Empfehlung für die Verwendung von Cloud Speicherdiensten

Guido Bunsen, IT Manager Security, IT Center, RWTH Aachen University

Cloud-Speicherdienste ermöglichen Anwendern persönliche Dateien im Internet zu sichern und lokal zu synchronisieren. Durch dieses Prinzip ist es besonders einfach geworden, Dateien auf mehreren Geräten ohne nennenswerten Aufwand synchron zu halten.

Ein weiteres Merkmal dieser Dienste ist das Teilen von Dateien und Ordnern mit anderen Nutzern, sodass diese Daten auch über mehrere Nutzer hinweg synchronisiert bleiben.

Ein erhebliches Problem jeglicher Cloud-Dienste ist allerdings die Sicherheit der Daten. Da die Server der meisten Anbieter im Ausland stehen, fallen die dort gespeicherten Daten nicht unter das deutsche Datenschutzgesetz. Und obwohl stets versichert wird, dass die Daten verschlüsselt gespeichert werden und die Anbieter keinen Zugriff haben, ist es für den einzelnen Anwender nicht nachprüfbar.

sciebo – Cloudspeicher der NRW Universitäten

Eine Alternative bietet der Dienst sciebo. Er wird durch ein Konsortium nordrhein-westfälischer Hochschulen unter der Führung der Westfälische Wilhelms-Universität (WWU) Münster bereitgestellt. Die Daten werden ausschließlich an drei Universitäten in NRW verarbeitet, und zwar in Münster sowie in Bonn und Duisburg-Essen. Dadurch, dass sciebo seinen Sitz in NRW hat, gilt das deutsche Datenschutzgesetz – eines der strengsten weltweit.
Diese Handreichung soll den Angehörigen der RWTH Aachen eine Hilfestellung bieten, wenn es darum geht, welche Daten in sciebo abgelegt werden dürfen und welche nicht.
Der Endnutzer kann sciebo über einen Webbrowser (Up- and Download) oder über einen lokalen Client nutzen.

Nutzungsbedingungen und Eigenschaften der zu speichernden Informationen

Um sciebo nutzen zu können, muss der Anwender den Nutzungsbedingungen[1] zustimmen. Wesentliche Aussagen sind u. a., dass die Nutzung ausschließlich für Studium Lehre, Forschung oder Verwaltung zulässig ist. Weiterhin ist festgelegt, dass „ausschließlich solche personenbezogenen Daten von weiteren Personen neben dem Endnutzer in den Dienst gegeben werden“ dürfen, „für die eine Einwilligung der Betroffenen besteht oder für die ein gesetzlicher Erlaubnistatbestand greift.“
Das bedeutet, dass eine Ablage personenbezogener Daten, wie z. B. Bewerbungsunter-lagen, nicht gestattet ist.

Für die weitere Beurteilung ob Daten für die Speicherung in sciebo geeignet sind, ist der Schutzbedarf der Daten von Bedeutung. Dieser kann „normal“, „hoch“ oder „sehr hoch“ sein.
Die folgende Tabelle bietet einen ersten Anhaltspunkt. Eine vereinfachte Anleitung zur Bestimmung des Schutzbedarfs im Kontext von sciebo ist im Anhang aufgeführt.

[1] sciebo Nutzungsbedingungen, abgerufen am 6. Januar 2016 von https://www.sciebo.de/agb/index.html

Ursprung der Daten	**Typische Schutzbedarfskategorie**
Daten aus öffentlich zugänglichen Quellen	„normal“
Dienstliche nicht wissenschaftliche Daten (z. B. Prüfungsergebnisse, Gutachten)	„normal“ bis „sehr hoch“
Wissenschaftliche Daten (z. B. Untersuchungsergebnisse, vertrauliche Forschungsdaten)	„normal“ bis „sehr hoch“
Personalaktendaten	„sehr hoch“

In jedem Fall sind die folgenden Aspekte zu beachten:

- Für personenbezogene Daten gelten die Bestimmungen des Datenschutzes, d. h. für die Speicherung ist die Zustimmung des Betroffenen erforderlich (informationelle Selbstbestimmung)
- Auch Daten ohne Personenbezug können einen sehr hohen Schutzbedarf haben, z. B. auf Grund von Geheimhaltungsvereinbarungen.

