Hochschule Düsseldorf
University of Applied Sciences

HSD

Campus IT
Campus IT

CIT

ADDENDUM 2021

ZUR IKM-STRATEGIE DER HOCHSCHULE DÜSSELDORF

IMPRESSUM

Herausgeber

Autoren
Dipl.-Math. Henning Mohren
Die Mitarbeiter*innen der Campus IT

Redaktion und Ansprechpartner
Henning Mohren
CIO und Leiter Campus IT
Münsterstr. 156
40476 Düsseldorf

1 VORWORT

Die Hochschule Düsseldorf (HSD) hat mit der IKM-Strategie 2017 richtungsweisend die strategische Ausrichtung der Informations-, Kommunikations- und Medienservices (IKM) festgelegt. Die zyklische und qualitätssichernde Revision des zitierten Dokumentes hat die Gültigkeit seiner Aussagen auch im Jahr 2021 bestätigt.
Aufgrund der Aktualität von Cloud-Services und deren Implementierung sowohl in der Private Cloud der HSD als auch im Rahmen von Public Cloud Angeboten hat sich die HSD dazu entschieden, die vorliegende, im Jahr 2017 verfasste IKM-Strategie, um ein Addendum zum Thema Cloud-Computing zu ergänzen.

2 RAHMUNG DES THEMAS „CLOUD-COMPUTING“

Die Geschwindigkeit, mit der IKM-Lösungen entwickelt werden, nimmt permanent zu. Daraus ergibt sich die Herausforderung für IT-Abteilungen als Service Provider in Hochschulen, diese Lösungen zeitnah in Betrieb nehmen zu können. Mit der Umsetzung der IKM-Strategie und dem IKM-Konzept aus dem Jahr 2017 hat die Campus IT an der Hochschule Düsseldorf folgerichtig eine Private Cloud Lösung aufgebaut, auf welcher Fachbereiche im Self-Service Verfahren IKM für Forschung und Lehre (nicht IKM für den Hochschulbetrieb) in Eigenregie und ohne technische/ administrative Verzögerungen auf- und abbauen können. Die Rolle der Campus IT ist es in diesem Kontext also den Service „virtuelle Maschinen“ bereitzustellen. Dieser Service ist im Service Katalog der Campus IT als „Cumulus“ (virtuelle Maschinen im Self-Service für Fachbereiche) beschrieben. Die Campus IT fungiert hier also als „Service Provider“.

Neben den selbst zu administrierenden IKM-Services werden an der HSD zunehmend auch Services aus der Public Cloud bezogen. Treiber hierfür sind technische Entwicklungen auf Anbieterseite, z. B. die Produktentwicklung von Microsoft („M365“ und „Azure“ – bereitgestellt über den Microsoft Bundesvertrag 3.0 bzw. über das OCRE-Framework (Open Clouds for Research Environments, vertreten durch das Deutsche Forschungsnetz (DFN))), aber auch die in weite Teile der Hochschule einziehende „Digitalisierung“, die das schnelle Integrieren externer Services erfordert. Der sich stetig beschleunigende Fortschritt im Bereich der IKM mit raschen Innovationszyklen erfordert auch für die Campus IT klare Wege im Erkennen, Beschaffen und Einführen von Neuerungen. Kompetenzen im Bereich des Aufbaus einer flexiblen und sicheren IKM-Architektur gewinnen an Bedeutung im Spannungsfeld sinkender oder höchstens gleichbleibender Ressourcen. Um die Zukunftsperspektive gestalten und beherrschen zu können, sind daher dort, wo möglich, Betriebsaufgaben zu minimieren. Gerade im Falle standardisierter Services ist daher der Bezug über die Public Cloud eine gute Option.

Abgerundet wird das Thema Cloud-Computing durch die Community Cloud. Die HSD ist in unterschiedlichen Vorhaben und Kooperationsprojekten involviert – vor allem im Bereich der Digitalen Hochschule Nordrhein-Westfalen, DH.NRW. Im Rahmen dieser Kooperationen ist die HSD sowohl Servicegeber als auch Serviceempfänger. Die Services werden dabei jeweils im Rahmen einer Community Cloud erbracht. In diesen beiden Fällen wandelt sich das Aufgabenspektrum der Campus IT. Hier fungiert sie nunmehr als Service Broker.

