Empfehlungen für die Verwendung des Cloudspeicherdienstes „sciebo“

IV-Sicherheitsteam der WWU – November 2014

Dieses Dokument soll darüber aufklären, welche Daten von Mitgliedern und Angehörigen der WWU in „sciebo“ verarbeitet werden dürfen und welche nicht. Es ist eine Anwendung der Cloud-Richtlinie [1] der WWU auf die speziellen Gegebenheiten des „sciebo“ genannten Cloudspeicherdienstes. Grundsätzlich ist darauf hinzuweisen, dass der Dienst nur zu Zwecken von Forschung, Lehre und Studium genutzt werden darf.

Die in „sciebo“ gespeicherten Daten befinden sich auf Servern der WWU in Münster oder ihrer Kooperationspartner in Bonn und Duisburg-Essen, für die Speicherung und Verarbeitung gilt daher das deutsche Datenschutzgesetz. Der Zugriff auf die Daten kann mittels einer Clientsoftware oder durch einen Webbrowser erfolgen. Die Clientsoftware hält die Daten auf allen mit einem „sciebo“-Konto verbundenen Geräten synchron. Dadurch passiert es schnell, das evtl. schützenswerte Daten auf unzureichend geschützte Endgeräte gelangen. Auf Grund der Regelungen zur IV-Sicherheit an der WWU [2] dürfen personenbezogene Daten nur auf Servern gespeichert werden und sind ggfs. zu verschlüsseln. Die Endnutzerordnung von „sciebo“ untersagt insbesondere die Speicherung personenbezogener Daten Dritter ohne deren Einwilligung. Über einen Webbrowser kann aus der ganzen Welt mittels einer Nutzername/Passwort-Kombination auf die Daten zugegriffen werden. Der Zugriff kann auch mit oder ohne Passwort über einen speziellen Link erfolgen, um Daten mit anderen zu teilen.

Schutzbedarf

Für die Entscheidung, unter welchen Bedingungen eine Auslagerung von Daten in „sciebo“ in Frage kommt, bildet der Schutzbedarf der Daten die grundlegende Richtschnur. Der Schutzbedarf von Daten ist an der WWU mittels der am ISidoR - Security-Audit angelehnten Schutzbedarfsanalyse zu bestimmen (vgl. Seite 3).

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
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
› Auch Daten ohne Personenbezug können einen sehr hohen Schutzbedarf haben (zum Beispiel auf Grund von Geheimhaltungsvereinbarungen).

Der Schutzbedarf wird grundsätzlich hinsichtlich der drei Schutzziele *Verfügbarkeit*, *Integrität* und *Vertraulichkeit* differenziert bestimmt. Entsprechend differenziert sollten Vorkehrungen zur Sicherheit der Daten getroffen werden. Aus dem Schutzbedarf der Daten folgt zwingend die Eignung oder Nicht-Eignung zur Speicherung in „sciebo“:

Schutzbedarf	Eignung für die Ablage
Daten mit keinem oder normalen Schutzbedarf	Ja

Daten mit hohem Schutzbedarf	Nur verschlüsselt
Daten mit sehr hohem Schutzbedarf	nein

Empfehlungen

Bevor Daten in „sciebo“ abgelegt werden, sollten die im vorangegangenen Abschnitt betrachteten Abhängigkeiten zwischen der Datenkategorie, dem Schutzbedarf der Daten und der Eignung beachtet werden.

Sparsamer Umgang

Prinzipiell sollte bei der Nutzung von „sciebo“ die Datenmenge auf das notwendige Mindestmaß begrenzt werden. Beispielsweise kann bei der Übertragung ganzer Verzeichnisbäume in die Cloud leicht übersehen werden, dass in einem Unterverzeichnis sensible Daten abgelegt wurden, die den Bereich der Einrichtung nicht verlassen dürfen. Bevor Daten auf Endgeräte synchronisiert werden, sollten erwarteter Nutzen und damit verbundene Risiken gegeneinander abgewogen werden.

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 Schutzzielen 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. Die WWU haftet nicht für Schäden aus dem Verlust von Daten. Der Endnutzer ist für Datensicherungen verantwortlich.

Wenn *sehr hohe Anforderungen* an die Verfügbarkeit gestellt werden, kommt eine Datenablage in „sciebo“ 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 WWU-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 WWU-intern 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 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 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). Die Schutzbedarfsanalyse wird an der WWU mit dem Security-Audit ISidoR [3] durchgeführt.

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 IV-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:

- Verstöße gegen Gesetze,
- Beeinträchtigungen der Unversehrtheit,
- Beeinträchtigungen der Aufgabenerfüllung und
- Finanzielle Auswirkungen.

Diese Themenbereiche werden betrachtet unter den Aspekten:

- Integrität/Vertraulichkeit der Daten und
- Verfügbarkeit der Daten und Dienste

Schutzbedarfskategorie: „Keine“

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

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.

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.

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.

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.

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.

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.

Weitere Informationen

[1] IV-Sicherheitsteam, „Cloud-Richtline,“ Juni 2013. [Online]. Available: https://www.uni-muenster.de/imperia/md/content/ziv/pdf/cloud_richtlinie_wwu.pdf.

[2] A. d. L. W. R. i. N. (ARNW), „Regelungen zur IV-Sicherheit in der Universität Münster,“ 21 Feb 2002. [Online]. Available: http://www.uni-muenster.de/Rektorat/abuni/ab020507.html.

[3] T. Rensing, „ISidoR Onlinedokumentation,“ 24 November 2010. [Online]. Available: http://www.nic.uni-muenster.de/Sec_Glossar/sec_handbuch.asp.