IT Center | RWTH AACHEN UNIVERSITY

Hand-reichung Cloudnutzung

Autoren: Guido Bunsen, Dr. Thomas Eifert, Helmut Löbner, Andreas Schreiber

Einführung

In den Angeboten der IT-Branche sind Cloud-Dienste allgegenwärtig und sehr einfach zugänglich. Die Nutzung dieser Angebote ist bei der eigenen wissenschaftlichen Arbeit als Teil des Forschungsprozesses ebenso hilfreich wie bei der IT-Umsetzung von Geschäftsprozessen jeder Art.

Weiterführende Informationen entnehmen Sie der Webseite http://www.itc.rwth-aachen.de/cloudnutzung

Gerade wegen dieser einfachen Verfügbarkeit ist es unverzichtbar, sich über Zweck, Art und Umfang der beabsichtigten Nutzung Gedanken zu machen und den Nutzen ggf. gegen den Schutzbedarf der zu verarbeitenden Daten abzuwägen. Dazu muss man sich fragen, welcher Schaden entsteht, wenn Vertraulichkeit, Integrität oder Verfügbarkeit der Daten verletzt werden. Zu solchen Schäden zählen z.B. Gesetzesverstöße, Verlust von Forschungsgeheimnissen oder Reputationsverlust. Sollen insbesondere personenbezogene Daten in Cloud-Diensten gespeichert und/oder verarbeitet werden, sind darüber hinaus die Bestimmungen der Datenschutzgrundverordnung (DSGVO) und des Datenschutzgesetz NRW (DSG NRW) zu berücksichtigen.

Das Ziel dieser Handreichung ist es, einen ersten Überblick über relevante Aspekte der Cloud-Nutzung zu geben. Im Falle von Überlegungen zur Verlagerung von Geschäftsprozessen (ganz oder in Teilen) wird dringend empfohlen, sich gezielt mit dem IT Center (für Angehörige von wissenschaftlichen Einrichtungen), dem Dezernat 5 (für Angehörige der Zentralen Hochschulverwaltung) oder dem Datenschutzbeauftragten in Verbindung zu setzen und bestehende Rahmenverträge über Cloud-Dienste bei der Auswahl zu berücksichtigen.

Für die folgenden Empfehlungen liegt ein einfaches Rollenmodell zugrunde. Es ist hilfreich, sich über die eigene Rolle und die damit verbundenen Verantwortlichkeiten im Kontext der Cloud-Nutzung klar zu sein.

- Individueller Nutzer: Jede Einzelperson, die für die eigene Arbeit oder für die Zusammenarbeit im unmittelbaren organisatorischen oder Projekt-Zusammenhang die Nutzung von Cloud-Diensten in Anspruch nimmt.
- Verantwortliche für einen Geschäftsprozess: Hiermit sind diejenigen Personen beschrieben, die Prozesse definieren, die über den individuellen Zusammenhang Einzelner hinausgehen. Dies ist ein Leiter/Geschäftsführer eines Instituts ebenso wie beispielsweise Dez. 7 für die hochschulweite Beschaffung.
- IT-Betrieb: Dies beschreibt die Personen oder organisatorisch zusammengefasste Personengruppen, die die IT-technische Umsetzung von Geschäftsprozessen verantwortungsvoll ausführen.
- Hierbei sind alle Ebenen der IT gemeint, die Person bzw. Personengruppe, die tatsächliche Administrationsaufgabe durchführt bis hin für die Organisation von IT-Prozessen zur geregelten Bereitstellung von Services zuständigen Personen.

Individuelle Nutzer

Für den individuellen Nutzer, der für sich oder als Mitglied eines Teams entscheidet, Cloud-Dienste zu nutzen, bedeutet „Cloud“ vor allem, dass er sich in eine Abhängigkeit von einem Anbieter begibt. Damit übergibt er möglicherweise besonders zu schützende Daten an Dritte.

Stand: 03. Mai 2019

Vorher zu prüfende Aspekte sind:

- Klärung des Schutzbedarfs der Daten (s.o.) im Hinblick auf die Vertraulichkeit, Verfügbarkeit und Integrität der Daten
- Sorgfältige Auswahl des Cloud-Anbieters unter Berücksichtigung seines Geschäftsmodells und der Vertragsgestaltung.

Verantwortliche für einen Geschäftsprozess

Die Verantwortung für einen Geschäftsprozess ist auf der organisatorischen bzw. Leitungs-Ebene angesiedelt. Entsprechend bestehen Fragestellungen hinsichtlich der Eignung eines bestimmten Angebots für den jeweiligen Prozess. Diese Fragestellungen bestehen i.d.R. unabhängig von konkreten IT-technischen Umsetzungen.

Zur Vorbereitung der Auslagerung von IT Ressourcen, die Geschäftsprozesse in der eigenen Verantwortung betreffen, müssen diese Aspekte in Betracht gezogen werden:

- Definition und Kontrolle der Sicherheitsanforderungen (Schnittstellen, Schutzniveau der Daten und Berechtigungen).
- Sorgfältige Auswahl und Vertragsgestaltung mit einem geeigneten Dienstleister unter rechtzeitiger Beteiligung der Personalvertretungen.
- Planung der geordneten Beendigung des Auftragsverhältnisses sowie der Notfall-Szenarien z.B. nicht beeinflussbarerer Beendigung, Ausfall oder Versagen des Dienstes u.ä..
- Prozessbezogenes Sicherheitskonzept auf Seiten der RWTH in Abstimmung mit dem projektspezifischen Sicherheitskonzept des Dienstleisters.
- Sichere Migration der Daten zum Dienstleister und sichere Rückholung der Daten.

Für die Gebrauchsphase von Cloud-Diensten verantwortet er die Servicedefinition durch die Anwender („Wo liegt der Nutzen?“).

Sofern der angedachte Cloud-Dienst als Teilprozess einer weiteren Prozesskette dient, verantwortet er die sichere Einbindung.

- Erstellung des Notfallkonzeptes für den genutzten Clouddienst, die
- Aufrechterhaltung und Nachweis der ausreichenden Informationssicherheit in der laufenden Cloud-Nutzung.
- Richtlinien für die Fernwartung.

IT Betrieb

Für die Personen und Organisationseinheiten, die für den Betrieb von Cloud-Anwendungen verantwortlich sind, bedeutet „Cloud“ vor allem eine Umstellung bei der Wartung dieser Anwendungen. Dies erfordert

- Erstellung eines Notfallkonzeptes für einen Cloud-Dienst

Da die Systeme nicht mehr im physischen Zugriff sind müssen – bei entsprechenden Anforderungen an die Verfügbarkeit – Maßnahmen vorbereitet werden, um den Betrieb aufrecht zu erhalten und/oder den Datenbestand zu sichern.

Darüber hinaus bedingen regelmäßig anfallende administrative Aufgaben den Zugriff auf die Anwendungen und die darunterliegenden Systeme den Zugriff über das Internet. Der Auswahl geeigneter Werkzeuge, gesicherter Verbindung und Authentifizierung kommt damit erheblich höhere Bedeutung zu als beim Zugriff über das gut geschützte Instituts-LAN. Einzelne Aspekte sind:

- Planung des Einsatzes der Fernwartung
- Sicherer Verbindungsaufbau und Absicherung der Kommunikationsverbindungen
- Regelungen zu Kommunikationsverbindungen und Dokumentation
- Sichere Protokolle und kryptographische Verfahren
- Auswahl und Verwaltung geeigneter Fernwartungswerkzeuge
- Datensicherung der Cloud-Anwendung