Cloud-Dienste

Addendum zu den Empfehlungen der Kommission für IT Infrastruktur 2011-2015

Deutsche Forschungsgemeinschaft
Kennedyallee 40 · 53175 Bonn · Postanschrift: 53170 Bonn

Telefon: + 49 228 885-1 · Telefax: + 49 228 885-2777 · postmaster@dfg.de · www.dfg.de

Deutsche
Forschungsgemeinschaft
2014

Informationsverarbeitung an Hochschulen –
Organisation, Dienste und Systeme
Empfehlungen der Kommission für IT-Infrastruktur
für 2011–2015 - Addendum

Verantwortlich für den Inhalt:
Gruppe Wissenschaftliche Geräte und Informationstechnik der DFG
Fragen beantwortet:
Dr. Marcus Wilms (Tel. 0228 - 885 2471, E-Mail: marcus.wilms@dfg.de)

Bezug: Bereich Presse- und Öffentlichkeitsarbeit der DFG

Onlineversion der Empfehlungen auf den Internetseiten der DFG unter
http://www.dfg.de/wgi

Inhalt

Vorwort

Die Kommission für IT-Infrastruktur der DFG (KfR) veröffentlicht regelmäßig Empfehlungen für Planung und Betrieb der IT-Infrastruktur an Hochschulen und Universitätsklinika. Aufgrund der Aktualität des Einsatzes von Cloud-Diensten in den Hochschulen und Universitätsklinika hat sich die Kommission entschlossen zu dem Thema ein Addendum zu den bisherigen Empfehlungen von 2011-2015 zu veröffentlichen und dies nicht erst in die anstehenden nächsten Empfehlungen für 2016-2020 aufzunehmen. Das Addendum soll als Leitfaden zur Nutzung von Cloud-Diensten dienen.

1 Motivation

Die Nutzung von Cloud-Diensten ist ein wesentlicher IT Trend. Für den Betrieb von Infrastruktur ist eine Verlagerung von Rechen- und Speicherleistungen zu Anbietern von Cloud-Diensten eine interessante Alternative geworden, die Vorteile in Bezug auf Flexibilität und Kosteneffizienz verspricht. Der Trend wird aus dem privaten Umfeld unterstützt, wo Nutzer regelmäßig orts- und geräteungebunden auf Cloud-basierte Dienste zugreifen. Kommerzielle Cloud-Anbieter stellen hierfür zahlreiche attraktive Dienste und Werkzeuge bereit.

Auch im wissenschaftlichen Bereich drängt sich damit die Frage auf, inwieweit Cloud-basierte Angebote eine Alternative oder Ergänzung zu den bisherigen Infrastrukturlösungen darstellen. Daraus leiten sich Fragen an die Förder- und Finanzierungsmöglichkeiten von solchen Diensten ab, da hier ein Übergang von klassischen Investitionen und dem Betrieb von Geräten und Systemen hin zu einer Verrechnung von Dienstleistungen erfolgt.

Die Nutzung von Cloud-Diensten birgt neben Vorteilen auch Risiken in Bezug auf Sicherheit, Datenschutz und Nachhaltigkeit. Daher ist eine intensivere Betrachtung zu diesen Angeboten im Rahmen der wissenschaftlichen IT-Infrastruktur notwendig. Im Weiteren werden hierzu einige Anhaltspunkte gegeben.

2 Definition von Cloud-Diensten

Der Begriff Cloud Computing als Oberbegriff für Cloud-basierte Infrastrukturen, -Dienste und -Anwendungen wird in unterschiedlichen Kontexten verwendet. Die am häufigsten genannte Definition stammt vom NIST (*National Institute of Standards and Technology*)[1] und lautet wie folgt:

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Nach dieser Definition zeichnen sich Cloud-basierte Infrastrukturen durch folgende Eigenschaften aus:

1. Die Bereitstellung von Ressourcen erfolgt hoch automatisiert und ohne menschliche Interaktion (on-demand, self service).
2. Ein netzwerkbasierter Zugang zu Ressourcen erfolgt über standardisierte Schnittstellen.
3. Die vorhandenen Ressourcen werden dynamisch auf die anfragenden Nutzer verteilt, unabhängig von der geografischen Position der Ressourcen und der Nutzer.
4. Ressourcen können kurzfristig hinzugebucht oder freigegeben werden (Elastizität).
5. Die Ressourcennutzung wird protokolliert und abgerechnet.

