Bundesministerium
für Wirtschaft
und Technologie

WIRTSCHAFT.
WACHSTUM.
WOHLSTAND.

Nationaler IT Gipfel
München 2011

Anbieterwechsel im Cloud Computing

Wege zur Steigerung von Akzeptanz und Vertrauen

AG2 Fachinitiative „Cloud Computing“

Inhaltsverzeichnis

Vorwort

Die Projektgruppe Cloud Computing der Arbeitsgruppe 2 „Digitale Infrastrukturen“ des Nationalen IT Gipfels hat sich zur „Fachinitiative Cloud Computing“ entwickelt. Ziel der Fachinitiative ist es, die Rahmenbedingungen von Anbietern und Anwendern zu analysieren und so zu entwickeln, dass die Innovationspotenziale des Cloud Computings in Deutschland genutzt werden können. Wesentlicher Hebel hierfür ist das gemeinsame Wirken über Unternehmens- und Branchengrenzen hinweg.

Die Fachinitiative Cloud Computing ist unabhängig und versteht sich als marktübergreifendes Gremium von Experten und Marktbeteiligten. Sie wird getragen von führenden Unternehmen der Telekommunikations-, IT- und Internet-Wirtschaft, aber auch von Vertretern der Wissenschaft, von neutralen Prüfinstituten sowie dem Bundesamt für Sicherheit in der Informationstechnik. Dabei setzt die Initiative an drei relevanten Stellen an:

1. der Förderung von Vertrauen in und Akzeptanz von Cloud-Diensten bei gewerblichen Nutzern, der öffentlichen Hand und Privatkunden,

2. der Klärung von Fragen der Interoperabilität und des Anbieterwechsels und

3. dem Ausbau sicherer und hochleistungsfähiger Breitbandnetze und sicherer technischer Plattformen in der Cloud.

In der IKT-Strategie der Bundesregierung „Deutschland Digital 2015“[1], veröffentlicht im November 2010 durch das Bundesministerium für Wirtschaft und Technologie, wird Cloud Computing derzeit als eines der vielversprechendsten Themen für Anbieter und Anwender in der IKT beschrieben. Es bietet dem Anwender eine bedarfsgerechte und flexible Nutzung von Informations- und Kommunikationstechnologien. Aber damit Cloud Computing sicher und zuverlässig eingesetzt werden kann, sind besondere Aspekte zu beachten.

Die Bundesregierung strebt das Ziel an, die Entwicklung und Einführung von Cloud-Computing-Lösungen zu beschleunigen. Gerade mittelständische Unternehmen und der öffentliche Sektor sollen frühzeitig von den Chancen und Wachstumsimpulsen durch Cloud Computing profitieren, die sich für nahezu alle Branchen ergeben.

Die Bundesregierung adressiert mit Blick auf das Cloud-Computing-Aktionsprogramm vier konkrete Handlungsfelder:

- Innovations- und Marktpotenziale erschließen (Forschungsprogramm Sichere Internet-Dienste – Cloud Computing für den Mittelstand und öffentlichen Sektor [Trusted Cloud]),

- Innovationsfreundliche Rahmenbedingungen schaffen (Sicherheit und rechtliche Rahmenbedingungen, Standards, Zertifizierungen),

- Internationale Entwicklungen mitgestalten und

- Orientierungswissen geben.

1 http://www.bmwi.de/BMWi/Navigation/Technologie-und-Innovation/Digitale-Welt/IKT-Strategie-Nationaler-IT-Gipfel/deutschland-digital-2015.html

1. Einleitung und Zielsetzung

Die zugrunde liegende Technologie des Cloud Computings ist nicht neu. Im Gegenteil, viele Bestandteile – wie beispielsweise Outsourcing, Service-on-Demand – sind bereits seit Jahren in vielen Unternehmen und Organisationen im Einsatz. Neu ist, dass sich aus Cloud Computing neue und veränderte Geschäftsmodelle ergeben (können). Neue Geschäftsmodelle gelangen allerdings nur dann zur Reife, wenn die Technologie wirtschaftlich attraktiv und sicher ist und auf breite Akzeptanz im Markt und bei den Anwendern stößt.

Die Stärkung von Vertrauen und Akzeptanz bezüglich Cloud Computing hat viele Facetten. Neben betriebswirtschaftlichen Aspekten bei der Auswahl des „richtigen“ Cloud-Anbieters spielen Sicherheitsaspekte, Vertragselemente, Verfügbarkeit der IT-Ressourcen und vor allem auch die Möglichkeit zum Wechsel des Cloud-Anbieters eine sehr wichtige Rolle.

Der Cloud-Computing-Markt ist dynamisch und hoch innovativ mit erheblichem Effizienzpotenzial. Aus diesem Grund werden Anwender darauf achten, möglichst unabhängig von ihrem Cloud-Anbieter zu sein, um ihn jederzeit wechseln zu können.

Ohne Zweifel würde diese Unabhängigkeit von einem bestimmten Cloud-Anbieter das Vertrauen in Cloud-Computing-Lösungen stärken. Ziel der Fachinitiative Cloud Computing der Arbeitsgruppe 2 des IT Gipfels ist es deshalb, das Vertrauen in und die Akzeptanz von Cloud- Computing-Lösungen zu stärken.

Zu diesem Zweck soll aufgezeigt werden, welche Kriterien bei einem Wechsel des Cloud-Anbieters zu berücksichtigen sind. Cloud-Anwendern sollen Hinweise gegeben werden, welche Kriterien bereits beim Einstieg in die Cloud beachtet werden sollten, um in der Zukunft ausreichend Flexibilität für einen Wechsel des Cloud-Anbieters zu haben. Zum besseren Verständnis werden diese Entscheidungskriterien ab Kapitel 6 am Beispiel des Cloud-Computing-Typs Infrastructure-as-a-Service (IaaS) näher erläutert.

Gleichzeitig sollen Handlungsempfehlungen an die Politik gegeben werden, auf welche Art und Weise die Akzeptanz von Cloud Computing in Deutschland erhöht werden kann.

