Themenkreis 4: Fokus Dienstleistungen & Produkte

Sicher in der Cloud – Best Practice Sicherheitskonzept

Monika Kuberek, Universitätsbibliothek der Technischen Universität Berlin

Zusammenfassung:
Cloudbasierte Bibliothekssysteme, die als Software as a Service von einem externen IT-Dienstleister betrieben werden, stellen das Bibliotheksmanagement vor neue Herausforderungen – vor allem im Hinblick auf die Gewährleistung von Datenschutz und Datensicherheit. Insbesondere die Risiken hinsichtlich Vertraulichkeit, Verfügbarkeit und Integrität der zu schützenden Daten sind andere als bei den herkömmlichen Systemen, die im Eigenbetrieb laufen, und neu zu bewerten. Am Beispiel des Alma-Sicherheitskonzepts der Berliner Universitätsbibliotheken wird ein Best Practice Sicherheitskonzept vorgestellt, das den Anforderungen des Datenschutzes in Deutschland genügt. Es beruht in seinem Kernbereich, der Gefährdungs- und Risikoanalyse, auf dem Eckpunktepapier „Sicherheitsempfehlungen für Cloud Computing Anbieter" des Bundesamts für Sicherheit in der Informationstechnik (BSI), in dem grundlegende Risiken benannt und Anforderungen für ein hohes Sicherheitsniveau dargelegt sind.

Summary:
Cloud-based library systems which are hosted by external IT-service providers in a Software as a Service model (SaaS) create new challenges for the library management – especially with regard to the guarantee of data protection and data security. In particular, the risks relating to confidentiality, availability and integrity of the data to be protected are different from those in conventional systems operated by the libraries themselves. These risks have to be re-evaluated. Using the example of the Alma security concept of the Berlin University Libraries, we present a best practice security concept, which complies with the requirements of data protection in Germany. In its core area, the analysis of threads and risks, it is based on the White Paper "Security Recommendations for Cloud Computing Providers" of the Federal Office for Information Security (BSI), which names basic risks and sets out requirements for a high level of safety.

Zitierfähiger Link (DOI): https://doi.org/10.5282/o-bib/2017H4S82-93
Autorenidentifikation: Kuberek, Monika: ORCID: http://orcid.org/0000-0002-1672-5271
Schlagwörter: Bibliothekssystem; Cloud-Computing; Datenschutz; Datensicherheit; Informationssicherheit; Sicherheitskonzept

1. Alma und Primo in der Cloud

Die Bibliotheken der vier Berliner Universitäten – Freie Universität, Humboldt-Universität, Technische Universität und Universität der Künste – sind 2016 von ihren Aleph-Systemen auf das neue, cloudbasierte Bibliothekssystem Alma der Firma Ex Libris umgestiegen und gleichzeitig mit ihren Primo-Recherchesystemen, die bislang vom Kooperativen Bibliotheksverbund Berlin-Brandenburg

gehostet wurden, in die Ex Libris-Cloud gewechselt. Die Auslieferung der beiden cloudbasierten Systeme erfolgt im Servicemodell „Software as a Service" (SaaS). Infolgedessen haben die Bibliotheken sämtliche Alma- bzw. Primo-Komponenten in die Private Cloud von Ex Libris ausgelagert; der Zugriff der Bibliotheken erfolgt mittels Webbrowser. In seinem Vortrag auf dem Bibliothekartag 2015[1] benannte Jiři Kende, Direktor der Universitätsbibliothek der Freien Universität Berlin, Gründe für den Umstieg, wie die vereinheitlichte Bearbeitung von Print- und E-Ressourcen, effizientere Workflows, Entlastung der Bibliotheken von technischen und systemadministrativen Arbeiten, Anpassung an internationale Bibliotheksstandards durch den Einsatz von MARC in Alma.[2]