Die in der IKM-Strategie 2017 formulierten Ziele sind daher nach wie vor gültig. Im Sinne der Umsetzung der Ziele operiert die HSD jedoch inzwischen mit einer 3-Cloud-Strategie, bestehend aus Private, Community und Public Cloud. Die Folge der 3-Cloud-Strategie ist dann sogar die Generierung von Services aus einer Hybrid Cloud.

3 CHANCEN UND RISIKEN

Der Trend, cloudbasierte IKM-Services (Public Cloud) zu konsumieren, hat im privaten Umfeld spätestens mit dem Einzug von Smartphones begonnen. Apps und die dahinter liegenden cloudbasierten Services sind konsumentenfreundlich geworden und unterstützen die Anwender*innen in allen Lebenslagen. Der mit dem Zugriff verbundene Komfort – Rechenleistungen nicht selbst bereitstellen zu müssen; ortsunabhängigen Zugriff zu besitzen; geräteunabhängigen Zugriff zu besitzen; … – verspricht daher nicht nur im privaten, sondern möglicherweise auch im kommerziellen Umfeld Flexibilität in der Bereitstellung und Konsumierung von IKM-Services bei hohen (Kosten-) Effizienzvermutungen. Naheliegend ist daher der Ansatz, (Public) Cloud-Computing als einen Aspekt der Sourcingstrategie im Hochschulkontext zu nutzen.

Mit den Vorteilen gehen jedoch auch Risiken einher. In erster Linie beziehen sich diese auf die in den Medien präsenten Themen, vor allem den Datenschutz. Problematisch mag aber auch die Bewertung von Cloud-Computing in Hinsicht der Nachhaltigkeit (der Lösung und des Anbieters) und der Anbieterabhängigkeit (vendor lock-in) betrachtet werden. Bei jedem über die Cloud bezogenen IKM-Service, sowohl in der Public als auch in der Community Cloud, ist daher im Grundsatz eine Kosten-Nutzen-Analyse durchzuführen.

Flankiert wird die hochschulinterne Entscheidung zugunsten oder zulasten der Einführung von (Public oder Community) Cloudservices stets durch eine Data-Governance. Im Vorfeld ist abzuwägen, ob die Schutzbedarfskategorie der durch den Service zu verarbeitenden Daten eine cloudbasierte Lösung (in Relation zum Anbieterprofil) zulässt oder nicht.

Auch die Betriebs- und Kostensituation ist für eine Sourcing-Entscheidung relevant. Während Cloudcomputing das Potenzial hat, Betriebskosten zu minimieren, steigen möglicherweise dennoch die Gesamtkosten (Total Cost of Ownership, TCO) – denn Cloudangebote sind möglicherweise funktionsreicher als on-premises Alternativen. Auch das ist zu hinterfragen.

Im Sinne eines klimafreundlichen Hochschulbetriebs wird bei Sourcing-Entscheidungen auch die Energieeffizienz eines Service betrachtet. Dabei ist die umwelt- und ressourcenschonende Gestaltung dessen über den gesamten Lebenszyklus hinweg entscheidender Parameter. Die Services werden daher auf Energieverbrauch hin untersucht, insbesondere bei unterbrechungsfreier Stromversorgung, benötigter Kühlung oder ähnlichen Werten. Die Campus IT trägt mit wohlüberlegten Sourcing-Entscheidungen daher durch den Betrieb von green IT aktiv zum Klimaschutz bei.

Neben den eher operativ/ technischen Merkmalen geht aber mit den neuen Aufgaben ein Wandel in der Kultur der Campus IT einher. Vom „Systembetreiber“ der Jahrtausendwende hat sich die Campus IT in den letzten Jahren zum Service Provider entwickelt. Die ganzheitliche Sichtweise auf Services, die entlang von fachgetriebenen Prozessen definiert werden, hat das Aufgabenfeld der Campus IT neu justiert – Fähigkeiten, wie Anforderungs- oder Prozessmanagement mussten neben der schon vorhandenen Kompetenz „Projektmanagement“ aufgebaut und betrieben werden. Eine neue Beratungs- und Schulungskomponente hat das individuelle Aufgabenfeld der Beschäftigten abgerundet. Mit dem Einzug der Community und Public Cloud Lösungen steht ein erneuter Wandel der Arbeitsplätze bevor. Die Beschäftigten vermitteln nun nicht mehr nur die eigenen, on-premises abgebildeten, Services. Hinzu kommen Services von Fremdanbietern, die auch dort entwickelt und gepflegt werden. Damit geht dann eine weitere Breite und Tiefe in den Beratungsdienstleistungen einher, die bis hin in Aspekte des Datenschutzes und der Informationssicherheit, der Lizenzfragen oder auch in ethische Aspekte (z.B. Einsatz künstlicher Intelligenz) reichen. Gleichermaßen reduziert wird die vor Ort benö-