Die Fachinitiative Cloud Computing will sich im kommenden Jahr mit der Ausarbeitung der Kriterien zum Anbieterwechsel auf den Ebenen Platform-as-a-Service (PaaS) und Software-as-a-Service (SaaS) beschäftigen. Dazu soll die Fachinitiative ausgebaut werden und den Dialog mit unterschiedlichen Branchen suchen.

2. Cloud Wertschöpfungskette

Cloud Computing ist einer der zentralen Entwicklungstrends der IKT-Branche. Immer mehr Business-Modelle mit innovativen Produkten und Dienstleistungen werden auf Basis von Cloud-basierten Lösungen realisiert. Dieser Entwicklungstrend umfasst sowohl Lösungen für den Privatkunden/Endverbraucher als auch Lösungen für professionelle Nutzungsszenarien.

Einhergehend mit dieser Entwicklung verändert sich – mit ebenso hoher Dynamik – die bisherige Wertschöpfungskette hin zu einem sehr ausdifferenzierten „Ökosystem Cloud-Computing“. War es noch in der Vergangenheit gang und gäbe, dass man im Zuge von IT-Outsourcingprojekten einen Auftragnehmer hatte, der in der Regel das komplette Portfolio der Infrastruktur, Plattform, Applikation und Webspace anbot, hat sich der Markt auf Seiten der Anbieter erheblich differenziert. So ist es mittlerweile üblich, dass ein Auftraggeber gleichzeitig mehrere Dienstleister beauftragt, unterschiedliche Wertschöpfungen zu übernehmen.

Das Auslagern von Wertschöpfungsketten in die Cloud ist heute in vielen Unternehmens- und Verwaltungsbereichen bereits Realität. Von einfachen Webdiensten wie beispielsweise Webmail oder das Anmieten von Speicher oder Storage bis hin zur Auslagerung einer vollständigen Unternehmens-IT-Infrastruktur oder der Auslagerung ganzer Geschäftsprozesse (etwa im Bereich des Kundenbeziehungsmanagements) ist bei Cloud Computing alles möglich. Charakterisierend hierfür ist stets, dass der Anwender bereit ist, Daten und Informationen in die Cloud zu geben, und zwar bei dem Cloud-Anbieter seiner Wahl, bei dem er die dafür notwendigen Services (Infrastruktur oder Funktionalität) anmietet. Der Anwender zahlt in gleichem Maße, wie er die Ressourcen des Anbieters nutzt. Sehr vereinfacht dargestellt, stellt ein Cloud-Anbieter einem Cloud-Anwender die gewünschte IT-Infrastruktur (Plattform, IT-Infrastruktur, Speicher bis hin zu betriebswirtschaftlicher Anwendungssoftware) zur Verfügung und der Anwender zahlt nach entsprechendem Verbrauch.

So ist es beispielsweise möglich, über eine einfache Webservice-Schnittstelle eine beliebige Datenmenge zu jeder Zeit und von jedem Ort im Internet aufzurufen und zu speichern. Diese Vorgehensweise kann die hauseigenen Server oder ggf. auch das Speichermedium (Festplatte) des Endgerätes vollständig ersetzen.

Durch Cloud Computing findet ein Prozess des Wandels statt. Waren es früher klassische Telekommunikations-, Software und Hardwareanbieter, die IKT-Dienste zur Verfügung gestellt haben, sind es heute beispielsweise E-Commerce-Unternehmen, welche eigene (ungenutzte) IT-Ressourcen gegen Nutzungsgebühr zur Verfügung stellen. Gemein ist ihnen, dass sie dafür die Netze und die erforderlichen bewährten Technologien benötigen.

Es müssen also nicht mehr alle Akteure im Cloud-Computing-Markt die gesamte Wertschöpfungskette bedienen. Über das Cloud Computing vollzieht sich der Wandel zu globalen und relativ komplexen Wertschöpfungsnetzen.

3. Eigenschaften und Einsatzarten des Cloud Computings

Für den Anbieterwechsel ist es entscheidend, eine einheitliche Definition für Cloud Computing zu haben, die den Vergleich verschiedener Cloud-Angebote überhaupt erst ermöglicht. Eine einheitliche Definition des Begriffs „Cloud Computing“ ist derzeit jedoch nicht verfügbar. Die bestehenden Definitionen weisen weitgehende Gemeinsamkeiten und zugleich auch Unterschiede auf. Unterschiede existieren in der Einordnung des „Cloud Computings“ als Paradigma, Modell, oder Verwendung von Dienstleistungen sowie der Menge der jeweils zur Definition verwendeten Eigenschaften und im technischen Umfang (z. B. IT-Strukturkomponenten, Schnittstellen, Protokolle).

Ausgehend von den verbreiteten Definitionen des National Institute of Standards and Technology (NIST)[2], der European Network and Information Security Agency (ENISA)[3] und des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[4], werden für eine solche Definition zunächst die wesentlichen Eigenschaften und Einsatzarten des Cloud Computings zusammenfassend dargestellt.

In den verfügbaren Definitionen werden Adjektive wie zum Beispiel „bequem oder schnell“ sowie auch Umschreibungen wie „stets verfügbar“ und „mit minimalem Verwaltungsaufwand“ verwendet. Diese Begriffe unterstützen zwar die zumeist subjektive Bewertung einzelner Realisierungen, jedoch nicht die Bestimmung, ob etwas „Cloud Computing“ ist oder bis zu welchem Grad eine Realisierung diese Anforderungen erfüllt bzw. erfüllen muss. Soweit diese Begriffe nicht zu einer klaren Abgrenzung des Begriffs „Cloud Computing“ von anderen Begriffen der IT beitragen, wird auf sie verzichtet. Die im Folgenden verwendeten Eigenschaften der IT werden in fast allen verfügbaren Definitionen des Begriffs „Cloud Computing“ verwendet

3.1. Eigenschaften und Typisierung von Cloud Computing

Cloud Computing ist durch die folgenden Eigenschaften gekennzeichnet:

- IT-Ressourcen können zeitgleich von mehreren Nutzern verwendet werden. Das heißt zum Beispiel, unterschiedliche Organisationen können den gleichen Server eines Cloud-Anbieters nutzen (Mehrfachverwendung von IT-Ressourcen). Dies kann beispielsweise bei Webmail der Fall sein.

