Umgang mit Risiken für IT-Dienste im Hochschulumfeld am Beispiel des Münchner Wissenschaftsnetzes

Silvia Knittl
Technische Universität München
knittl@tum.de

Wolfgang Hommel
Leibniz-Rechenzentrum
hommel@lrz.de

Abstract:
Die steigenden Benutzererwartungen und Kosten zur Erbringung der komplexen IT-Dienste, die zur technischen Umsetzung und Unterstützung der Geschäftsprozesse mit hoher Servicequalität erforderlich sind, machen Ansätze wie Infrastructure, Platform bzw. Software as a Service auch für Hochschulen zunehmend attraktiv. Im Zusammenspiel zwischen Hochschulverwaltungen, zentralen Einrichtungen, Fachbereichen und Hochschulrechenzentren wurden entsprechende Dienstleistungsansätze bereits lange genutzt, bevor sie unter dem Stichwort Cloud Computing neu aufgegriffen wurden. Auf Basis des Cloud Computings sind jedoch jüngst neue Methoden und Werkzeuge entstanden, um diese Formen der Diensterbringung systematisch auf ihre Risiken hin zu analysieren; auf dieser Basis können fundierte, risikogetriebene Entscheidungen darüber getroffen werden, welche Dienste lokal erbracht bzw. zu welchen hochschulinternen oder auch externen Dienstleistern sie ausgelagert werden können. In diesem Artikel stellen wir unsere Erfahrungen mit Hochschuldiensten in diesen drei Kategorien und die mit ihnen verbundenen Risiken am Beispiel des Münchner Wissenschaftsnetzes vor. Wir stellen sie mit den an vielen europäischen Hochschulen zu beobachtenden Entwicklungen gegenüber und geben einen Ausblick auf die sich abzeichnenden Herausforderungen und Möglichkeiten in diesem Bereich.

1 Motivation

Die strategische Ausrichtung der IT-Dienste an den Kern-Geschäftsprozessen nimmt seit einigen Jahren auch auf die Hochschulinfrastrukturen massiven Einfluss. Hochgradig integrierte Campus-Management-Systeme, Groupware-Lösungen und die nahtlose Integration mobiler Endgeräte dominieren die aktuelle Weiterentwicklung der technischen IuK-Infrastrukturen und weisen an vielen Stellen Parallelen zu Entwicklungen in privatwirtschaftlichen Unternehmen auf. Mit der Nutzung der neuen technischen Möglichkeiten steigt jedoch zwangsweise auch die Komplexität der Dienste und Komponenten. Diese wiederum führt zu einer Reihe von Herausforderungen und Risiken, die sich von der Betreibbarkeit mit den vorhandenen Personalressourcen bis hin zur erforderlichen Hardwareredundanz zur Sicherstellung der prozesszielkritischen Systeme erstreckt.

Die Verlagerung des Betriebs von IT-Diensten unter Beibehaltung der vollständigen Prozesskontrolle wird deshalb auch für viele Hochschulen nicht nur finanziell attraktiv, sondern mehr und mehr auch zwingend erforderlich, um die benötigten Dienste flexibel und in der notwendigen Servicequalität zur Verfügung stellen zu können. Im Hochschulum-

feld ist – im Unterschied zu vielen privatwirtschaftlichen Szenarien – häufig eine Dreiteilung zu beobachten: Zunächst werden IT-Systeme, die die Kernaufgaben der Hochschulverwaltung direkt unterstützen, beispielsweise Studenten-, Personal-, Lehrveranstaltungs- und Prüfungsverwaltungssysteme, überwiegend von einer EDV-Abteilung der Hochschulverwaltung selbst betrieben. Ferner werden klassische netzbasierte, aber nicht zwingend hochschulspezifische Dienste wie WLAN, VPN, Mailserver, Fileserver und Arbeitsplatzsysteme vom jeweiligen Hochschulrechenzentrum bereitgestellt. Eine Kopplung der Systeme findet dabei in der Regel mindestens auf Ebene des Identity-Managements statt, um die Account-Erstellung und -Terminierung mit den Prozessen der Personal- und Studentenverwaltung zu koppeln. Schließlich existieren eine Reihe von Diensten, die bei externen Dritten in Auftrag gegeben werden. Dabei handelt es sich einerseits um Dienste, die nur von einem zu geringen Teil aller Hochschulmitglieder genutzt werden, so dass eine zentrale, hochschulweite Bereitstellung durch das Rechenzentrum nicht ökonomisch sinnvoll wäre; andererseits können für Standarddienste auch die erzielbaren Kosteneinsparungen ausschlaggebend sein, wobei sich durch den externen Ort der Datenspeicherung und -verarbeitung neue, zu beachtende Risiken ergeben.

