Technische Hochschule Brandenburg
University of Applied Sciences

07.12.2017 **Amtliche Mitteilungen der Technischen Hochschule Brandenburg** **25. Jahrgang**
Nummer 34

Datum	Inhalt	Seite

Herausgeber
Die Präsidentin
Technische Hochschule Brandenburg
Körperschaft des öffentlichen Rechts

Technische Hochschule Brandenburg
Magdeburger Str. 50
14770 Brandenburg an der Havel
T +49 3381 355 – 0, F +49 3381 355 - 199

Richtlinie zur Auslagerung von Daten in die Cloud (Cloudrichtlinie)[1]

Inhaltsverzeichnis

[1] Basierend auf dem entsprechenden Dokument der FU Berlin vom 2. Dezember 2011

1 Einleitung

Diese Richtlinie beinhaltet grundsätzliche Regelungen für alle Mitglieder der Hochschule, die im Rahmen ihrer dienstlichen Tätigkeit öffentliche Cloud-Dienste (so genannte Public Clouds) zur Datenablage nutzen wollen. Sie informiert über allgemeine Risiken und hilft bei der Klärung der Frage, in welchen Fällen oder unter welchen Bedingungen Cloud-Dienste genutzt werden dürfen.

Wenn Daten mit Hilfe von Cloud-Diensten gespeichert oder verarbeitet werden, drohen spezielle Gefahren. Insbesondere die dynamische Verteilung der Speicherkapazitäten über verschiedene Standorte, die in der Regel dem Nutzer nicht bekannt sind, verlangen eine spezifische Vorsorge hinsichtlich der Informationssicherheit und des Schutzes der Daten.

Für die Verarbeitung personenbezogener Daten in der Cloud gelten die Bestimmungen des Brandenburgischen Datenschutzgesetzes (BbgDSG). Es fordert entweder die Einwilligung der Betroffenen (im Fall der Datenverarbeitung außerhalb der EU), oder die Anwendung der Regelungen zur Auftragsdatenverarbeitung (Datenverarbeitung innerhalb der EU).

Im privaten Umfeld werden Cloud-Dienste häufig relativ sorglos genutzt. Vor dem Hintergrund der sich immer mehr auflösenden Trennung von privaten und dienstlichen Belangen, speziell im IT-Umfeld, soll diese Richtlinie zur Sensibilisierung gegenüber den potentiellen Risiken beitragen und entsprechende Handlungsanleitungen geben.

Sollten Sie bei der Entscheidungsfindung Beratungsbedarf haben, können Sie sich an das Rechenzentrum der Hochschule wenden.

2 Geltungsbereich

Diese Richtlinie gilt für alle Mitglieder und Angehörigen der Hochschule, wenn sie im Rahmen dienstlicher Tätigkeiten für die Hochschule Daten erheben, speichern oder verarbeiten.

3 Abgrenzung und Begriffsdefinition

IT-Dienste, die unabhängig von Ort und Zeit über ein Daten- oder Kommunikationsnetz genutzt werden können, werden allgemein als „Cloud Computing" bezeichnet. Allerdings existieren verschiedene leicht variierende Definitionen des Begriffs. Im Folgenden benutzen wir eine Begriffsdefinition, die sich an die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) festgelegte Definition des Begriffs Cloud Computing anlehnt:

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. In der Regel können diese IT-Dienstleistungen unabhängig von Ort und Zeit mit Hilfe aller gängigen IT-Geräte genutzt werden. Für die Nutzer bleibt die bereitgestellte IT-Infrastruktur verborgen [Bundesamt für Sicherheit in der Informationstechnik (BSI), „Eckpunktepapier Sicherheitsempfehlungen für Cloud Computing Anbieter", [Online].
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/EckpunktepapierSicherheitsempfehlungen-CoudComputing-Anbieter.pdf].

IT-Dienste werden dabei als:

- Infrastruktur-Dienste (Speicher- oder Serverkapazität)
- Plattform-Dienste (Betrieb eigener Anwendungen oder Entwicklungsumgebungen auf externen Servern)
- Software-Dienste (Anbieter stellt Software zur Verfügung)

angeboten.