- Art und Umfang der verwendeten IT-Ressourcen (z. B. Systeme, Bandbreite, Speicher) sind bei Bedarf veränderbar (Skalierbarkeit). Das heißt zum Beispiel, wird mehr Speicherplatz benötigt, kann dieser unverzüglich durch den Cloud-Anbieter zur Verfügung gestellt werden.

- Die Abrechnung erfolgt nach tatsächlichem Verbrauch. Grundlage einer Abrechnung, sofern der Dienst nicht kostenfrei ist, sind zum Beispiel die Anzahl der verwendeten Systeme und ihre Nutzungsdauer.

- Art und Umfang der IT-Ressourcen sowie der Umfang, in dem diese genutzt werden, können vom Nutzer des Cloud Computing verändert werden (Selbstversorgung). Der Nutzer kann sich für den eigenen Bedarf selbst und ohne manuelle Zuarbeit des Cloud-Anbieters mit IT-Ressourcen versorgen, zum Beispiel Speicherkapazität erweitern oder die Anzahl der verwendeten Systeme reduzieren.

- Die Nutzung kann durch unterschiedliche handelsübliche Endgeräte erfolgen. Dies bedeutet, dass die Nutzung des Cloud Computing nicht die Verwendung bestimmter Router, Betriebssysteme oder Client-Software voraussetzt.

2 http://www.nist.gov/index.html
3 http://www.enisa.europa.eu/
4 https://www.bsi.bund.de/DE/Home/home_node.html

Im Cloud Computing – insbesondere in der Definition des NIST – werden klassischerweise folgende Typen differenziert: die dienstorientierten Typen und die nutzungsorientierten Typen.

3.1.1. Dienstorientierte Typen des Cloud Computing

Infrastructure-as-a-Service (IaaS)
Die Leistungen, die dem Nutzer zur Verfügung gestellt werden, umfassen Rechenleistung, Speicher, Netze und andere grundlegende IT-Ressourcen, die vom Nutzer benötigt werden, um beliebige Software (Betriebssysteme, Anwendungen) einzusetzen und auszuführen.

Die zugrunde liegende Infrastruktur der Cloud wird vom Nutzer weder verwaltet noch betrieben. Betriebssystem, Speicher, eingesetzte Software und möglicherweise in begrenztem Umfang ausgewählte Netzkomponenten, wie zum Beispiel Firewalls, unterliegen jedoch der Kontrolle des Nutzers.

Platform-as-a-Service (PaaS)
Bei PaaS hat der Nutzer die Kontrolle über die eingesetzten Anwendungen und möglicherweise über die Konfiguration der IT-Umgebung. Die Kontrolle über die zugrunde liegende Cloud Infrastruktur, einschließlich der Netze, Server, Betriebssystem, Speicher, Application Programming Interfaces oder auch zusätzlichen Dienste-Angeboten obliegt dem Diensteanbieter.

Software-as-a-Service (SaaS)
Die dem Nutzer zur Verfügung gestellte Leistung umfasst die Verwendung von Anwendungen des Betreibers. Die Anwendungen können mittels beispielsweise eines Web-Browsers (zum Beispiel. webbasierte E-Mail) von verschiedenen Endgeräten (PC, Smartphones, Tablet PC) aus genutzt werden.

3.1.2. Nutzungsorientierte Typen des Cloud Computings

Individuelle Cloud (Private Cloud)
Die Cloud Infrastruktur wird für genau eine Organisation betrieben. Der Betrieb kann durch die Organisation oder einen IKT-Dienstleister erfolgen. Der Nutzer weiß genau, wo seine Daten liegen.

Gemeinschafts-Cloud (Community Cloud)
Die Cloud Infrastruktur wird von mehreren Organisationen mit gemeinsamen Interessen (zum Beispiel Aufgaben, Sicherheitsanforderungen, Richtlinien oder Compliance-Anforderungen) genutzt. Der Nutzer weiß nicht, wo sich seine Daten befinden – es sei denn, er legt den Standort der Daten mit dem Cloud-Anbieter fest.

Öffentliche Cloud (Public Cloud)
Die Public Cloud Infrastruktur ist über das Internet offen zugänglich. Der Nutzer weiß definitiv nicht, an welchem Standort sich seine Daten befinden.

Gemischte Cloud (Hybrid Cloud)
Die Cloud Infrastruktur besteht aus Mischformen aus den oben genannten nutzungsorientierten Cloud-Typen.

3.2. Vergleich von Cloud-Computing-Lösungen

Erst wenn Dienst- und Nutzungstyp unterschiedlicher Anbieter identisch sind, ist ein Vergleich der Cloud-Lösungen möglich. Mögliche Unterscheidungsmerkmale sind zum Beispiel:

- das Maximum von zeitgleicher Nutzung der IT-Ressourcen,
- Skalierbarkeit von IT-Ressourcen,
- die Abrechnungsgrundlage für die Nutzung von IT-Ressourcen,

- der Umfang, in dem der Nutzer selbst Einfluss auf verwendete IT-Ressourcen nehmen kann,
- die Zugriffsmöglichkeiten durch unterschiedliche handelsübliche Endgeräte,
- die Art und Weise, wie mit Endgeräten von außen auf die IT-Ressourcen zugegriffen wird und
- die zeitlichen Beschränkungen (zum Beispiel. stündlich oder täglich), unter denen die Eigenschaften einer Cloud-Computing-Lösung verändert werden können.

Der Vergleich von Cloud-Computing-Lösungen wird einfacher und transparenter, wenn durch anerkannte Standards einheitliche Rahmenbedingungen und Anforderungen an die Realisierung definiert werden.

4. Klare Normen und Standards für maximale Interoperabilität

4.1. Bedeutungszuwachs und hohe Dynamik im Markt erfordern Interoperabilität

Die dynamische Entwicklung im Cloud Computing führt dazu, dass zwei wesentliche Aspekte unabdingbar werden:

1. **Transparenz und Zertifizierung:** Je transparenter die Dienstleistung von einem Cloud-Anbieter erbracht wird, desto einfacher ist es, sie mit anderen Anbietern zu vergleichen. Zertifizierungen geben dem Anwender einen Orientierungsrahmen, in welchem Maße und Umfang ein Dienstleister besondere Kriterien (zum Beispiel Datensicherheit, Datenschutz) erfüllt.