In diesem Artikel stellen wir den Umgang mit ausgewählten Risiken für essenzielle Hochschul-IT-Dienste am Beispiel des Münchner Wissenschaftsnetzes (MWN) vor. Wir differenzieren dabei in Anlehnung an aktuelle Diskussionen unter dem Stichwort *Cloud Computing* zwischen den Kategorien *Infrastructure*, *Platform* und *Software as a Service* (IaaS, PaaS und SaaS), um eine Einordnung und Risikoeinschätzung der Hochschul-IT-Dienste vorzunehmen [ENI09]. Wir stellen deshalb im nächsten Abschnitt zunächst das MWN im Allgemeinen vor und gehen im Anschluss auf die drei Dienstkategorien und den Umgang mit den jeweiligen Risiken ein. In Abschnitt 3 stellen wir diese konkreten Ergebnisse den allgemeinen Entwicklungen an deutschen und internationalen Hochschulen gegenüber und schließen mit einem Ausblick auf die sich aktuell abzeichnenden Möglichkeiten und Herausforderungen in diesem Bereich.

2 Dienste im MWN und deren Risikomanagement

In diesem Abschnitt werden typische IT-Dienste im Hochschulumfeld am Beispiel des Münchner Wissenschaftsnetzes dargestellt. Es wird gezeigt, dass es durchaus üblich ist, Dienste auch an externe Dienstleister auszulagern – teils sogar im Sinne eines „Cloud Computings“. Risiken, die durch die steigende Komplexität beim Outsourcing entstehen, müssen entsprechend offensiv gemanagt werden. Unsere Ansätze hierfür werden ebenfalls in diesem Abschnitt dargelegt.

Das MWN ist das technische Rückgrat der Vernetzung der Hochschulen im Münchner Umkreis und wird vom Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften (LRZ) betrieben. Neben diesen Netzdiensten stellt das LRZ als gemeinsamer Dienstleister der Münchner Hochschulen auch weitere Services bereit. Abbildung 1 zeigt einen kleinen Ausschnitt typischer Dienste, welche die Mitglieder der Hochschulen in ihrer täglichen Arbeit verwenden.