Mit dem Schritt in die Cloud und ihrem Alma-Sicherheitskonzept[3] haben die Berliner Bibliotheken im deutschen Bibliothekswesen Neuland betreten. Auch die Nutzerdaten der Bibliotheken liegen künftig in der Ex Libris-Cloud und werden dort verarbeitet; entsprechende Vereinbarungen zum Schutz personenbezogener Daten sind im Vertrag festgeschrieben worden. Kende thematisiert in seinem Beitrag die Vertragsverhandlungen mit Ex Libris, die von den vier Berliner Universitäten gemeinsam durchgeführt wurden, wobei er den Schwerpunkt auf den Datenschutz legt.[4] Diesen beschreibt er als „die schwierigste Herausforderung (…), denn zumindest in den beteiligten Hochschulen ist das Bibliothekssystem die erste große Applikation, die in die Cloud außerhalb der Hochschule bzw. der Öffentlichen Hand verlagert wird".[5] Bereits in die Vertragsverhandlungen wurden die behördlichen Datenschutzbeauftragten der Universitäten eingebunden, die ihrerseits die Berliner Beauftragte für Datenschutz und Informationsfreiheit mit hinzugezogen haben.

Im Vertrag sind in einer eigenen Anlage die datenschutzrechtlichen Belange umfassend geregelt sowie technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten festgelegt. Die Basis bildet das Berliner Datenschutzgesetz.[6] Zwei Punkte seien erwähnt, die in den Berliner Bibliotheken besonders intensiv diskutiert wurden.

- *Die Frage, wo sich das Rechenzentrum befindet.* Die Diskussion dieser Frage erübrigte sich recht schnell, da die Firma Ex Libris, die ihren Sitz in Israel hat, die Systeme in einem Rechenzentrum in Amsterdam betreibt; damit unterliegen die Daten dem EU-Recht.
- *Die Frage, von wo der Zugriff auf die Daten erfolgt.* Hier stellte sich heraus, dass das Berliner Datenschutzgesetz die Auftragsdatenverarbeitung durch eine Firma außerhalb der EU nicht zulässt,[7] d.h. es darf keinen direkten Zugriff aus Israel auf die Daten geben. In der Folge hat Ex Libris die Administration des Amsterdamer Rechenzentrums nach Hamburg verlegt und

1 Jiři Kende, „Software as a Service – Herausforderungen bei der Einführung des Bibliothekssystems Alma in der Freien Universität Berlin," *o-bib* 2, Nr. 4 (2015): 134–139. https://doi.org/10.5282/o-bib/2015H4S134-139.
2 Ebd., 135
3 Auch für Primo wurde ein Sicherheitskonzept erstellt, analog zum Alma-Sicherheitskonzept. Zur besseren Lesbarkeit ist im Text lediglich vom Sicherheitskonzept bzw. Alma-Sicherheitskonzept die Rede.
4 Kende, 136–139
5 Ebd., 136
6 „Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz - BlnDSG) in der Fassung vom 17. Dezember 1990. Zum 30.09.2017 aktuellste verfügbare Fassung der Gesamtausgabe", zuletzt geprüft am 06.10.2017, http://gesetze.berlin.de/jportal/?quelle=jlink&query=DSG+BE&psml=bsbeprod.psml&max=true.
7 Ebd., § 3, Abs. 4

dort ein Servicezentrum aufgebaut, aus dem der First Level Support erfolgt. Im Vertrag wurde festgelegt, dass die Unterauftragsdatenverarbeitung im Rechenzentrum in Amsterdam erfolgen kann. Hinsichtlich der Wartung hat Ex Libris Deutschland einen Auftragswartungsvertrag mit Ex Libris Israel abgeschlossen, der ebenfalls Bestandteil des Vertrags ist.[8] Falls die Problembehebung durch den First Level Support nicht möglich ist, erfolgt der Second Level Support durch das Entwicklerteam in Israel – allerdings immer fallbezogen sowie immer mit vorheriger Anfrage an die Bibliothek und erst nach deren Zustimmung. Auch dies ist vertraglich festgelegt.

Laut Berliner Datenschutzgesetz sind „vor einer Entscheidung über den Einsatz oder wesentliche Änderungen der automatisierten Datenverarbeitung (…) die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse und eines Sicherheitskonzepts zu ermitteln".[9] Dies wurde in den Vertrag aufgenommen und die Erstellung eines Sicherheitskonzepts inklusive Risikoanalyse dort verankert.