tigte technische Betriebskompetenz, vor allem in der quantitativen Auslegung von Services. Trotz dieser quantitativen Anpassung müssen die qualitativen Betriebskompetenzen mit den Entwicklungen im Bereich der Public Cloud Schritt halten. Mit neuen Servergenerationen und Betriebssystemen halten dann z.B. auch Services wie Container Einzug ins lokale Datacenter. Die bevorstehende Transformation im Bereich der Beschäftigten ist also die Entwicklung von „Service Provider“ hin zum „Service Broker“. Diese findet in der kommenden Entwicklungsphase der Campus IT in verschiedenen Abstufungen statt und wird mit dem vorliegenden Addendum zur IKM-Strategie initiiert. Dabei bleibt jedoch die Komponente „Service Provider” als integraler Bestandteil erhalten, solange im Rahmen des Betriebs der Private Cloud auch hochschulspezifische, profilbildende Services angeboten werden.

Die Entwicklung hin zum Service Broker erfordert aber auch eine neue basistechnologische Ausrichtung. Allein aus Gründen der Informationssicherheit müssen Services aus dem Bereich der Community und der Public Cloud denselben Anforderungen genügen, wie jene aus der Private Cloud. Die bisher betriebenen Netzwerk- und Securitykonzepte stoßen damit an ihre Grenzen. Denn die Absicherung des Dreiklangs aus Private, Community und Public Cloud Modells etwa nach einem „Burgen und Schlösser Modell“ ist hier nicht mehr möglich. Die Campus IT wird daher ihr Securitykonzept fortschreiben und zu einem Zero-Trust-Konzept entwickeln.

4 ERWEITERTES ZIELBILD IKM

Das in der IKM-Strategie 2017 definierte architektonische Zielbild zur Systemarchitektur behält auch im Jahr 2021 noch Gültigkeit im Bereich der Private Cloud.