Für den Betrieb der Dienste werden vier Modelle unterschieden:

- Private Cloud (Betrieb des Dienstes in der eigenen Organisation),
- Community Cloud (gemeinsamer Betrieb der Dienste in einem Verbund),
- Public Cloud (Betrieb des Dienstes durch externe Anbieter),
- Hybrid Cloud (Mischform Private Cloud und Public Cloud zur Leistungserhöhung).

Diese Richtlinie betrachtet Aspekte der Speicherung von Daten, die kurzzeitig oder längerfristig über IT-Dienste der Cloud erstellt und verarbeitet werden.

4 Datenkategorien und ihre Eignung zur Cloud-Nutzung

Für die Entscheidung, unter welchen Bedingungen eine Auslagerung von Daten in die Cloud in Frage kommt, bildet der Schutzbedarf der Daten die grundlegende Richtschnur. Hinweise auf den Schutzbedarf können zum einen aus der systematisch durchgeführten Schutzbedarfsanalyse und zum anderen aus der Datenkategorie abgeleitet werden. Daten lassen sich in die folgenden Kategorien einteilen:

Kategorie	**Hinweis auf typischen Schutzbedarf**
Daten, die aus öffentlich zugänglichen Quellen stammen	keinen
Allgemeine Daten aus dem Bereich der Lehre (z. B. Lehrskripte, Projektpräsentationen, Versuchsanleitungen)	normal
Dienstliche (nicht wissenschaftliche) Daten aus den Bereichen Lehre (z. B. Prüfungsergebnisse, Klausuren, Lehrplanung, Lehrabrechnung, EDL, u.a.m.) und Verwaltung (z. B. Haushaltsdaten, Leistungsbeschreibungen, Verträge u. a. m.)	hoch bis sehr hoch
Wissenschaftliche Daten mit offener Lizenz	keinen
Wissenschaftliche Daten, sofern sie für Dritte nicht interpretierbar sind	normal
Wissenschaftliche Daten mit Geheimhaltungsbedarf	sehr hoch
Personalaktendaten, personenbezogene Daten	sehr noch

In jedem Fall sind die folgenden Aspekte zu beachten:

- Für personenbezogene Daten (sowohl mit dienstlichem als auch privatem Bezug) gelten die Bestimmungen des Datenschutzes. Sie besitzen einen sehr hohen Schutzbedarf.

- Auch Daten ohne Personenbezug können einen sehr hohen Schutzbedarf haben (z. B. auf Grund von Geheimhaltungsvereinbarungen).

Ein Schutzbedarf wird grundsätzlich hinsichtlich der drei Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit differenziert bestimmt. Entsprechend differenziert müssen Vorkehrungen zur Sicherheit der Daten getroffen werden. Aus dem Schutzbedarf der Daten folgt zwingend die Eignung oder Nicht-Eignung für eine Speicherung in der Cloud:

Kategorie	**Eignung**
Daten ohne oder mit normalem Schutzbedarf	Für Ablage geeignet.
Daten mit hohem Schutzbedarf	Nur für die verschlüsselte Ablage geeignet.
Daten mit sehr hohem Schutzbedarf	Nicht für die Ablage geeignet.

Insbesondere dürfen die folgenden Daten nicht in der Cloud abgelegt werden:

Personalaktendaten	Nicht für die Ablage geeignet.
Dienstliche Daten mit Personenbezug	Nicht für die Ablage geeignet.
Haushaltsdaten	Nicht für die Ablage geeignet.

5 Regelungen

Bevor Daten in einer Cloud abgelegt werden, müssen die im vorangegangenen Abschnitt 4 betrachteten Abhängigkeiten zwischen der Datenkategorie, dem Schutzbedarf der Daten und der Eignung brachtet werden. Darüber hinaus gelten die in diesem Abschnitt aufgestellten Regelungen.

