auswirken kann. Das Outsourcing-Modell vereinfacht zudem eine Reihe sicherheitsrelevanter Aufgaben, weil diese zentral und durch einen spezialisierten Anbieter erbracht werden. Dazu gehören Implementierung, Konfiguration, Aktualisierung (Release-, Update- und Patch-Management), Backup sowie Überwachung und Pflege. Viele Anwender haben dagegen Probleme, solche regelmäßig notwendigen Arbeiten mit der nötigen Qualität selbst durchzuführen. Die Übertragung auf einen Dienstleister kann sich sehr positiv auf das Sicherheitsniveau auswirken. Dies gilt für die meisten Formen von „Outsourcing“.

4. Zusammenfassung

Mit jedem Modell der IT-Produktion sind Risiken bezüglich der IT-Sicherheit verbunden. Anwender müssen zweierlei „Unsicherheiten“ unterscheiden:

- das Vorhandensein unakzeptabler Risiken (also mangelnde IT-Sicherheit) oder
- mangelndes Wissen über die real vorhandenen Risiken bzw. die integrierten Sicherheitsmaßnahmen (mangelnde Vertrauenswürdigkeit).

Mit der Übertragung von IT-Services an einen Anbieter und der damit einhergehenden weiteren Dezentralisierung und Verteilung von IT entstehen neue Angriffsvektoren und mögliche Risiken. Besonders ausgeprägt ist dies beim Cloud-Computing. Neben länderspezifischen Risiken sind auf operativer Ebene weitere Bereiche zu betrachten. Eine „due dilligence“ des Anbieters schafft die notwendige Transparenz. Bei jeder Art von „Outsourcing“ muss der Anwender folgende Phasen durchlaufen:

- Strategiebildung,
- Anforderungsdefinition,
- Marktanalyse und Anbieterauswahl,
- Verhandlungen und Abschluss, sowie schließlich den
- Betrieb.

In jeder dieser Phasen muss die IT-Sicherheit von Anfang an bedacht werden. Dazu gehört auch die Berücksichtigung gesetzlicher Anforderungen zum Beispiel hinsichtlich des Datenschutzes.

Die Arbeitsteilung in modernen Dienstleistungsmodellen schafft aber nicht nur Risiken, sondern senkt die Kosten und kann sogar das Sicherheitsniveau anheben. In jedem Falle hat der Anwender eine geschäftliche Entscheidung zu treffen. Der Beitrag beschreibt wichtige Sachverhalte und Vorgehensweisen, die Anwender im Rahmen ihres Risikomanagements bei der Entscheidungsfindung und Ausgestaltung ihrer Vertragsbeziehungen mit externen Dienstleistern berücksichtigen sollten.

5. Literatur

- [1] Bruce Robertson: Top Five Cloud-Computing Adoption Inhibitors; Gartner Research, 13. May 2007
- [2] Arabella Hellowell: Security and Privacy Considerations with Global Outsourcing; Track Session, Gartner IT Security Summit 2007, 17-19 Sept. 2007, London

© 2009 Eberhard von Faber und Friedrich-L. Holl, Brandenburg an der Havel, alle Rechte vorbehalten. Verwertung ist nur mit vollständiger Quellenangabe und unter Angabe der Bezugsquelle erlaubt. Reproduktion und anderweitige Wiedergabe des Dokumentes bedarf darüber hinaus der ausdrücklichen Genehmigung der Rechteinhaber.

Titel: The Bulletin Security Management
Herausgeber: Eberhard von Faber und Friedrich-L. Holl

ISSN: 1869-2125
Bezugsquelle: www.security-management.de

Kontakt:



Prof. Dr. Eberhard von Faber und
Prof. Dr. Friedrich Lothar Holl
Fachhochschule Brandenburg
Fachbereich Wirtschaft
Studiengang Security-Management
Magdeburger Str. 50, 14770 Brandenburg

Unterstützt von:



Infos und Kontakt: www.t-systems.de/ict-security