2. **Offene Standards und Normen:** Es sollten klare offene Standards und Normen entwickelt werden, die der hohen Dynamik in der Wertschöpfungskette Rechnung tragen und ein Mindestmaß an Interoperabilität ermöglichen, um ein reibungsloses Zusammenspiel der unterschiedlichen Beteiligten zu gewährleisten.

4.2. Cloud Computing Standards und Normen

Standards und Normen haben sich als wichtiges Instrument in vielen Lebensbereichen entwickelt, die es erst ermöglichen, dass unterschiedlichste Prozesse reibungslos vonstattengehen. Standards werden beispielsweise in Standardisierungsorganisationen (DIN, ETSI) oder offenen Foren und Konsortien gesetzt.

Sowohl in Deutschland als auch auf europäischer und internationaler Ebene haben unterschiedliche Normierungsgremien und Industrieinitiativen den Dialog gestartet, um wesentliche Standardisierungen zu erreichen. Momentan gibt es keine speziell für Cloud Computing entwickelten Standards und Normen. Internationale Standardisierungs-Organisationen arbeiten an der Anpassung bestehender sowie der Entwicklung neuer Normen.

Vor allem im internationalen Gremium ISO/IEC JTC 1/ SC 38 „Distributed application platforms and services“ (DAPS), das sich mit der Normung von Cloud-Computing-Themen befasst, wird derzeit erarbeitet, welche bereits bestehenden Dokumente von offenen Foren und Konsortien, wie beispielsweise der Open Group, OASIS oder W3C sich eignen, modifiziert als ISO-Standard übernommen zu werden.

Auch andere Gremien im Bereich der Informationstechnologie, beispielsweise JTC 1/ SC 27 „IT Security techniques“, haben das Thema Cloud Computing in ihr Arbeitsprogramm aufgenommen. Eine Konsolidierung der Arbeiten wird also auf internationaler Ebene zu den nächsten Schritten gehören. Bisher sind aus diesen Aktivitäten noch keine Normen hervorgegangen. Es ist jedoch zu erwarten, dass mittelfristig einige Standards erarbeitet werden, in denen beispielsweise terminologische Festlegungen getroffen werden.

4.3. Zertifizierungen schaffen Transparenz

Überall dort, wo die klassische Massenfertigung und Serienproduktion ihre Grenzen findet und trotzdem gleichbleibende Qualitätsstandards eingehalten werden sollten, kommen Zertifizierungen zum Einsatz. IT-Systeme und insbesondere Cloud-basierte Lösungen sind Systeme mit einem sehr hohen Spezifizierungs-/Individualisierungsgrad. Gleichbleibende Qualitätsanforderungen an Produkte können bislang in vielen Bereichen mit Prüfsiegeln oder Ähnlichem dokumentiert werden. Bei stark individualisierten Produkten (wie beispielsweise Cloud-basierten Lösungen) ist dies allerdings nur schwer möglich. Hier wäre eine Zertifizierung der Geschäftsprozesse beim Anbieter eine zielführende Alternative, mit deren Hilfe ein Mindestmaß an Qualitätsanforderungen dokumentiert und hervorgehoben wird – ähnlich wie die bisherigen Zertifizierungen nach ISO 9001, bei denen eine gleichbleibende Prozessqualität zertifiziert wird – weniger ein konkretes Produkt. Eine Garantie geben Zertifizierungen dem Nutzer jedoch nicht.

Ein zentraler Diskussionspunkt ist allerdings die Frage, welche Kriterien den Hauptfokus einer Zertifizierung darstellen. In der Diskussion sind momentan sehr stark Sicherheitsaspekte – insbesondere mit Blick auf Cloud-basierte Lösungen. Hier wäre beispielsweise die strikte Anwendung eines Privacy and Security Assessments, wie es bereits von einzelnen ITK-Unternehmen angewandt wird, zu zertifizieren.

5. Auswahlkriterien für den Anbieterwechsel (Fokus Infrastructure-as-a-Service)

Bei einer dynamischen Entwicklung von Cloud Computing sind künftig Anbieterwechsel – ähnlich wie im Strom- oder Gasmarkt – zu erwarten. Unabhängig von der Motivation des Anbieterwechsels ist es zwingend erforderlich, Klarheit über die Unterschiede des aktuell genutzten Cloudangebots sowie des Angebots des künftigen Anbieters zu haben. Nur so kann sichergestellt werden, dass der mit dem Wechsel erhoffte Zusatznutzen auch tatsächlich eintritt.

Der folgende Abschnitt führt Eigenschaften von Kriterien, Ressourcen und Kostenpunkte auf, über die aus Konsumentensicht vor dem Cloud-Anbieterwechsel (und am besten auch bereits vor dem Einstieg in die Cloud) Transparenz geschaffen werden sollte. Aufgrund der vielfältigen Anforderungen verschiedener Dienste-Nutzer lassen sich keine pauschalen Aussagen über Vor- und Nachteile verschiedener Ausgestaltungen von Diensteangeboten machen. Vielmehr erfordert die Auswahl des passenden Diensteanbieters eine Analyse der Anforderungen beim Anwender. Im Anschluss ist ein Vergleich verschiedener Anbieter entlang dieser Anforderungen möglich.

5.1. Ressourcen

Ein wichtiges Kriterium ist die Art der zur Verfügung gestellten Ressourcen und/oder deren Leistungsmerkmale – dies ist insbesondere in einem IaaS-Szenario von Bedeutung, da der Dienste-Nutzer direkt auf der zur Verfügung gestellten Infrastruktur aufsetzt. Des Weiteren muss für bestimmte Anwendungen der Standort der Ressourcen zugesichert werden.