Die wesentlichen Dienstmodelle sind dabei (Iaas, PaaS, SaaS):

1. *Infrastructure as a Service* (IaaS): der Betreiber stellt dem Nutzer eine Infrastruktur wie virtuelle Maschinen oder Speicher zur Verfügung. Der Nutzer hat meist keinen Einfluss auf die physikalische Infrastruktur.
2. *Platform as a Service* (PaaS): der Nutzer kann eigene Anwendungen auf vordefinierte Plattformen (Bibliotheken, Datenbanken, Computing-, Analyse-Lösungen) implementieren und muss diese nicht selbst betreiben.
3. *Software as a Service* (SaaS): in diesem Fall stellt der Betreiber eine komplette Anwendung zur Verfügung. Der Nutzer hat keinerlei Kontrolle und ggf. Kenntnis über die darunterliegende Infrastruktur oder über den Betriebsort.

[1] P. Mell, T. Grance: “The NIST Definition of Cloud Computing”, Technical Report, National Institute of Standards and Technology, 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Ein wesentliches Unterscheidungsmerkmal ist das Betriebsmodell. Hierbei wird zwischen

1. Public,
2. Private,
3. Hybrid oder
4. Community Clouds

unterschieden. Eine Public Cloud wird auf externen Ressourcen eines Anbieters betrieben und kann von einer breiten Öffentlichkeit in Anspruch genommen werden, während die Private Cloud einer a-priori definierten Gruppe von Nutzern (z.B. Mitgliedern einer Organisation) meist auf lokalen Ressourcen zur Verfügung steht.

Daneben gibt es Mischformen, bei denen Dienste z.B. innerhalb organisationsübergreifender Nutzergruppen (Community Clouds) betrieben werden, oder lokale mit externen Ressourcen verbunden werden (Hybrid Clouds).

3 Vorteile

Es ist absehbar, dass ein wachsender Bedarf an Cloud-basierten Infrastrukturen existiert. Die Vorteile sind dabei sowohl für Cloud-Nutzer als auch für Cloud-Anbieter sehr vielfältig.

Als Vorteile für die Nutzer gelten die Einsparung von Anschaffungskosten für Hard- und Software sowie die Möglichkeit einer individuellen Skalierung der benötigten Kapazitäten je nach Bedarf und ohne eine längere Bindung, wie sie sich aus einer Beschaffung von Hardware ergibt. Des Weiteren lässt sich der Aufwand für Wartung, Weiterentwicklungen, Lizenz- und Personalkosten bis auf ein Minimum reduzieren. Die Verlagerung der operativen Verantwortung auf den Cloud-Anbieter führt ebenfalls zu geringerem Zeit- und Kostenaufwand. Ein weiterer wichtiger Vorteil besteht in der möglichen Nutzung gemeinsamer Plattformen für verschiedene Einrichtungen und Nutzergruppen. So kann die Arbeit an gemeinsamen Projekten im Forschungsbereich aber auch in der Lehre bei einer dezentralen Verteilung der Nutzer durch den Einsatz gemeinsam genutzter Speicher-, Rechen- oder Bibliotheks-Clouds wesentlich vereinfacht werden. Nutzer von Cloud-Angeboten können mit geringen initialen Kosten neue Konzepte erproben und entwickeln.

Cloud-basierte Infrastrukturen bieten aber auch für den Cloud-Anbieter viele Vorteile. Sie können die Anschaffungskosten für Hard- und Software auf mehr Kunden verteilen, hochgradig standardisieren und entsprechend automatisieren. Die damit verbundene „Economy-of-Scale“ reduziert Verwaltungs- und Betriebskosten, z.B. durch erhöhte Auslastung einzelner Systeme und Optimierung von Energiekosten.

4 Risiken

Ein zentrales Problem ist die entstehende Abhängigkeit des Cloud-Nutzers vom Provider. Je mehr Daten und Dienste an einen Cloud-Anbieter verlagert werden, desto größer ist die Abhängigkeit von diesem, da ein späterer Wechsel meist aufwändig ist und erschwert wird (vendor-lock-in).