- *Vorrangig Dienste der Hochschule nutzen*
  Services, die jetzt oder zukünftig von der Hochschule bereitgestellt werden, sind Cloud-Diensten externer Anbieter vorzuziehen. Nur wenn der benötigte Dienst nicht von der Hochschule bereitgestellt wird oder der bereitgestellte Dienst den Anforderungen nicht genügt, darf unter Beachtung der hier formulierten Grundsätze auf Angebote externer Anbieter zurückgegriffen werden. Die aktuell verfügbaren Dienste der Hochschule sind Bestandteil des Dienste-Katalogs und können über das Rechenzentrum erfragt werden.

- *Vorrangig Dienste des DFN nutzen*
  Können Cloud-Dienste der Hochschule nicht genutzt werden, sind Services des DFN oder Dienste von Hochschulverbünden (Community Cloud) den Diensten kommerzieller Anbieter (Public Cloud) vorzuziehen.

- *Dienste in der Public Cloud*
  Werden Dienste kommerzieller Anbieter genutzt, sind für die Authentisierung grundsätzlich andere Passwörter als an der Hochschule (IDM-Zugang) zu verwenden. Für die Datenübertragung über öffentliche Netze sind verschlüsselte Übertragungsprotokolle zu nutzen. Vertragliche Regelungen kommen jeweils zwischen der Nutzerin oder dem Nutzer und dem Dienstanbieter zustande. Treten jeweils einzelne Nutzerinnen oder Nutzer in Vertragsverhältnisse, ist die Haftung der Hochschule gegenüber dem Anbieter und Dritten ausgeschlossen.

- *Schutzbedarf der Daten bestimmt den Umfang der Cloud-Nutzung*
  Aus dem Schutzbedarf der für eine Auslagerung vorgesehenen Daten folgt nicht nur, ob eine Auslagerung zulässig ist, sondern auch unter welchen Bedingungen dies geschehen kann. Dabei ist der Schutzbedarf getrennt nach den drei Schutzzielen Verfügbarkeit, Integrität und Vertraulichkeit zu betrachten:

1. Verfügbarkeit

   Es muss vorab geprüft werden, welche Aussagen der Anbieter des Cloud-Dienstes zur Verfügbarkeit macht. Wenn sehr hohe Anforderungen an die Verfügbarkeit gestellt werden, kommt eine Datenablage in der Cloud nur in Frage, wenn der Anbieter des Cloud-Dienest eine sehr hohe Verfügbarkeit garantiert.

   Es muss sichergestellt werden, dass das Eigentum der dienstlichen Daten an der Hochschule liegt. Wird der Cloud-Service nicht mehr genutzt oder scheidet die Primärnutzerin oder der Primärnutzer des Cloud-Dienstes aus der Hochschule aus, ist die weitere Verfügbarkeit der Daten für die Hochschule sicherzustellen.

2. Integrität

   Die Unverfälschbarkeit der Daten (Integrität) wird im Allgemeinen von Anbietern von Cloud-Speichern nicht garantiert. Wenn in dieser Hinsicht hohe oder sogar sehr hohe Anforderungen bestehen, muss die Nutzerin oder der Nutzer selbst geeignete Maßnahmen zur Gewährleistung der Integrität ergreifen. Beispielsweise können Prüfsummen verwendet werden, mit deren Hilfe eine Veränderung an den Daten erkannt werden kann. In Systemen zur Datenverschlüsselung (siehe folgender Absatz) sind derartige Verfahren in der Regel bereits integriert.

3. Vertraulichkeit

   Wenn hohe Anforderungen an die Vertraulichkeit gestellt werden, ist als adäquate Maßnahme der Einsatz eines Datenverschlüsselungssystems zwingend notwendig. Viele Anbieter von Speicherplatz in der Cloud bieten auch Dienste zur Datenverschlüsselung an. Bei der Nutzung dieser Verschlüsselungsdienste ist in der Regel nicht zuverlässig nachvollziehbar, wer Zugriff auf die Schlüssel und damit auf die Daten hat. Der Zugriff des Dienstanbieters auf die Schlüssel muss ausgeschlossen sein. Darum sollte die Verschlüsselung selbst vorgenommen werden, bevor die Daten in die Cloud übertragen werden. Die Sicherheit verschlüsselter Daten hängt u. a. von der Qualität des Verschlüsselungsalgorithmus, der Verschlüsselungssoftware, der Schlüssellänge und dem Schlüsselmanagement ab. Beim Einsatz von Verschlüsselung muss darauf geachtet werden, dass sie nach allgemein anerkannten Regeln als sicher gilt.