5.1.1. Art der angebotenen Infrastruktur

Manche Anwendungen setzen gewisse Hardwareanforderungen voraus bzw. sind für diese optimiert. In diesen Fällen muss das Angebot des zukünftigen Dienste-Anbieters klar regeln, welche Hardware bereitgestellt wird. Dies bezieht sich generell auf alle Ressourcen, die kritisch für die Lauffähigkeit und Performance der darauf aufzusetzenden Anwendungen sind. Beispiele hierfür sind:

- Prozessortyp
- Hauptspeicher
- Speichermedien
- Netzwerkanbindung
- Virtualisierungsumgebung

Vor einem Wechsel empfiehlt es sich, die Kompatibilität der zur Verfügung gestellten Hardware eines Dienste-Anbieters mit den eigenen Anwendungen zu prüfen und gegebenenfalls auch zu testen, um Lauffähigkeit und ausreichende Performance sicherzustellen. Je nach Komplexität der Anforderungen und Anwendungen kann dieser Punkt viel Zeit und Kosten in Anspruch nehmen, die in der Planung entsprechend zu berücksichtigen sind.

5.1.2. Standort der Ressourcen

Neben der Art der bereitgestellten Ressourcen stellt auch die Standortfrage der Ressourcen ein wichtiges Kriterium dar. Zu bedenken sind hierbei sowohl die rechtlichen Rahmenbedingungen am Standort als auch die Verfügbarkeit der Anbindung.

Unterschiedliche Länder haben verschiedene gesetzliche Regelungen hinsichtlich gespeicherter Daten. So ist es beispielsweise US-Geheimdiensten möglich, unter gewissen Bedingungen im Rahmen des Patriot Acts auf Daten, die in den USA oder global bei US-Unternehmen gespeichert sind, zuzugreifen. Gleiches gilt im Übrigen auch für Indien und China. Daher gilt es genau zu prüfen, welche Datenschutzregelungen an dem Standort gelten.

Die Dienstverfügbarkeit hängt zum einen von der Internetanbindung des Standorts und den politischen Rahmenbedingungen des Landes ab, in dem die Server stehen. Eine stabile Internetanbindung ist eine wesentliche Voraussetzung für den erfolgreichen Betrieb und Einsatz von Cloud-Services. Die Zerstörung von Unterseekabeln im Mittelmeer im Jahre 2008 hat zu einem Wegfall von 60 Prozent der Bandbreite zwischen Indien und dem atlantischen Raum geführt. Dies hatte erheblichen Einfluss auf netzbasierte Dienste.

5.2. Kosten

Neben der Art und dem Standort der Ressourcen ist eine Transparenz bezüglich der zu erwartenden Kosten unerlässlich, um das Angebot eines potenziellen zukünftigen Dienste-Anbieters einschätzen zu können. Je nach Ausgestaltung der Dienstleistung ist eine Vielzahl von Preismodellen denkbar. An dieser Stelle werden grundlegende Vertragsbestandteile, wie die Preisgestaltung, Bonus- und Malusregeln und Ausstiegsklauseln aufgeführt, auf die ein Angebot überprüft werden muss.

5.2.1. Preismodell

Das Preismodell muss klar den Preis für eine vom Dienstleister zu erbringende Leistung sowie die zu erwartende Dienstqualität definieren. Hierbei sind die unterschiedlichsten Modelle auf Basis von Rechenzeit oder Anzahl und Ausstattung der Server denkbar. Unabhängig von der Preisgestaltung und der Eignung für einen bestimmten Anwendungsfall muss im Preismodell eine Aussage über die zeitliche Entwicklung der Preise sowie eine Regelung für das Volumen enthalten sein.

5.2.2. Bonus- und Malus-Regelungen bei Vertragsabweichungen

Ein wichtiger Punkt, der beim Vergleich der Kosten verschiedener Anbieter berücksichtigt werden muss, sind Regelungen bei Abweichungen des zu erbringenden Dienstes beziehungsweise der Dienstqualität. Beispiele hierfür sind die Art und Performance der zugesicherten Hardware oder die zugesicherte maximale Dauer bis zur Bereitstellung von neuen IT-Ressourcen. Oftmals wird das über Bonus/Malusregeln in den Verträgen geregelt. Um gegen diese Vertragsabweichungen abgesichert zu sein, ist es unerlässlich, Transparenz über diese entsprechenden Regelungen zu haben.

5.2.3. Ausstiegsklauseln

Die Auslagerung von Dienstleistungen in die Cloud sollte grundsätzlich einer längerfristig angelegten Strategie folgen. Unabhängig davon gibt es verschiedene Gründe, die einen vorzeitigen Ausstieg aus einem Dienstleistungsvertrag notwendig machen. Daher sollten die Kosten für einen (vorzeitigen) Ausstieg beider Parteien klar geregelt sein und beim Anbieterwechsel mitbedacht werden. Ein wichtiges Kriterium dabei ist, wie lange der Anbieter den Service noch gewährleisten muss, nachdem der Anwender gekündigt hat.

Die Daten gehören dem Anwender. Darum muss der Anwender die Verfügungsgewalt über seine Daten behalten. Dazu gehört die Dokumentationspflicht der Daten-Exportschnittstellen, die die Weiterführung der Daten in einer anderen Betriebsumgebung ermöglichen. Dabei sollen nach einer Kündigung bearbeitungsfähige Daten zur Verfügung stehen.

Der Anbieterwechsel besteht nicht nur aus der Übergabe der Daten, sondern kann auch das Löschen unter Fristen beinhalten, wenn der Anwender dazu schriftlich auffordert. Die Löschung sollte dann auch schriftlich bestätigt werden.

Vorsorglich sollte der Anwender für den Fall einer Insolvenz des Anbieters ausreichende Fristen vereinbaren, so dass das Risiko eines Datenverlustes minimiert wird.

5.3. Ausfallsicherheit

Grundlage für alle Arten von Cloud-Diensten, also IaaS, PaaS und SaaS ist (mindestens) ein Rechenzentrum, in welchem Software installiert, zum Ablauf gebracht und Informationen hinterlegt werden.

Eine Bewertung der Qualität und Güte eines Rechenzentrums ist wichtig. Als oberstes Qualitätsmerkmal ist hierbei die Sicherheit, speziell die Ausfallsicherheit des Rechenzentrums, zu sehen. Zum einen bestimmt sie, wie häufig und wie lange ein genutzter Dienst nicht zur Verfügung steht. Zum anderen gibt sie an, wie sicher die Daten gegen Verlust geschützt sind.