Dem von den Bibliotheken erarbeiteten Sicherheitskonzept haben die universitären Datenschutzbeauftragten nach intensiver Begutachtung ihre Zustimmung erteilt, wobei sie wiederum die Berliner Beauftragte für Datenschutz und Informationsfreiheit mit einbezogen haben.

Das Alma-Sicherheitskonzept kann als beispielhaft für Cloud-Anwendungen im deutschen Bibliothekswesen angesehen werden. Es folgt den gesetzlichen Datenschutzregelungen in Deutschland und entspricht den Sicherheitsanforderungen des Bundesinstituts für Sicherheit in der Informationstechnik (BSI) an das Cloud-Computing. Inhalt ist die Gewährleistung der Informationssicherheit (Datenschutz, Datensicherheit, etc.). Gemäß den gesetzlichen Vorgaben des Berliner Datenschutzgesetzes ist die Zielsetzung die Wahrung von Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz der Daten.[10] Bei der Erstellung des Sicherheitskonzepts haben sich die Berliner Bibliotheken an den Empfehlungen zum Cloud-Computing des BSI orientiert. Zu nennen sind die Webseite „Dossier Anwender-Management"[11] mit verschiedenen Unterlagen des BSI zum Cloud-Computing und das BSI-Eckpunktepapier „Sicherheitsempfehlungen für Cloud Computing Anbieter".[12]

8 Dies ist im Rahmen des Berliner Datenschutzgesetzes zulässig, da Israel von der EU-Kommission als Land mit einem angemessenen Datenschutzniveau eingestuft wurde, in das personenbezogene Daten übermittelt und verarbeitet werden dürfen. Siehe BlnDSG §§ 3a, Abs. 2, Pkt. 10 und 14, Abs. 2 sowie „Beschluss der Kommission vom 31. Januar 2011 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus im Staat Israel im Hinblick auf die automatisierte Verarbeitung personenbezogener Daten". Brüssel, 31. Januar 2011, zuletzt geprüft am 06.10.2017, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:027:0039:0042:DE:PDF.

9 BlnDSG, § 5, Abs. 3.

10 Ebd., § 5, Abs. 2.

11 „Dossier Anwender-Management", Bundesamt für Sicherheit in der Informationstechnik, zuletzt geprüft am 06.10.2017, https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Zielgruppen/Anwender/AnwenderManagement/AnwenderManagement.html

12 „Eckpunktepapier. Sicherheitsempfehlungen für Cloud Computing Anbieter – Mindestanforderungen für die Informationssicherheit", Bundesamt für Sicherheit in der Informationstechnik – BSI (Hrsg.) (Stand: Februar 2012), zuletzt geprüft am 06.10.2017, https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Eckpunktepapier/Eckpunktepapier_node.html

Das BSI-Eckpunktepapier beschreibt grundlegende Anforderungen der Informationssicherheit mit einem Schwerpunkt auf Cloud-Diensten und wird vom BSI als „ein erster Schritt in Richtung zur Schaffung von Standards, auf deren Basis die Sicherheit von Cloud Computing Plattformen überprüft werden kann“,[13] gesehen. Es richtet sich zunächst an Cloud Service Provider (CSP), um ihnen eine „Richtschnur für die Umsetzung von Sicherheitsmaßnahmen“[14] zu geben, gleichzeitig aber auch an Cloud-Nutzer, denn: „Andererseits können Cloud-Nutzer, die sich mit den vorliegenden Empfehlungen beschäftigen, die CSPs nach deren Umsetzung fragen. Der erste Schritt für einen Cloud-Kunden sollte es jedoch immer sein, sich über die Schutzbedürftigkeit der eigenen Daten und Anwendungen klar zu werden.“[15] In dieser Weise wurde das Eckpunktepapier von den Berliner Bibliotheken genutzt, um die eigenen Daten und Anwendungen zu analysieren, sich über die Sicherheitsanforderungen für das Cloud-Computing klar zu werden und die Erfüllung der Anforderungen bei Ex Libris zu erfragen.