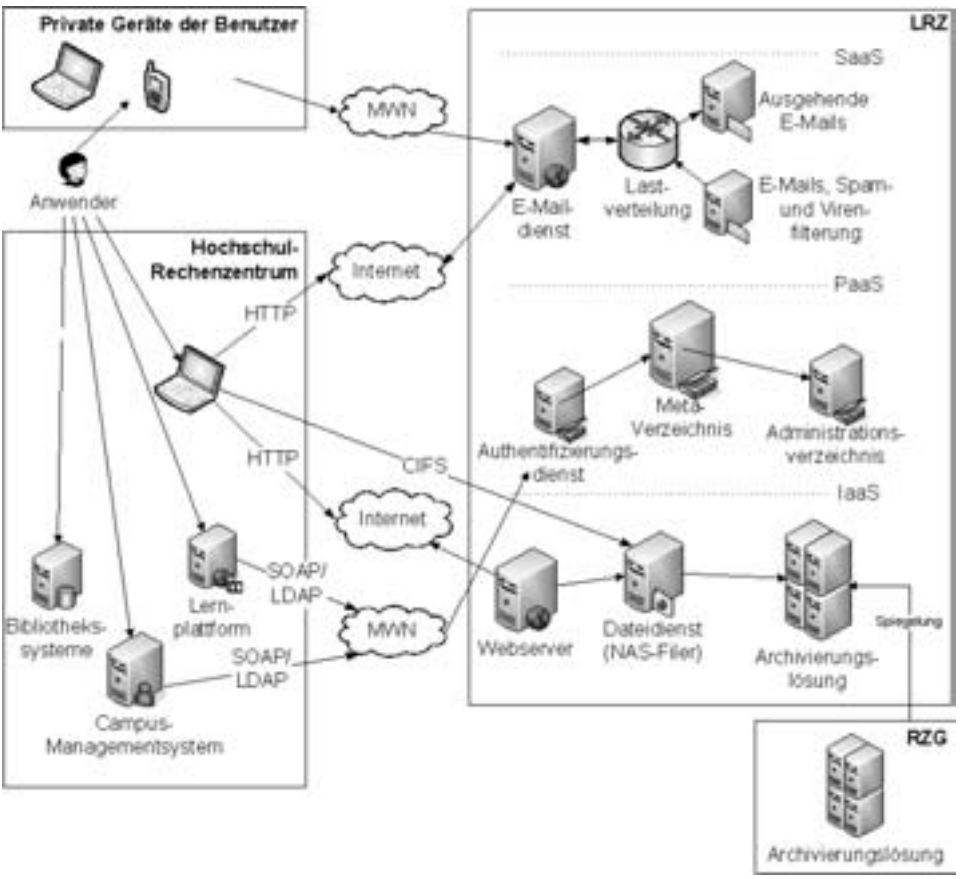

Abbildung 1: Auszug verwendeter Dienste der Benutzer im Münchner Wissenschaftsnetz

Die vom LRZ bereitgestellten Dienste in der Abbildung sind auf unterster Ebene dem Bereich IaaS zuzuordnen. Hierzu zählen flexibel zugängliche Speicherbereiche für jeden Hochschulbenutzer im Sinne eines „Storage as a Service“, aber auch Netzinfrastrukturkomponenten wie die WLAN-Zugänge. Zur Sicherstellung eines kontinuierlichen Betriebs – auch im Falle größerer Störungen – werden die Daten des Speicherdienstes zusätzlich an einen weiteren externen Dienstleister ausgelagert [HKP09]. Die nächste Ebene zeigt vereinfacht die Identity- und Access-Management-Infrastruktur (IAM), welche bedarfsgerecht in hochschulinterne Anwendungen integriert werden kann. Auf oberster Ebene stehen den Hochschulen als SaaS zu bezeichnende Dienste wie E-Mail-Lösungen oder virtuelle Webserver zur Verfügung. Die jeweiligen Grenzen zwischen IaaS, PaaS und SaaS sind dabei nicht immer scharf definiert und unterliegen der Dynamik der Weiterentwicklung des Dienstportfolios. Neben den vom LRZ zur Verfügung gestellten Diensten betreiben die Hochschulen dedizierte Lösungen für den Bereich der Studentenverwaltung (Campus-Managementsysteme) und Bibliothekssysteme. Zunehmend erwarten die Benut-

zer jedoch auch die Möglichkeit der nahtlosen Integration eigener (mobiler) Geräte wie etwa Smartphones oder Laptops in ihre Arbeitsumgebung.

Ein strukturiertes Vorgehen im Risikomanagement einer von zunehmender Komplexität gekennzeichneten IT-Infrastruktur ist hierbei der wesentliche Erfolgsfaktor. Unsere Aktivitäten folgen dem in [SGF+04] beschriebenen Vorgehen und der von ENISA (European Network and Information Security Agency) eingeführten Risikokategorisierung in organisationsbedingte, technische und allgemeine Risiken [ENI09]. Die allgemein notwendigen Schritte sind die Charakterisierung der Systeme, Identifikation von Schwachstellen und Gefährdungspotential, Bewertung der Wahrscheinlichkeit des Auftretens und die resultierenden Auswirkungen, um damit schließlich Empfehlungen zur Steuerung und Kontrolle von Risiken zu geben. Unser Vorgehen bei der Durchführung der Risikoanalyse haben wir in [Kni10] ausführlich dargelegt. Als Grundlage der Identifikation möglichst aller potentiellen Risiken bei der Verwendung von Cloud-Diensten dienten die im ENISA-Bericht aufgelisteten Risiken [ENI09]. Je höher man sich auf der Dienstestruktur (Infrastruktur–Plattform–Software) bewegt, umso mehr verlagern sich die notwendigen Risikosteuerungsaktivitäten vom Kunden bzw. Benutzer zum Provider. So stellen IaaS-Dienstleister lediglich die physische Infrastruktur und deren Grundsicherungsmechanismen zur Verfügung, wie etwa Strom, Kühlung, Firewall, während es den Kunden überlassen bleibt, für die Zugangssysteme oder das Patch-Management zu sorgen. Bei SaaS jedoch ist es auch die Aufgabe der Dienstleister, u.a. für das Patch-Management zu sorgen. Private Geräte stellen eine Besonderheit dar, da deren Management i.d.R. komplett vom Benutzer selbst übernommen wird. Tabelle 1 zeigt Auszüge der wesentlichen Ergebnisse unserer Risikoanalyse. In der linken Spalte werden die identifizierten Schwachstellen und Gefährdungen, in der rechten Spalte unsere gewählten Risikosteuerungsstrategien beschrieben.