Es gibt unabhängige Organisationen, die Qualitätskriterien und Güteklassen für Rechenzentren definiert haben, siehe zum Beispiel Uptime Institute[5], oder ISO27001, und es gibt neutrale Institutionen (zum Beispiel TÜV[6]), die Rechenzentren entsprechend dieser Kriterien auditieren. Ein Nutzer sollte deshalb auf entsprechende Informationen und Verweise beim Anbieter achten.

5 Data Center Site Infrastructure Tier Standard: Topology, Uptime Institute, LLC, New York 2010.

6 TÜV Rheinland AG: Trusted Cloud Certification, Secure Data Center, Energieeffizienz im RZ. TÜViT GmbH: Trusted Site Family

Ein Nutzer von Cloud-Diensten sollte schon bei der Anbieterauswahl darauf achten, dass die Erfüllung seiner Verfügbarkeitsanforderungen keine zu große Abhängigkeit von einem einzigen Anbieter erzeugt. Diese kann entstehen, wenn der Nutzer seine Software-Architektur auf programmatische Schnittstellen aufbaut, die von nur einem Anbieter unterstützt werden. Software-Architekturen, die auf offenen Standards basieren, können einen Anbieterwechsel erleichtern.

Neben der rein statischen Analyse von programmatischen Schnittstellen und Gütesiegeln kann sich ein Nutzer von Cloud-Diensten bei kommerziellen Anbietern, wie zum Beispiel „CloudHarmony“[7], aktuelle Angaben und Messwerte zu Verfügbarkeit, Ausfallzeiten, Latenzzeiten etc. eines Cloud-Dienstes einholen.

7 www.cloudharmony.com (2011)

6. Checkliste zum Anbieterwechsel mit Fokus auf Infrastructure-as-a-Service (IaaS)

Infrastructure-as-a-Service stellt den in der Regel professionellen Nutzern die IT-Infrastruktur beispielsweise in Form von virtuellen Servern („virtual machines"), Netzen, Speicher- und Verarbeitungskapazitäten sowie Rechenleistung bereit. Ein wichtiges Kernelement ist hierbei, dass der Nutzer selbst Anwendungen und Programme nach eigenen Wünschen auf der Infrastruktur installieren und Anforderungen an die IT autonom konfigurieren kann. Die Hardware kann flexibel um Instanzen erweitert oder auch verkleinert werden (sogenannte Elastizität), um kurzfristig auf die spezifischen Anforderungen der Nutzer reagieren zu können. Dies ist ein großer wirtschaftlicher wie auch administrativer Vorteil gegenüber den traditionellen Rechenzentren, in denen systemimmanent nicht schnell auf veränderte Rahmenbedingungen, wie zum Beispiel Lastspitzen/Nachfrageveränderungen, reagiert werden kann oder Veränderungen nur mit erheblichen finanziellen Investitionen zu realisieren sind.

Die nachfolgende Checkliste soll Anhaltspunkte für Infrastructure-as-a-Service-Angebote geben, die entweder beim Einstieg in die Cloud und/oder auch vor dem Hintergrund eines Anbieterwechsels eine Rolle spielen können:

- **Welches Geschäftsmodell verfolgt der Cloud-Nutzer und welche Investitionen und Anforderungen ergeben sich daraus für ihn?**
  Letztlich muss sich der Nutzer im Klaren darüber sein, ob er mit Infrastructure as a Service-Angeboten am besten seine Ziele erreichen kann. Die Nutzung von Infrastructure-as-a-Service-Dienstleistungen setzt unter anderem voraus, dass auf der Seite des Nutzers auch Kompetenzen in der Administration von Server-Systemen bestehen. Der Nutzer übernimmt letztlich die Bespielung/Installation und Konfiguration des Systems eigenverantwortlich.

- **Werden Lastspitzen automatisiert oder durch manuellen Eingriff der Systemadministratoren abgefangen?**
  Im professionellen Alltag werden sich Schwankungen in der Nutzungsintensität der Systeme ergeben. Es kann Lastspitzen geben, an denen die Leistungsfähigkeit der Systeme ausgereizt wird. Dies kann passieren, wenn temporär eine erhöhte Nutzung zu erwarten ist. Grundlage hierfür ist die Frage, wie Lastspitzen überhaupt festgestellt werden. In diesem Zusammenhang stellt sich die Frage, inwie weit Monitoring-Instrumente zur Verfügung stehen.

- **Welcher administrative Aufwand muss durch den Nutzer betrieben werden?**
  Infrastructure-as-a-Service-Angebote ermöglichen dem Nutzer ein Höchstmaß an Freiheit in der Ausgestaltung der IT. Die IT-Infrastruktur wird in der Regel durch virtuelle Maschinen (VM) bereitgestellt. Die konkrete Ausgestaltung der Systeme durch Anwendungen oder Dienste erfolgt durch den Nutzer. Dies setzt erhebliche Kompetenzen beim Nutzer sowie auch die Bereitschaft voraus, wesentliche Aufgaben selbst zu übernehmen.

- **Wie dynamisch kann der Anbieter auf veränderte Rahmenbedingungen reagieren?**
  Der große Reiz von Cloud-basierten Lösungen ist ein Höchstmaß an Elastizität und Dynamik der Systeme. Bei veränderten Rahmenbedingungen sollte der Anbieter in der Lage sein, seinem Kunden angepasste Ressourcen zur Verfügung zu stellen. Eine zentrale Frage ist, innerhalb welchen Zeitraums sich weitere Ressourcen zur Verfügung stellen lassen (zum Beispiel die volle Rechenleistung einer neuen VM)? Hier sind kurzfristige Reaktionen immer wünschenswert.

- **Welche System-Verfügbarkeiten kann der Anbieter gewährleisten?**
  Beim IT-Einsatz stellt sich immer die Frage, in welchem Umfang System-Verfügbarkeit vom Anbieter der Dienstleistung gewährleistet werden kann. Dies hängt von den unterschiedlichsten Faktoren ab. Zentrale Bedeutung hat allerdings die Frage, wie reagiert wird, wenn unterschiedliche Elemente ausfallen. Auch hier stellt sich zunächst die Frage, auf welche Art und Weise Ausfallzeiten festgestellt und charakterisiert werden. Wesentlicher Aspekt ist hierbei, dass Infrastrukturen oder die Nutzerdaten redundant gehalten werden, um Datenverluste im Fehlerfall

oder bei Ausfall der Regelsysteme zu vermeiden. Gleichzeitig ist es wichtig, dass der Anbieter solcher Dienstleistungen den Nutzer bei der Fehleranalyse unterstützt, um so das Risiko künftiger Ausfälle zu minimieren oder ggf. Vorkehrungen zu treffen.