Das Alma-Sicherheitskonzept ist nicht öffentlich zugänglich, da es Informationen der Firma Ex Libris zur Umsetzung ihrer Schutzmaßnahmen enthält, die den Bibliotheken vertraulich zur Verfügung gestellt wurden. Aufgrund seines Umfangs – es umfasst in seinem allgemeinen Teil, der für die vier Berliner Universitäten gemeinsam gilt, 51 Seiten und in den institutsspezifischen Teilen jeweils zwischen 12 und 24 Seiten[16] – können die einzelnen Komponenten nur kurz erläutert und beispielhaft wiedergegeben werden; eine vollständige Auflistung aller in den Komponenten enthaltenen Punkte würde den Rahmen dieser Veröffentlichung sprengen. Zum Teil wird in den Beispielen Bezug genommen auf die Technische Universität Berlin, der die Autorin dieses Beitrags angehört.

2. Sicherheitskonzept – einzelne Komponenten

Das Erstellen eines Sicherheitskonzepts, ob nun für ein herkömmliches oder ein cloudbasiertes System, bedeutet zunächst einmal die gründliche Analyse und Beschreibung der Bibliotheksdaten und informationstechnischen Gegebenheiten vor Ort, um auf dieser Basis bestehende Schutzmaßnahmen darzulegen bzw. die notwendigen Schutzmaßnahmen zu bestimmen und festzulegen.

Das Alma-Sicherheitskonzept umfasst verschiedene Kapitel, in denen folgende Einzelkomponenten abgehandelt werden: (1) *Verantwortlichkeiten*, (2) *Rechtemanagement*, (3) *IT-Komponenten der Bibliothek*, (4) *Abhängigkeiten zwischen Alma und anderen Systemen*, (5) *In Alma gespeicherte Daten*, (6) *Schutzbedarf der gespeicherten Daten* und schließlich (7) *Risikoanalyse*. Bis auf die Risikoanalyse, die spezifisch auf das Cloud-Computing ausgerichtet ist, unterscheiden sich die Komponenten nicht von denen eines IT-Sicherheitskonzepts für Bibliothekssysteme, die in einer herkömmlichen Systemumgebung auf eigenen Servern betrieben werden.

Während die Komponenten 1, 2 und 3 sich auf die Bibliothek beziehen, dienen die systembezogenen Komponenten 4, 5 und 6 der Sicherheitsanalyse für das Cloud-Computing, die als Grundlage für die Risikoanalyse (Komponente 7) herangezogen wird. Diese ist die Kernkomponente des

13 Ebd., 9.
14 Ebd., 8.
15 Ebd.
16 Zum Aufbau des Sicherheitskonzepts siehe Kapitel 3.

Alma-Sicherheitskonzepts, wird darin doch die Entscheidung der Bibliothek, ob sie die Risiken des Cloud-Computing für ihre Alma-Installation tragen kann und will, begründet und festgehalten.

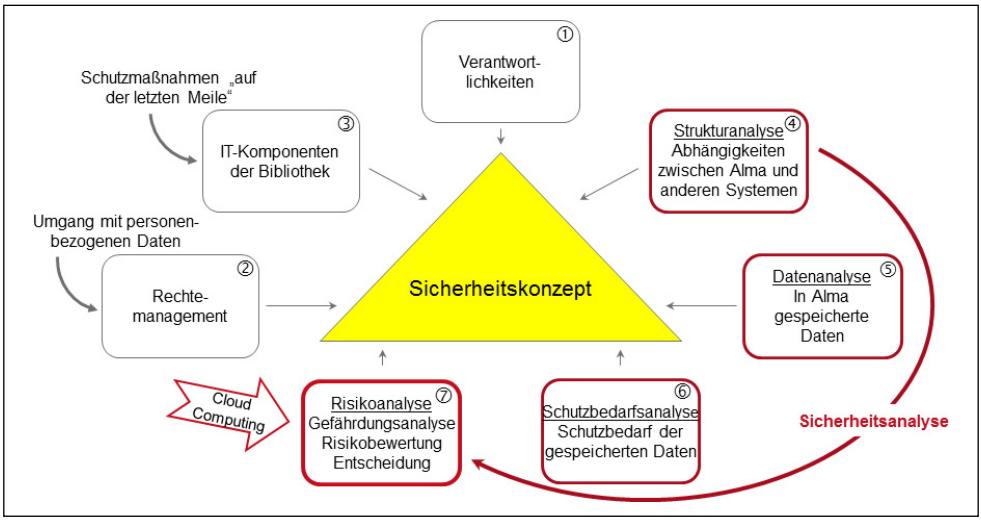

Abb. 1: Einzelkomponenten des Alma-Sicherheitskonzepts

Im Folgenden wird kurz auf die einzelnen Komponenten eingegangen, zunächst auf die allgemeinen bibliotheksbezogenen Komponenten.