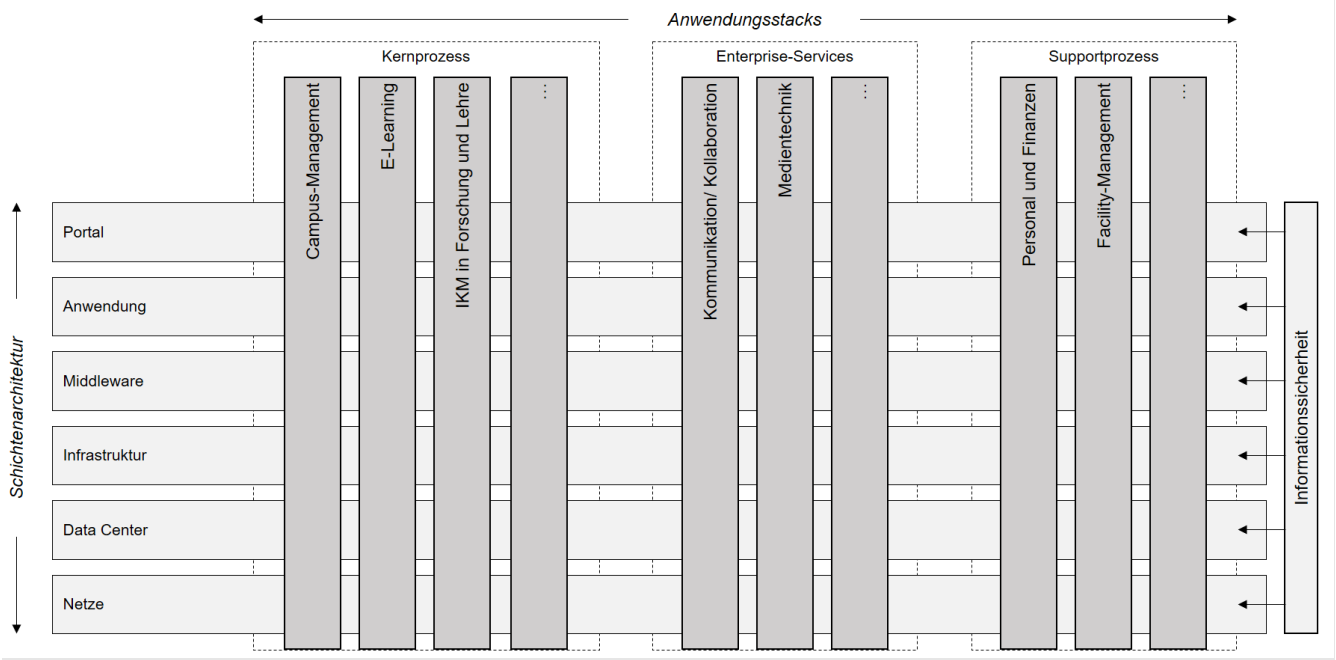

Abbildung 1: Zielbild Systemarchitektur

Es wird aber nunmehr ergänzt durch die beiden neuen Sourcing- oder Bereitstellungsmodelle der Community und Public Cloud. Letztlich entsteht dadurch für die Campus IT eine hybride Cloudarchitektur:

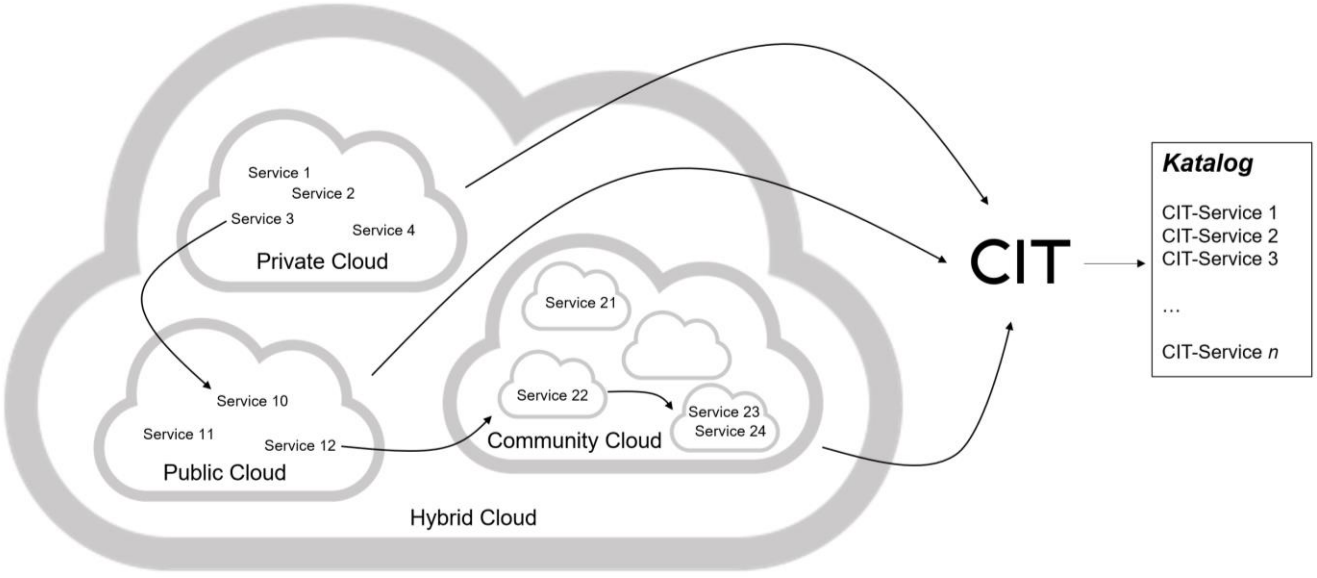

Abbildung 2: Hybrid Cloud

Die Campus IT bezieht aus den jeweiligen Clouds geeignete Services und stellt diese entlang den Anforderungen und Prozessen der Nutzer*innen als „CIT-Services“ in der Rolle des Service Brokers zur Verfügung. Die Services sind geeignet, über das Cloud Deployment-Modell hinaus zu wechselwirken. Zum Beispiel kann abstrakt Service 3 auf Service 10 zugreifen und Service 12 kann Service 23 ermöglichen. Konkret provisioniert das in der Private Cloud betriebene Identitätsmanagement hybride Identitäten in der Private und Public Cloud. Mithilfe von Public Cloud Services wird für eine korrekte Autorisierung und starke Authentifizierung bei Services in der Private und Community Cloud gesorgt.

Zur Wahrung der Informationssicherheit ist damit das bisherige Sicherheitskonzept auszudehnen und konzeptuell an den Hybrid Cloud Betrieb anzugleichen.