Dementsprechend ist die Beziehung zwischen Nutzer und Anbieter von Cloud-Diensten genau zu analysieren und zu bewerten. Bei der Nutzung von Cloud-Diensten sind dabei

insbesondere Aspekte zur Betriebssicherheit und Verfügbarkeit von Daten zu berücksichtigen. Die folgenden Fragen liefern hierzu Anhaltspunkte:

- Welche Sicherungsmaßnahmen gegen Datenverlust unternimmt der Anbieter?
- Wie sieht ein Notfallkonzept bei Ausfall eines Cloud-Dienstes aus?
- Wie werden Daten und Dienste gegen den Zugriff von Dritten geschützt?
- Welche Verantwortlichkeiten zum Datenschutz (Passwortstrategien, Datentransport zwischen Nutzer und Anbietern, Verschlüsselung der Daten) verbleiben beim Nutzer?
- Welche Verfügbarkeit wird garantiert?
- Wie können Daten und Dienste von einem Anbieter wieder zurück in die eigene Institution oder zu einem anderen Anbieter migriert werden (Insourcing und Providerwechsel)?
- Wie sind die rechtlichen Rahmenbedingungen für die Erbringung der Dienstleistung (z.B. welcher Rechtsstand gilt: deutsch, europäisch, Drittland)?
- Welche Durchgriffsmöglichkeiten bestehen bei Verstößen oder Insolvenz eines Anbieters?

5 Daten in der Cloud

Die Schutzziele von Daten betreffen allgemein die Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Autorisierung (Rollenkonzepte), Zurechenbarkeit, Verbindlichkeit und Revisionsfähigkeit. Für die Nutzung von Cloud-Angeboten und die Verlagerung von Daten zu einem Cloud-Anbieter muss unabhängig vom Betriebsmodell festgelegt werden, welche Schutzanforderungen bestehen und ob die Daten nach den nationalen Gesetzen geschützt werden müssen. Dies betrifft insbesondere nach Datenschutzrecht zu schützende personenbezogene Daten. Im medizinischen Umfeld sind diese Anforderungen typischerweise besonders hoch, wie z. B. bei Geninformationen, Patientenstudien, Krankheitsregister, Biomaterialdatenbanken, und unterliegen insbesondere auch noch der jeweils landesspezifischen Datenschutzgesetzgebung. Die Nutzung eines Cloud-Dienstes entspricht immer einer Auftragsverarbeitung durch Dritte, die datenschutzrechtlich nur in ganz besonderen begründeten Ausnahmesituationen erlaubt ist. Je nachdem, ob für die Nutzung bestimmter Services seitens betroffener Patienten eine schriftliche informierte Einwilligung vorliegt oder nicht sind die Daten zumindest zu pseudonymisieren oder auch vollständig zu anonymisieren. Hierbei sind jeweils aktuelle De-Identifizierungsverfahren zu verwenden. Letztendlich muss in Bezug auf die Auslagerung medizinischer Daten in eine Cloud außerhalb medizinischer Einrichtungen immer noch der Aspekt des Beschlagnahmungsschutzes berücksichtigt werden, der entfällt, wenn sich medizinische Daten nicht mehr im Gewahrsam einer medizinischen Einrichtung befinden.

Im Falle vertraulicher technischer Daten (Patente) sollte ebenso sichergestellt sein, dass keine dritte Partei Zugriff auf diese Daten erhält. Es ist zu klären, wer die Verantwortung für die Datenkontrolle einschließlich der einzelnen Schritte des Datentransfers, der Datenspeicherung und der Datenlöschung hat.

Typischerweise ist die Zusicherung und Überwachung dieser Aspekte ein Problem bei der Nutzung von Cloud-Diensten. Bei größeren kommerziellen Cloud-Providern finden sich Hochschulen und Klinika häufig in einem ungünstigen asymmetrischen Machtverhältnis, bei dem individuelle Anforderungen und Rechtsansprüche nur schwer durchzusetzen sind. Hier ist daher eine differenzierte Einzelfallbetrachtung notwendig, welche Daten welchen

Sicherheits- und Datenschutzanforderungen unterliegen und damit für den Einsatz in Cloud-Angeboten geeignet sind.

Bei einer Private Cloud-Lösung in den eigenen Rechenzentren bzw. in Community-Lösungen, bei denen die Daten bei Partnern liegen, die dem gleichen Rechtsraum zugehören und keine kommerziellen Interessen erfolgen, sind die Anforderungen an Datensicherheit und Datenschutz häufig leichter zu erfüllen. Kooperative Lösungen innerhalb des öffentlichen Wissenschaftssystems sind daher meist Angeboten von kommerziellen, externen Dienstleistern vorzuziehen.