(1) Verantwortlichkeiten

Im Alma-Sicherheitskonzept wurden zunächst für alle Betriebsbereiche der Bibliothek, die mit Alma in Zusammenhang stehen, die Verantwortlichkeiten festgestellt und niedergeschrieben – angefangen von der Gesamtverantwortung für das Bibliothekssystem über die Verantwortung für den IT-Bereich der Bibliothek, für die systembibliothekarische Administration von Alma, für die Administration der Mitarbeiter- und Benutzer-Endgeräte bis hin zum Identitätsmanagement und zum Active Directory.

(2) Rechtemanagement

In diesem Kapitel ist der Umgang der Bibliothek mit personenbezogenen Daten umfassend beschrieben, wie z.B. die Authentifizierung und Autorisierung sowohl der Mitarbeiterinnen und Mitarbeiter als auch der Benutzerinnen und Benutzer oder auch das Rollen- und Rechtekonzept von Alma.[17] Die Regelungen im Kapitel Rechtemanagement sind zum Teil nicht neu, sondern wurden in der Universitätsbibliothek der TU Berlin bereits für das Alma-Vorgängersystem Aleph mit der behördlichen Datenschutzbeauftragten abgestimmt, so beispielsweise zeitliche Festlegungen zu Anonymisierung und Löschung von Benutzerdaten.

17 Die Alma-Benutzerrollen und die damit verbundenen Rechte sind im Knowledge-Center von Ex Libris dokumentiert. „Verwalten von Benutzerrollen", zuletzt geprüft am 06.10.2017, https://knowledge.exlibrisgroup.com/Alma/Product_Documentation/Alma_Online_Help_(Deutsch)/Administration/030Benutzerverwaltung/060Verwalten_von_Benutzerrollen.

(3) IT-Komponenten der Bibliothek

Die Schutzmaßnahmen „auf der letzten Meile" gehören ebenfalls zu den grundlegenden Komponenten eines jeden Sicherheitskonzepts. Hier ist festgehalten, welche Schutzmaßnahmen die Bibliothek für ihre Mitarbeiter- und Benutzer-Endgeräte, die Thekenarbeitsplätze, die Verbuchungsautomaten, das Rechnernetz sowie Identitätsmanagement und Active-Directory – kurz: für alle IT-Komponenten, die mit dem Bibliothekssystem zusammenhängen – getroffen hat. Im Alma-Sicherheitskonzept ist in diesem Kapitel auch dargelegt, wie die Kommunikation mit dem Dienstleister Ex Libris erfolgt – nämlich über das Internet mittels verschlüsselter Verbindungen. Um aufseiten der TU Berlin eine lückenlose Verschlüsselung, beispielsweise für die Mailkommunikation, sicherzustellen, hat die Universitätsbibliothek diese Verbindungen im Rahmen des Alma-Projekts in Zusammenarbeit mit dem TUB-Rechenzentrum eingerichtet.

Die weiteren Komponenten des Alma-Sicherheitskonzepts, bestehend aus Strukturanalyse, Datenanalyse und Schutzbedarfsanalyse, sind Teil der Sicherheitsanalyse, einem essenziellen Bestandteil eines jeden Sicherheitskonzepts für Cloud-Computing-Anwendungen.

(4) Strukturanalyse (Abhängigkeiten zwischen Alma und anderen Systemen)

Die Feststellung der generellen Abhängigkeiten zwischen Alma und anderen Systemen im Rahmen einer Strukturanalyse war unabdingbar, um alle Anwendungen, mit denen Alma zusammenarbeitet, und alle Schnittstellen zu identifizieren. Ausgehend von den Fragestellungen „Aus welchen Systemen erhält Alma Daten?" und „An welche Systeme liefert Alma Daten?" wurden alle mit Alma verbundenen Systeme aufgelistet. Gleichzeitig wurde die Frage beantwortet: „Was passiert, wenn Alma bzw. das andere System nicht zur Verfügung steht?", um die Relevanz von Alma und den mit Alma verbundenen Systemen für die Nutzerservices und den Betrieb der Bibliothek zu ermessen. Entsprechend sind Schutzmaßnahmen in der Bibliothek (siehe Komponente 3) wie auch bei Ex Libris (siehe Komponente 7) zu treffen.