Organisationsbedingte Risiken	**Strategie und Maßnahmen**
Obige Infrastruktur zeigt interorganisationale Abhängigkeiten. Diese sind im Falle von Störungen schwierig zu erfassen, was eine schnelle Störungsbehebung behindert.	Eine Reduzierung des Risikos kann hierbei durch eine bessere Transparenz mittels Methoden insbesondere der Softwarekartographie erfolgen.
Eine Lock-in-Situation ergibt sich durch den Einsatz dienstleisterspezifischer Entwicklungen anstelle von Standardlösungen. In unserem Fall betrifft das die IAM-Plattform. Ein Wechsel zu einem anderen Dienstleister würde mit extremem Aufwand verbunden sein.	Dieses Risiko wurde speziell im Fall des LRZs bewusst eingegangen, nachdem es die übergreifende Governance-Struktur den Hochschulen erlaubt, Einfluss auf die Leitung durch Beteiligung am Direktorium des LRZs zu nehmen.
Der Einsatz privater Endgeräte birgt Sicherheitsrisiken, da diese nicht in der Hoheit des eigenen IT-Managements sind, u.a. durch ungesicherten Zugriff auf Daten oder wenn die Geräte aufgrund mangelnder Wartung technisch nicht auf dem neuesten Stand sind.	Risikominimierung erfolgt durch Beschränkung der Zugangswege. Zugriff auf E-Maildienste mit privaten mobilen Geräten ist nur via Zertifikaten und aktivierter Datenverkehrsverschlüsselung möglich. Hierdurch werden die Vertraulichkeit, Authentizität und Integrität von Daten adäquat garantiert.

Technische Risiken	**Strategie und Maßnahmen**
Das Risiko der Überbuchung von Ressourcen kann in unserem Beispiel beim Speicherdienst auftreten, welcher von den Angehörigen der Münchner Universitäten genutzt werden kann. Ursache hierfür kann ein schlechtes Kapazitätsmanagement sein.	Splitten der Verantwortlichkeiten und des Risikos ermöglichen ein bedarfsgerechtes Kapazitätsmanagement. Speicherverantwortliche in den Hochschulorganisationseinheiten erhalten vorkontigentierte Speicherbereiche zur flexiblen Zuteilung; die globale Verantwortung des Kapazitätsmanagements liegt weiterhin beim LRZ.
Eine mangelnde Ressourcenisolation von Komponenten verschiedener Kunden, die in der gleichen Dienstleisterumgebung betrieben werden, kann zu Fehlern oder Angriffen führen. Dieses Risiko wird häufig auch in Verbindung mit virtualisierten Ressourcen gebracht.	Das Auftreten dieses Risikos wird aufgrund des Kooperationscharakters im MWN-Umfeld in unserer Umgebung als niedrig erachtet, weshalb es neben üblichen Sicherheitsverfahren keine weiteren Maßnahmen hierfür gibt.
Allgemeine Risiken	**Strategie und Maßnahmen**
Allgemeine Risiken ergeben sich durch die zunehmende Abhängigkeit von Internettechnologien. Netzstörungen können zu erheblichen Beeinträchtigungen des Normalbetriebes führen, nicht zuletzt, da die Hochschulen durch die Einführung digitaler Verwaltungsprozesse immer mehr vom Internet abhängig sind.	Aufgrund der enormen Abhängigkeit von Netzdiensten wird im Hochschulumfeld auf eine professionell gemanagte Dienstleistung wert gelegt. Diese stellt das LRZ als Netzprovider der Münchner Hochschulen durch umfassende eigene Risikomaßnahmen, wie etwa redundante Anbindung der wichtigsten Komponenten und Standorte sicher.
Der Diebstahl von Equipment ist ein Risiko, welches in jedem Unternehmen auftreten kann.	Maßnahmen sind restriktive Zugangsmechanismen des Dienstleisters durch den Betrieb in einem so genanntes „Dark Center“. Verlust persönlicher Daten kann durch Vermeidung lokaler Speichermöglichkeiten und dem Einsatz oben dargestellter Speicherlösung verhindert werden.