   Bei Daten mit sehr hohen Anforderungen an die Vertraulichkeit ist grundsätzlich von der Ablage in der Cloud abzusehen. Wenn in sehr seltenen Fällen dennoch derartige Daten in die Cloud ausgelagert werden müssen, sind die Daten zwingend vorher zu verschlüsseln. In diesem Fall sollte die Verschlüsselung inklusive des Schlüsselmanagements mit Unterstützung des Hochschulrechenzentrums erfolgen.

- *Löschung von Daten*
  Es ist vorab zu prüfen, welche Aussagen der Anbieter des Cloud-Dienstes zum Löschen von Daten trifft. Anbieter von Cloud-Speicher setzen verschiedene Speichertechniken und Archivierungslösungen ein. Aufgrund dieser Speichertechniken werden Daten oft erst nach einer gewissen Zeitspanne oder Archivierungsfrist gelöscht. Grundsätzlich kann nicht ausgeschlossen werden, dass beim Absetzen des Löschbefehls die Daten lediglich für den Anwender ausgeblendet, aber nicht gelöscht werden. Daher sind Daten, die beispielsweise einer gesetzlichen Löschverpflichtung unterliegen, für die Ablage in der Cloud ungeeignet. Nach Vertragskündigung mit einem Cloud-Anbieter muss sichergestellt sein, dass die Nutzerdaten vollständig gelöscht wurden.

- *Dienstrechtliche Vorgaben beachten*
  Insbesondere für Daten der Verwaltung (vor allen Dingen Personal-, Gesundheits- und Haushaltsdaten) existieren oft detaillierte Vorschriften, wie mit diesen Daten umzugehen ist. Beispielsweise regeln verschiedene Vorschriften, dass Personalakten die Personalabteilung nicht ohne weiteres verlassen dürfen. Somit dürfen derartige Personaldaten auch nicht auf Speicher außerhalb der Hochschule abgelegt werden. Inwieweit bei der Datenspeicherung dienstrechtliche Vorschriften zu beachten sind, muss im Zweifel, unter Einbeziehung des jeweiligen Vorgesetzten, geklärt werden.

- *Sparsamer Umgang*
  Prinzipiell sollten bei der Nutzung entsprechender Cloud-Dienste die in Frage kommenden Datenmengen auf das notwendige Mindestmaß begrenzt werden. Beispielsweise kann bei der Übertragung ganzer Verzeichnisbäume leicht übersehen werden, dass in einem Unterverzeichnis sensible Daten abgelegt wurden, die den Bereich der Hochschule nicht verlassen dürfen.
  Cloud-Dienste unterliegen zudem einem Geschäftsmodell und sind kostenpflichtig. Bevor Daten auf Speichersysteme externer Anbieter ausgelagert werden, müssen erwarteter Nutzen, Risiken und Kosten gegeneinander abgewogen werden.

- *Allgemeine Empfehlungen*
  Ergänzend zu den zuvor angesprochenen Themenbereichen sollten noch weitere Punkte beachtet werden.

    - Cloud-Betreiber mit Firmensitz außerhalt der EU

      Ein Umgang mit den Daten der Kunden gemäß den europäischen Datenschutzbestimmungen kann hier nicht vorausgesetzt werden. Insbesondere ist häufig unklar, welche Personen oder welche Stellen Zugriff auf die Daten erlangen. Für die Übermittlung personenbezogener Daten sind besondere Datenschutzvorschriften einzuhalten.

    - SLA (Service-Level-Agreement) bzw. AGB (Allgemeine Geschäftsbedingungen) des Anbieters

      Vor der Inanspruchnahme eines Dienstes müssen die (vertraglichen) Bedingungen, unter denen der Dienst genutzt wird, bekannt und akzeptabel sein. Hinweis: Die AGB der Anbieter können sich ändern und sollten deshalb regelmäßig überprüft werden.