Aus dem Schutzbedarf von Daten folgt zwingend die Eignung oder eben Nicht-Eignung zur Ablage in sciebo:

Schutzbedarfskategorie der Daten	**Eignung zu Ablage in sciebo**	**Eignung für andere Cloud-Dienste**
„normal“	Ja	Nur in Ausnahmefällen
„hoch“	Nur verschlüsselt	Nein
„sehr hoch“	Nein	Nein

Teile dieser Empfehlung wurden mit freundlicher Erlaubnis aus einem Dokument der WWU Münster übernommen (https://www.uni-muenster.de/imperia/md/content/ziv/pdf/sicherheit/sciebo-empfehlungen_zum_datenschutz.pdf)

Anhang

Schutzbedarf der Daten bestimmt den Umfang der Cloud-Nutzung

Aus dem Schutzbedarf der für eine Speicherung vorgesehenen Daten folgt nicht nur, ob eine Speicherung zulässig ist sondern auch unter welchen Bedingungen dies geschehen kann. Dabei ist der Schutzbedarf getrennt nach den drei Grundwerten *Verfügbarkeit, Integrität* und *Vertraulichkeit* zu betrachten.

Verfügbarkeit

Die Daten in sciebo befinden sich an einem von drei Standorten in NRW. Es gibt keine serverseitigen Backups der Daten. Beim Ausfall eines Standorts könnten die Daten daher zeitweise oder dauerhaft nicht für den Webzugriff oder zur Synchronisation zur Verfügung stehen. Das sciebo-Konsortium haftet nicht für Schäden aus dem Verlust von Daten. Der Endnutzer ist selber für die Datensicherungen verantwortlich.

Wenn *sehr hohe Anforderungen* an die Verfügbarkeit gestellt werden, kommt eine Datenablage in sciebo somit nicht in Frage.

Integrität

Die technische Sicherstellung der Datenintegrität erfolgt durch spezielle Speichersysteme. Die Wahrscheinlichkeit von unerkannten Fehlern in den Daten ist sehr gering, aber nicht ausgeschlossen. Auf Grund der Nutzung über das Internet und der höheren Nutzerzahl bietet sciebo eine größere Angriffsfläche als Dienste, die ausschließlich hochschul-intern angeboten werden. Im Falle von Sicherheitslücken in der verwendeten Systemsoftware oder kompromittierten Zugangsdaten ist eine Datenmanipulation durch unberechtigte Personen möglich.

Wenn in dieser Hinsicht *hohe* oder sogar *sehr hohe Anforderungen* bestehen, sollte 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 sind derartige Verfahren in der Regel bereits integriert.

Vertraulichkeit

Die Einhaltung der Datenschutzvorschriften wird durch die beteiligten Hochschulen sichergestellt. Insbesondere werden Daten nicht an Privatunternehmen weitergegeben, nicht durch diese verarbeitet und auch nicht außerhalb des Gebietes der Bundesrepublik Deutschland abgespeichert. sciebo bietet eine größere Angriffsfläche als ein nur hochschulintern angebotener Dienst. Im Falle von Sicherheitslücken in der verwendeten Systemsoftware oder kompromittierten Zugangsdaten könnten unberechtigte Personen an vertrauliche Daten gelangen.

Wenn *hohe Anforderungen* an die Vertraulichkeit gestellt werden, ist – als adäquate Maßnahme – daher der Einsatz eines Datenverschlüsselungssystems zwingend notwendig. Es wird keine serverseitige Verschlüsselung angeboten, da diese keinen ausreichenden Schutz bietet. 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 sollte 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 sciebo 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 unter der vollständigen Kontrolle durch kompetente Stellen der eigenen Einrichtung erfolgen.

Schutzbedarfsanalyse

Mit dem folgenden Fragenkatalog soll der Schutzbedarf der betreuten Daten festgestellt werden. Der Fragenkatalog ist angelehnt an die Richtlinien zum IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI).
Der Schutzbedarf definiert sich dabei ausschließlich aus den anzunehmenden Schäden, die entstehen, wenn die Daten nach einem auslösenden Ereignis (durch spezifische Bedrohungen wie Passwortkompromittierung, Ausfall eines Dienstes, Verlust eines Datenträgers etc.) beeinträchtigt werden und so mindestens einer der Grundwerte der IT-Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit) verletzt wird. Dabei ergibt sich der Schutzbedarf aus den unmittelbaren Schäden und durch die möglichen Folgeschäden
(z. B. Schadensersatzforderungen, Produktionsausfallkosten).

Eine quantitative Bewertung mit bezifferten Schadenshöhen wäre hier zu aufwendig und ist unter verschiedenen Aspekten auch kaum möglich (z. B. negative Außenwirkungen, "Ruf der Institution", Schädigung durch Ansehensverlust). Vielmehr soll die persönliche Wertung helfen, eine relative Bewertung aufzustellen, die für die Notwendigkeit und Umsetzung von Schutzmaßnahmen eine Dringlichkeitsreihenfolge ergibt.