Tabelle 1: Auszug von Risiken bei der Verwendung von Cloud-Diensten im MWN und durchgeführte Risikosteuerungsstrategien [Kni10]

3 Ausblick

Die Auslagerung von IT-Dienstleistungen, auch in Form von Cloud Computing, eröffnet Unternehmen wie auch Hochschulen ein breites Feld an Möglichkeiten zur Flexibilisierung und Kosteneinsparung. In diesem Beitrag haben wir am Beispiel des Münchner Wis-

senschaftsnetzes, einem Verbund der Münchner Hochschulen mit dem LRZ als zentralem IT-Dienstleister, dargestellt, welche Risiken komplexe IT-Umgebungen bergen und wie sie durch ein umfassendes Risikomanagement antizipiert werden können.

Zukünftig nach [Cla08] zu erwartende Entwicklungen, wie etwa die weitere Verwendung (privater) mobiler Endgeräte, die steigende Vernetzung von Anwendungen durch Web 2.0 Technologien, die damit verbundene Zunahme von zugehörigen Content und daraus ggf. resultierende Notwendigkeit der digitalen (Langzeit-)Archivierung, die Konkurrenz durch freie Anwendungen wie Google, Wikipedia oder Disney [Kat10] erfordern, dass ein erfolgreiches wissenschaftliches Unternehmen im digitalen Zeitalter eine Versorgungsstruktur entwickeln muss, welche Flexibilität als Schlüsselmerkmal versteht. Diese Trends und auch das verstärkte Auslagern von Diensten in Richtung Cloud führen zu einer Verwässerung der traditionellen institutionellen Infrastrukturen und werden leichtgewichtigere Architekturen hervorrufen, bei denen die zunehmend mobileren akademischen Angehörigen einfach ihre Umgebung selbst zusammenstellen oder herunterladen können sollen wie in den so genannten „App Stores“ mancher Mobilfunkgerätehersteller. Eine solche Umgebung erlaubt es den Hochschulen, sich auf ihre Kernkompetenzen Forschung und Lehre zu fokussieren. Diese Entwicklungen benötigen jedoch auch eine stärkere Konzentration des Hochschulmanagements auf Governance-, Risiko- und Compliance-Themen, speziell da die im universitären Bereich notwendige offene Umgebung im Konflikt mit allgemeinen Sicherheitsansprüchen steht. So wird sich mit zunehmendem IT-Outsourcing die Rolle des CIOs verändern, indem die Gestaltung von Vertragsverhältnisse mit formalen und informellen Dienstleistern eine steigende Bedeutung bekommt.

Literatur

[Cla08] M. J. Clark. The CIO world of Higher Education in 2015. In *14th International Conference of European University Information Systems (EUNIS 2008)*, Arhus, Denmark, Juni 2008.

[ENI09] European Network and information Security Agency ENISA. Cloud Computing - Benefits, risks and recommendations for information security. Verfügbar online unter http://www.enisa.europa.eu , Zugriff am 12.01.2010, November 2009.

[HKP09] W. Hommel, S. Knittl und D. Pluta. Availability and Continuity Management at Technische Universität München and the Leibniz Supercomputing Centre. In *15th International Conference of European University Information Systems (EUNIS 2009)*, Santiago de Compostela, Spanien, Juni 2009.

[Kat10] Richard N. Katz. Scholars, Scholarship, and the Scholarly Enterprise in the Digital Age. *EDUCAUSE Review*, 45(2):44–56, 2010.

[Kni10] Silvia Knittl. Addressing Risk Management Efforts for Cloud Services at the Technische Universität München. In *6th International Conference of European University Information Systems (EUNIS 2010)*, Warschau, Polen, Juni 2010.

[SGF+04] Gary. Stoneburner, Alice. Goguen, Alexis. Feringa, National Institute of Standards und Technology (U.S.). *Risk management guide for information technology systems : Recommendations of the National Institute of Standards and Technology*. U.S. Dept. of Commerce, National Institute of Standards and Technology, Gaithersburg, 2004.