6 Förderung durch die DFG

Bei der Beantragung von Ressourcen für Cloud-Dienste über die DFG sind einige Randbedingungen zu beachten. So kann die DFG im Rahmen ihrer Großgeräteprogramme Investitionen in Infrastrukturen empfehlen bzw. mitfinanzieren. Betriebskosten sind dabei ausgeschlossen. Da es sich bei Cloud-Diensten im rechtlichen Sinne um Dienstleistungen handelt, ist die bisherige Trennung nach Investitionen und Betriebskosten nicht oder nur eingeschränkt möglich. Es ist erkennbar, dass diese Einschränkung langfristig nicht den wissenschaftlichen Anforderungen angemessen sein wird und eine neue Betrachtung benötigt.

Die DFG kann bei Private und Community Cloud-Lösungen jedoch Investitionen in die Cloud-Infrastruktur empfehlen bzw. mitfinanzieren und damit Best Practice Modelle unterstützen.

Die Nutzung von Cloud-Diensten, etwa in DFG-Projekten, wird in der Regel aus der Grundausstattung zu bestreiten sein und kann in Analogie zur Nutzung einer Dienstleistung aus einem Rechenzentrum nicht als Ergänzungsausstattung finanziert werden. Ausnahmen bedürfen einer besonderen Begründung, die verdeutlichen muss, dass projektbezogener Mehrbedarf nötig ist, der über die Grundversorgung hinausgeht.

Künftig werden stärker die Gesamtkosten (Total Cost of Ownership) von Diensten oder Experimenten betrachtet werden müssen, um damit Dienstleistungen wie Cloud-Dienste mit reinen HW/SW-Beschaffungen vergleichbar und ggf. förderbar zu machen. Die Nachhaltigkeit und Wirtschaftlichkeit von Lösungen ist darzustellen, da die Kennwerte von öffentlichen Rechenzentren zeigen, dass kommerzielle Cloud-Lösungen typischerweise nicht kostengünstiger als eigene Betriebsmodelle sind. Dies setzt jedoch hohe Automation und eine kritische Größe für die Economy-of-Scale voraus. Entsprechend sind Community Cloud-Lösungen, die innerhalb des Wissenschaftssystems erbracht werden, Private und Public Cloud-Angeboten vorzuziehen.

Für Community Cloud-Lösungen muss ein geeigneter Rechtsrahmen für den Austausch von Leistungen etabliert werden. Hier müssen u.a. Antworten zu Fragen der Steuerproblematik, des Vergaberechts und der Verrechnung von Leistungen gefunden werden.

7 Empfehlungen

Eine Betrachtung der aktuellen technischen und rechtlichen Rahmenbedingungen zeigt, dass derzeit die Inanspruchnahme von Cloud-Diensten innerhalb eines Projektes eine sorgfältige Kosten-/Risiko-Analyse erfordert. Die Fördermöglichkeit ist aufgrund der rechtlichen Randbedingungen eingeschränkt und erfordert bei einer Beantragung eine differenzierte Stellungnahme, die u.a. folgende Punkte berücksichtigen sollte:

Bei Infrastrukturanträgen

a) Gesamtkostenbetrachtung inklusive laufender Kosten und bei Private bzw. Community Clouds auch der erforderlichen langfristigen Personalmittel. Dazu sollte eine tabellarische Übersicht über einen fünfjährigen Zeitraum aufgestellt werden.

b) Eine Betrachtung zur längerfristigen Nutzung der Cloud-Ressourcen, dem dafür zugehörigen Finanzierungsmodell und dem Ablöseszenario bei Anbieterwechsel oder Ausstieg.

Bei Projektanträgen

a) Vor einer Beantragung zur Nutzung kommerzieller Cloud-Dienste wird empfohlen, zunächst die Verfügbarkeit von alternativen Angeboten von lokalen Rechenzentren, anderen öffentlichen Einrichtungen oder Campusverbünden zu prüfen.

b) Eine Stellungnahme des lokalen RZ-Leiters bzw. eines IT-Verantwortlichen zu Art und Umfang der Ressourcennutzung sowie etwaiger alternativer Angebote (insbesondere innerhalb der Wissenschafts-Community) sollte dem Antrag beigefügt werden.

c) Eine Bewertung der jeweils geltenden datenschutzrechtlichen Anforderungen ist dem Antrag beizufügen, wenn personenbezogene Daten verarbeitet und gespeichert werden. Dies betrifft alle Betriebsmodelle von Cloud-Diensten inklusive der IT-Infrastruktur der Antragsteller.

d) Die Sicherstellung der Langzeitarchivierung und eines langjährigen Zugriffs auf die Daten ist darzustellen, insbesondere im Hinblick auf die Empfehlungen zur guten wissenschaftlichen Praxis.