Beispielsweise erhält Alma Daten aus Primo, den Verbuchungsautomaten, dem Fernleihsystem, dem B3Kat und einer Reihe weiterer Systeme. Alma liefert Daten unter anderem an Primo, an das Fernleihsystem, das Mailrelay, Einzelarbeitsplätze und andere Systeme.

Einige Beispiele für die Abhängigkeiten zwischen Alma und Systemen, die in der Bibliothek eingesetzt werden:

- *Verbuchungsautomaten – Alma:* Der Ausfall der Verbuchungsautomaten bedeutet eine Serviceeinschränkung, da die Ausleihe/ Rückgabe dann nur an der Ausleihtheke erfolgen kann.
- *Fernleihsystem – Alma / Alma – Fernleihsystem:* Ebenso bedeutet der Ausfall des Fernleihsystems eine Serviceeinschränkung, da die Bibliothek keine Fernleihbestellungen empfangen und keine Fernleihen für ihre Benutzerinnen und Benutzer durchführen kann. Auch bei einem Ausfall von Alma kann die Bibliothek keine Fernleihbestellungen empfangen und selbst keine ausführen.
- *Alma – Einzelarbeitsplätze:* Fällt Alma aus, sind partiell oder vollständig keine dienstlichen Arbeiten mehr möglich.

Während bei den ersten zwei Beispielen ein Ausfall des Systems „nur“ Serviceeinschränkungen zur Folge hat und die Folgen für eine gewisse Zeit hinnehmbar sind, sind die Folgen bei einem Alma-Systemausfall für die Bibliothek aufgrund des Arbeitsausfalls gravierend.

(5) Datenanalyse (In Alma gespeicherte Daten)

Laut Gesetzgebung[18] dürfen Daten nur zweckgebunden erhoben und gespeichert bzw. müssen gelöscht werden. Ziel der in diesem Kapitel durchgeführten Datenanalyse und Beschreibungen war es, darzustellen, wie die datenschutzrechtlichen Belange für die in Alma gespeicherten Daten gewahrt werden. Die Berliner Bibliotheken haben dies in tabellarischer Form gemacht.

Am Anfang stand die Analyse der Datenarten. So hat man es in den Berliner Universitätsbibliotheken, wie sicherlich in anderen vergleichbaren Bibliotheken auch, mit folgenden acht Datenarten zu tun: 1. Bibliografische Daten, 2. Etat-, 3. Lieferanten-, 4. Erwerbungs-, 5. Benutzer-, 6. Ausleih-, 7. Gebühren- und 8. Kommunikationsdaten. Je nachdem, ob die Daten durch die Bibliothek erhoben bzw. maschinell aus anderen Systemen eingespielt oder aus Alma exportiert werden, wurde im Sicherheitskonzept für jede einzelne dieser Datenarten beschrieben, wie im Hinblick auf den Datenschutz mit den Daten umgegangen wird. Auch diese Regelungen sind für die Universitätsbibliothek der TU Berlin nicht neu, sondern sind identisch mit den datenschutzrechtlichen Vereinbarungen, die mit der behördlichen Datenschutzbeauftragten zum Alma-Vorgängersystem Aleph getroffen worden waren.