→ **Welche Arten der Preisbildung bestehen?**
Ein wichtiges Entscheidungs- und Unterscheidungskriterium ist immer der Preis beziehungsweise die Preissystematik beim Einsatz von Cloud-basierten-Lösungen. Wichtig ist, dass der Kunde immer nur das bezahlt, was von ihm auch wirklich genutzt wird. Dies gilt auch bei der Bereitstellung von virtueller Infrastruktur.

→ **Welche Regelungen sind im Service-Level Agreement (Cloud-Vertrag) im Falle einer Insolvenz des Cloud-Anbieters getroffen?**
Wie bereits erwähnt, müssen Regelungen getroffen werden für den Fall, dass Dienste-Anbieter von einer Insolvenz betroffen sind. Es ist immer darauf zu achten, dass der Nutzer genaue Kenntnis darüber hat, was mit seinen Daten und Programmen passiert. Dies sollte auch Bestandteil des Vertrages sein und klären, wer letztlich Inhaber der Daten und Programme ist. Gleichzeitig ist es wichtig, über mögliche Übergangszeiträume Daten von den Servern sichern zu können.

→ **Wie wird Datensicherheit und Compliance sichergestellt und dokumentiert?**
Die Bedeutung von IT-Sicherheit nimmt immer weiter zu. Aus diesem Grund sollte der Aspekt eines Höchstmaßes an Sicherheit in die Entscheidungsfindung mit einbezogen werden. Neben klassischen Fragen der physikalischen Sicherheit von Systemen gehört hierzu aber auch, dass der Anbieter sein Sicherheitskonzept dem Nutzer transparent macht und gleichzeitig auch über geltende rechtliche Regelungen informiert. Hierzu gehört auch die Frage des behördlichen Zugriffs auf die Daten des Kunden.

Mit Blick auf einen möglichen Wechsel des Infrastructure-as-a-Service-Anbieters stellt sich die Frage, in welcher Weise Daten von einer Plattform zu einer anderen übertragen werden können. Das Industrieforum DMTF[8] hat beispielsweise ein Standardformat „Open Virtualization Format“ (OVF) entwickelt, um Softwarepakete in IaaS-Cloud-Diensten ablaufen lassen zu können. Das OVF beschreibt, wie man eine Virtualisierungsumgebung mit ihren Installationen und Konfigurationen von einem Anbieter zum anderen Anbieter überträgt. Dieser Standard erleichtert einen Anbieterwechsel.

Gleichzeitig sind in einer Cloud die Schnittstellen (sog. Application Programming Interfaces (API)) wichtig. Die Prozesse in der Cloud-Ebene Infrastructure-as-a-Service (IaaS) laufen auf allen Cloud-Plattformen ähnlich ab. Die Schnittstellen (APIs), auf deren Basis dies geschieht, sind derzeit noch nicht standardisiert. Es ist aber davon auszugehen, dass sich in Zukunft unterschiedliche offene APIs auf dem Markt etablieren werden. Es gilt also bei der Auswahl des Cloud-Anbieters darauf zu achten, dass die APIs miteinander kommunizieren können oder gar „offene APIs“ sind. Ansonsten bedeutet dies für den Nutzer einen erheblichen administrativen Mehraufwand bei der Übertragung von Daten sowie Applikationen.

8 http://www.dmtf.org/

7. Sicherheit in der Cloud

Sowohl Anbieter wie Anwender müssen ihren Beitrag zur Sicherheit der Cloud leisten. Das heißt: Der Anbieter muss dafür sorgen, dass die Cloud Rechenzentren und die Datenleitung gegen Hackerangriffe aus dem Netz geschützt sind.

Der Anwender muss seinerseits für die Sicherheit der eigenen IKT sorgen. Es reicht nicht aus, sich auf eine sichere Datenleitung oder sichere Cloud-Lösung des Anbieters zu verlassen. Der Anwender muss seine eigenen Geschäftsprozesse gemäß den Anforderungen an Datenschutz und Datensicherheit ausrichten und mit Hilfe von Compliance-Richtlinien sicherstellen. Firewall und Virenschutzprogramme alleine sind für die IT-Sicherheit nicht ausreichend. Kunden müssen selbst dafür sorgen, dass bei Angriffen Daten für den Angreifer unbrauchbar sind, egal wo sie sich befinden. Dafür sorgt die Verschlüsselung der Daten sowohl bei der Übertragung in die Cloud als auch bei der Speicherung. Das dafür notwendige asymmetrische Key-Management verwaltet ausschließlich der Kunde.

Im Endeffekt kommt es auf ein schlüssiges Sicherheitskonzept bei Anwender und Anbieter an, das die spezifischen Aspekte der Cloud berücksichtigt. Da dieses Konzept auch die Geschäftsprozesse beeinflusst, ist darauf zu achten, dass bei Key-Management und Identity-Management auf gängige Industriestandards zurückgegriffen wird. Für Identity-Management sind dies „SAML“ der Organisation OASIS und „OAUTH“ der IETF (internet engineering task force. Key-Management zur Verschlüsselung ist notwendig, wenn mehrere Parteien Einblick in die Daten haben müssen. Standards hierfür hat OASIS formuliert, eine gute Einführung hat NIST veröffentlicht. Für den Fall, dass die Daten lediglich unleserlich für Dritte abgelegt werden müssen, bieten einschlägige kryptographische Softwarepakete schon ausreichend Schutz mit wesentlich weniger Managementaufwand als eine PKI-Infrastruktur (public-key-infrastruktur).

8. Ausblick

Eine zentrale Aufgabe in den nächsten Jahren wird es sein, internationale Normen und Standards für Informationssicherheit neu zu erarbeiten bzw. bestehende zu modifizieren.

Auf diesen Grundlagen können dann Plattformen, Cloud-Computing-Anbieter und deren Cloud-Computing-Services überprüft und zertifiziert werden.