Insgesamt handelt es sich um vier Themenbereiche, die aus sicherheitsrelevanten Gesichtspunkten beleuchtet werden. Diese sind:

1. Verstöße gegen Gesetze,
2. Beeinträchtigungen der Unversehrtheit,
3. Beeinträchtigungen der Aufgabenerfüllung und
4. Finanzielle Auswirkungen.

Diese Themenbereiche werden für die Grundwerte der IT-Sicherheit wie folgt betrachtet:

- A: Integrität/Vertraulichkeit der Daten
- B: Verfügbarkeit der Daten und Dienste

Schutzbedarfskategorie: „Keine“

Schäden haben nur eine unwesentliche Beeinträchtigung der Institution oder anderer an sciebo teilnehmenden Institutionen zur Folge.

A: Vertraulichkeit und Integrität der Daten	
Verstoß gegen Gesetze und Vorschriften/Verträge	Verstöße gegen Vorschriften und Gesetze ohne nennenswerte Konsequenzen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts ist nicht nennenswert. Ein möglicher Missbrauch personenbezogener Daten hat keine nennenswerten Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.
Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung ist nicht nennenswert.
Negative Außenwirkung	Es ist keine nennenswerte Ansehens- oder Vertrauensbeeinträchtigung zu erwarten.
Finanzielle Auswirkungen	Es ist kein nennenswerter finanzieller Schaden zu erwarten.

B: Verfügbarkeit der Daten	
Beeinträchtigung der Aufgabenerfüllung	Es ist keine oder nur eine äußerst geringe Beeinträchtigung zu erwarten. In Ausnahmefällen liegt die maximal tolerierbare Ausfallzeit bei bis zu zwei Tagen.

Schutzbedarfskategorie: „Normal“

Schäden haben Beeinträchtigungen der Institution oder anderer an sciebo teilnehmenden Institutionen zur Folge.

A: Vertraulichkeit und Integrität der Daten	
Verstoß gegen Gesetze und Vorschriften/Verträge	Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts würde durch den Einzelnen als tolerabel eingeschätzt werden. Ein möglicher Missbrauch personenbezogener Daten hat nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.

Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung erscheint nicht möglich.
Negative Außenwirkung	Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
Finanzielle Auswirkungen	Der finanzielle Schaden bleibt für die Institution tolerabel.

B: Verfügbarkeit der Daten	
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit liegt in Ausnahmefällen bei bis zu 8 Stunden.

Schutzbedarfskategorie: „Hoch“

Im Schadensfall tritt Handlungsunfähigkeit wichtiger Bereiche der Institution oder anderer an sciebo teilnehmenden Institutionen ein; Schäden haben erhebliche Beeinträchtigungen der Institution selbst, anderer an sciebo teilnehmenden Institutionen, oder betroffener Dritter zur Folge.

A: Vertraulichkeit und Integrität der Daten	
Verstoß gegen Gesetze und Vorschriften/Verträge	Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen Vertragsverletzungen mit hohen Konventionalstrafen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. Ein mögliche Missbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen
Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
Negative Außenwirkung	Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
Finanzielle Auswirkungen	Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.

B: Verfügbarkeit der Daten	
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von einzelnen betroffenen als nicht tolerabel eingeschätzt. Die maximal tolerierbare Ausfallzeit liegt in Ausnahmefällen bei bis zu 4 Stunden.

Schutzbedarfskategorie: „Sehr hoch“

Der Schadensfall führt zum totalen Zusammenbruch der Institution oder anderer an sciebo teilnehmenden Institutionen, oder hat schwerwiegende Folgen für breite gesellschaftliche oder wirtschaftliche Bereiche, oder es besteht Gefahr für Leib und Leben von Personen.

Vertraulichkeit und Integrität der Daten	
Verstoß gegen Gesetze und Vorschriften/Verträge	Fundamentaler Verstoß gegen Vorschriften und Gesetze Vertragsverletzungen, deren Haftungsschäden ruinös sind
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. Ein möglicher Missbrauch personenbezogener Daten würde für den Betroffenen den gesellschaftlichen oder wirtschaftlichen Ruin bedeuten.
Beeinträchtigung der persönlichen Unversehrtheit	Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. Gefahr für Leib und Leben.
Negative Außenwirkung	Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, evtl. sogar existenzgefährdender Art, ist denkbar.
Finanzielle Auswirkungen	Der finanzielle Schaden ist für die Institution existenzbedrohend.

Verfügbarkeit der Daten	
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit liegt in Ausnahmefällen unter einer Stunde.

Stand: Juni 2017