Beispiel aus dem Alma-Sicherheitskonzept:

5.1 Durch die UBs erhobene und in Alma gespeicherte Daten

1. Daten	2. Inhalte	3. Erforderlichkeit	4.Daten-austausch/ mit wem	5. Speicherdauer	6. Anonymisierung/ Löschung	7. Zugriffs-rechte
5 Benut-zerdaten (Internal User)	Institution Benutzer-ID E-Mail-Adresse	Für die Abwick-lung der Benut-zerdienste, für Mahnungen und Rückforderungen erforderlich	Primo der UB der TUB	Mind. 12 bis max. 24 Monate nach der letzten Kontoak-tivität oder auf Verlangen des/der Benutzer_in, sofern das Konto ausgegli-chen ist	Anonymisierung in Alma nach der in Spalte 5 angegebe-nen Frist bzw. nach Ausgleich des Benut-zerkontos Löschung der in Alma deaktivierten Benut-zerkonten im Acitve Directory der UB einmal pro Monat	Alle für die Benutzung autorisierten Mitarbeiter_ innen der UB

Abb. 2: Regelungen zum Umgang mit Datenart 5 (Benutzerdaten) in Alma

(6) Schutzbedarfsanalyse (Schutzbedarf der gespeicherten Daten)

Für alle Datenarten, die in der Datenanalyse identifiziert wurden und oben in Komponente 5 aufgeführt sind, haben die Bibliotheken im Alma-Sicherheitskonzept untersucht, welche Auswirkungen der Verlust von Vertraulichkeit / Verfügbarkeit / Integrität hat, und zwar im Hinblick auf: (a)

18 Siehe beispielsweise BlnDSG §§ 5a, 9 und 11.

die Beeinträchtigung des informationellen Selbstbestimmungsrechts, (b) Verstoß gegen Gesetze, Vorschriften, Verträge, (c) Beeinträchtigung der Aufgabenerfüllung, (d) negative Außenwirkung der Einrichtung und (e) finanzielle Auswirkungen. Entsprechend wurden die Daten im Rahmen der Schutzbedarfsanalyse in die Schutzbedarfsstufen „niedrig", „mittel" oder „hoch" eingeordnet. Im Ergebnis ist festzuhalten, dass der Schutzbedarf für alle Datenarten hoch ist.

Beispiel aus dem Alma-Sicherheitskonzept:

Daten	Vertraulichkeit	Verfügbarkeit	Integrität	Schutzbedarf (Stufe)
1 Biblio-grafische Daten	Daten sind frei zugänglich (lesend). Schutzbedarf niedrig	Die Daten sollen 7x24 verfügbar sein. Kurzzeitige Ausfälle sind vertretbar. Ausfälle beeinträchtigen das Ansehen der Einrichtung in geringem Maß. Da die Mitarbeiter_innen nicht handeln können, entsteht hoher materieller Schaden. Schutzbedarf hoch	Die Daten müssen korrekt sein, da sie den Nachweis für den Besitz der Bibliothek darstellen. Die Verletzung der Integrität in einzelnen Daten hat geringe Folgen. Der Verlust der Daten insgesamt ist für den Betrieb der Bibliothek katastrophal. Schutzbedarf hoch	hoch

Abb. 3: Schutzbedarf für Datenart 1 (Bibliografische Daten)

(7) Risikoanalyse (Gefährdungsanalyse – Risikobewertung – Entscheidung)

In der Kernkomponente des Alma-Sicherheitskonzepts, der Risikoanalyse, geht es um die Entscheidung für oder gegen den Cloud-Betrieb und die Übernahme der Verantwortung für diese Entscheidung. Die Bedeutung dieses Kapitels wird auch darin deutlich, dass es rund ein Drittel des Sicherheitskonzepts ausmacht. In dieses Kapitel sind die Ergebnisse aus der Sicherheitsanalyse (Komponenten 4-6) eingeflossen.

Dem Kapitel Risikoanalyse wurde im Alma-Sicherheitskonzept das BSI-Eckpunktpapier zugrunde gelegt. Dort sind Schutzbedarfskategorien definiert, wie „Sicherheitsmanagement beim Anbieter", „Rechenzentrumssicherheit", „Server-Sicherheit", „Netzsicherheit" und weitere; insgesamt benennt das Papier 17 Schutzbedarfskategorien.[19] Im BSI-Eckpunktepapier sind für jede dieser Kategorien Schutzmaßnahmen beschrieben und die Grundbedrohungen im Hinblick auf Vertraulichkeit, Verfügbarkeit und Integrität benannt.