Die Zukunft liegt im Cloud Computing, nicht zuletzt deshalb, weil die Welt immer mobiler wird. Wichtig dabei für die Anwender ist eine sehr genaue Prüfung, welche persönlichen Daten und Informationen er bereit ist, in eine Cloud zu geben. Für Unternehmen gilt es ebenfalls genau zu prüfen, welche Arten der unternehmenseigenen Geschäftsprozesse sich eignen, um sie in eine Cloud auszulagern. Bei diesen Überlegungen ist immer auch der Prozess der Compliance-Regelungen mit zu berücksichtigen. Wenn dies alles gründlich und gegebenenfalls auch über geeignete Assessments erfolgt, sollte den unendlichen Nutzungspotenzialen des Cloud Computings nichts mehr im Wege stehen.

9. Handlungsempfehlungen für Cloud-Anwender

1. **Analyse der eigenen IT-Prozesse unter Compliance-Aspekten**
   Der potenzielle Cloud-Anwender sollte seine eigenen IT-Prozesse genau daraufhin analysieren, welche Anwendungen und Prozesse sich für die Cloud unter Compliance-Aspekten eignen. Im zweiten Schritt ist eine sehr genaue Angebots-Prüfung erforderlich. Hierzu kann eine neutrale Experten-Beratung in der Startphase hilfreich sein.

2. **Offene Standards als Basis für größtmögliche Interoperabilität**
   Der potenzielle Cloud-Anwender sollte prüfen, ob bei ihm die erforderlichen Kompetenzen zur Konfiguration/Administration vorliegen. Bei der Auswahl eines Cloud-Anbieters sind Cloud-Angebote basierend auf offenen Standards für den Cloud-Anwender ein Garant für größtmögliche Interoperabilität.

3. **Datenübergabe bei Insolvenz des Cloud-Anbieters vereinbaren**
   Der potenzielle Cloud-Anwender sollte Vorkehrungen treffen, die gewährleisten, dass die Eigenverantwortung, zum Beispiel in Sachen Datensicherheit, erfüllt wird (beispielsweise durch Verschlüsselung).

Literaturverzeichnis

[1] BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Hg.) (2009): Cloud Computing – Evolution in der Technik, Revolution im Business. BITKOM-Leitfaden. Online verfügbar unter http://www.bitkom.org/files/documents/BITKOM-Leitfaden-CloudComputing_Web.pdf, zuletzt aktualisiert am 18.09.2009, zuletzt geprüft am 18.08.2011.

[2] Bundesamt für Sicherheit in der Informationstechnik (Hg.): Cloud Computing Grundlagen. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html, zuletzt geprüft am 18.08.2011.

[3] European Network and Information Security Agency (Hg.) (2010): Cloud Computing. Benefits, risks and recommendations für information security. Online verfügbar unter http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport, zuletzt aktualisiert am 07.01.2010, zuletzt geprüft am 18.08.2011.

[4] Mather, Tim; Kumaraswamy, Subra; Latif, Shahed (2009): Cloud security and privacy. An enterprise perspective on risks and compliance. Sebastopol, CA: O'Reilly.

[5] Mell, Peter; Grance, Timothy (2011): The NIST Definition of Cloud Computing (Draft). Recommendations of the National Institute of Standards and Technology. Special Publication 800-145 (Draft). Hg. v. National Institute of Standards and Technology. Online verfügbar unter http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, zuletzt geprüft am 18.08.2011.

[6] Wang, Lizhe; Tao, Jie; Kunze, Marcel; Castellanos, Alvaro Canales; Kramer, David; Karl, Wolfgang (2008): Scientific Cloud Computing: Early Definition and Experience. In: 2008 10th IEEE International Conference on High Performance Computing and Communications: IEEE, S. 825–830.

[7] Foster, Ian; Kesselman, Carl (2004): The grid 2. Blueprint for a new computing infrastructure. 2nd. San Francisco, Calif, Oxford: Morgan Kaufmann; Elsevier Science.

[8] Ian Foster (2008): There's Grid in them thar Clouds*. Online verfügbar unter http://ianfoster.typepad.com/blog/2008/01/theres-grid-in.html, zuletzt aktualisiert am 08.01.2008, zuletzt geprüft am 29.08.2011.

Anhang

Übersicht der Mitwirkenden der Fachinitiative „Cloud Computing“

Name	Firma
Claudia Mrotzek*	ORACLE Deutschland B.V. & Co. KG
Udo Schäfer	Alcatel-Lucent Deutschland AG
Jochen Schwarz	Alcatel-Lucent Deutschland AG
Wolfgang Dorst	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM)
Faik Karaoglu	Deutsche Telekom AG
Mark Vasic	Deutsche Telekom AG
Johannes Wust	Hasso-Plattner-Institut für Softwaresystemtechnik GmbH
Günther Diederich	Hochschule Bremen
Dr. Johannes Prade	Nokia Siemens Networks GmbH & Co. KG
Dr. Gerhard Tobermann	ORACLE Deutschland B.V. & Co. KG
Dr. Jörg-Michael Hasemann	T-Systems International GmbH
Jens Mühlner	T-Systems International GmbH
Constantin Kontargyris	TÜV Rheinland Consulting GmbH
Rainer Wirtz	TÜV Rheinland Consulting GmbH

* Leiterin der Projektgruppe

Herausgeber
Bundesministerium für Wirtschaft
und Technologie (BMWi)
Öffentlichkeitsarbeit
10115 Berlin
www.bmwi.de

Das Bundesministerium für Wirtschaft und Technologie ist mit dem audit berufundfamilie® für seine familienfreundliche Personalpolitik ausgezeichnet worden. Das Zertifikat wird von der berufundfamilie gGmbH, einer Initiative der Gemeinnützigen Hertie-Stiftung, verliehen.

Redaktion
Fachinitiative „Cloud Computing“ der AG2
„Digitale Infrastrukturen für innovative Anwendungen“

Verantwortlich
Claudia Mrotzek, ORACLE Deutschland B.V. & Co KG
Mark Vasic, Deutsche Telekom AG

Stand
November 2011

Gestaltung und Produktion
PRpetuum GmbH, München