- Zertifizierung des Anbieters

  Wie ernst ein Anbieter die Sicherheit und den Schutz der Kundendaten nimmt, kann u. a. an dem Vorhandensein von anerkannten Prüfbescheinigungen (beispielsweise ISO 27001, entspricht BSI 100-1) abgelesen werden.

- Hinweise zu einer sicheren Cloud-Nutzung, zu Gefährdungen und Sicherheitsmaßnahmen können dem Baustein B1.17 des BSI-Grundschutzkatalogs entnommen werden.

6 Zusammenfassung

Der folgende Fragenkatalog soll bei der Eignungsprüfung des Cloud-Angebots helfen.

1. Wurde das Angebot innerhalb der Hochschule geprüft?
   Ist ein Hochschul-Service zur Ablage der Daten geeignet?

2. Wurden die Vertragsbedingungen, SLA (Service-Level-Agreement) bzw. AGB (Allgemeine Geschäftsbedingungen) des Anbieters angesehen?
   Passen die Bedingungen des Anbieters zu den Anforderungen?

3. Erfüllt der Cloud-Dienst die Anforderungen an die Verfügbarkeit der Daten?

4. Stellt der Nutzer die Verfügbarkeit der Daten für die Hochschule sicher?

5. Erfüllt der Cloud-Dienst die Anforderungen an die Integrität der Daten?
   Wurden Vorkehrungen getroffen, hohe Integritätsanforderungen zu erfüllen?

6. Gestatten die Anforderungen hinsichtlich der Vertraulichkeit der Daten eine unverschlüsselte Ablage in die Cloud?
   Werden sichere Protokolle bei der Datenübertragung über öffentliche Netze verwendet?

7. Wenn die Anforderungen hinsichtlich der Vertraulichkeit der Daten nur eine verschlüsselte Ablage in der Cloud erlauben:
   - Wird die Verschlüsselung vor der Abspeicherung durchgeführt?
   - Werden die Schlüssel im Bereich der Hochschule abgelegt?

8. Wenn personenbezogene Daten in der Cloud abgelegt werden sollen:
   - Dienstliche personenbezogene Daten dürfen nicht in der Cloud abgelegt werden.
   - Wurde geprüft, ob alle datenschutzrechtlichen Anforderungen, insbesondere hinsichtlich der Auftragsdatenbank, erfüllt sind?

9. Wurde geprüft, ob gesetzliche oder andere Vorschriften die Ablage der Daten auf Systemen außerhalb der Hochschule erlauben?

10. Wurde geprüft, ob die Daten bestimmten Löschfristen unterliegen?
    Genügen die vom Cloud-Dienstanbieter bereitgestellten Dienste diesen Anforderungen?

Neben den Auswahlkriterien Vertraulichkeit, Verfügbarkeit, Integrität können weitere Aspekte die Wahl des Anbieters bzw. des Cloud-Services beeinflussen. Diese Aspekte adressieren mit den Eigenschaften

- Performance,
- Bedienbarkeit und Handhabung der Anwendung sowie
- der Eignung für bestimmte Aufgaben

nicht primär Anforderungen des Datenschutzes und wurden daher nicht in der Richtlinie behandelt.

Die Nutzung von Cloud-Services ist ein moderner und zukunftsorientierter IT-Prozess. Er gewinnt zunehmend Bedeutung für unsere Hochschule. Die Ständige IT-Kommission der Hochschule hat sich für die Förderung von Cloud-Lösungen ausgesprochen. Die Hochschule wird diesen Prozess weiter aktiv gestalten.

7 In-Kraft-Treten

Die Cloudrichtlinie tritt am Tage nach ihrer Veröffentlichung in den Amtlichen Mitteilungen in Kraft.

Brandenburg an der Havel, 07.12.2017

gez. Prof. Dr.-Ing. Burghilde Wieneke-Toutaoui
Präsidentin