Die Risikoanalyse im Alma-Sicherheitskonzept umfasst folgende Schritte:

- *Gefährdungsanalyse:* Auf Basis des BSI-Eckpunktepapiers wurden bei der Erstellung des Alma-Sicherheitskonzepts zunächst für jede der 17 Schutzbedarfskategorien Gefährdungsszenarien aufgestellt, ausgehend von der Fragestellung: „Welche möglichen Gefährdungen können sich in diesem Bereich wodurch ergeben?". Festgehalten wurde zudem, welche der in den Bibliotheken vorkommenden Datenarten (siehe Komponente 5) von dem beschriebenen

19 Siehe Eckpunktepapier, 23–77.

Gefahrenszenarium hinsichtlich ihrer Vertraulichkeit, Verfügbarkeit und Integrität bedroht sind.

- *Risikobewertung:* Die Firma Ex Libris hat den Berliner Bibliotheken umfassende – auch vertrauliche – Informationen zu den Schutzmaßnahmen, die sie für das Cloud-Computing getroffen hat, zur Verfügung gestellt und alle Fragen der Bibliotheken beantwortet, inwiefern die im BSI-Eckpunktepapier geforderten Schutzmaßnahmen erfüllt sind. In Abwägung der Gefahrenszenarien und der Erfüllung der geforderten Schutzmaßnahmen durch die Firma Ex Libris haben die Bibliotheken für jede Schutzbedarfskategorie das verbleibende Restrisiko bewertet.
- *Entscheidung:* Ergebnis der Risikobewertung war die Entscheidung der Berliner Bibliotheken, dass das Restrisiko tragbar ist. Dies implizierte die Zustimmung zum Betrieb von Alma in der Private Cloud von Ex Libris. Die Entscheidung wird von den Bibliotheksleitungen als Gesamtverantwortliche für das Bibliothekssystem (siehe Komponente 1) getragen.

Beispiel aus dem Alma-Sicherheitskonzept:

Gefahrenszenarium und korrespondierende Maßnahmen	Grundbedrohung: Vertraulichkeit Verfügbarkeit Integrität	Grundbedrohung: Hohe Vertaulichkeit	Grundbedrohung: Hohe Verfügbarkeit	Bedrohte Daten	Sicherheitsmaßnahmen im Einzelnen	Risikobewertung unter Einbeziehung der Sicherheitsmaßnahmen
C. Server-Sicherheit Mögliche Gefährdungen ergeben sich z.B. durch: Angriffe wie Rechteüberschreitungen von Nutzern, Login Fehlversuche oder Schadsoftware (z.B. Trojanische Pferde)						Das verbleibende Risiko erscheint als so gering, dass das Betriebsrisiko hinsichtlich der genannten Gefährdung als tragbar erscheint.
Maßnahmen:						
12 Technische Maßnahmen zum Schutz des Hosts (Host Firewalls, regelmäßige Integritätsüberprüfungen, Host-based Intrusion Detection Systems)	x			1-8	Sicherheitsmaßnahmen Ex Libris *(vertrauliche Informationen)*	
13 Sichere Grund-Konfigurationen des Hosts (z.B. Einsatz gehärteter Betriebssysteme, Deaktivierung unnötiger Dienste, etc.)	x			1-8	Sicherheitsmaßnahmen Ex Libris *(vertrauliche Informationen)*	
14 Einsatz zertifizierter Hypervisoren (Common Criteria mindestens EAL 4)		x		5,6,7,8	Sicherheitsmaßnahmen Ex Libris *(vertrauliche Informationen)*	
			x	1-8		

Abb. 4: Risikobewertung für die Schutzbedarfskategorie „Server-Sicherheit"[20]

20 Ebd., 30ff.

Einige Erläuterungen zu Abbildung 4: Die unter „Maßnahmen“ und in der Spalte „Grundbedrohung“ aufgeführten Inhalte stammen aus dem BSI-Eckpunktepapier. Die Zahlen in der Spalte „Bedrohte Daten“ beziehen sich auf die im Text in Komponente 5 aufgeführten Datenarten. In der Spalte „Sicherheitsmaßnahmen im Einzelnen“ sind hier die von Ex Libris mitgeteilten Sicherheitsmaßnahmen ausgeblendet, da es sich um vertrauliche Informationen handelt. Die Spalte „Risikobewertung“ enthält das Ergebnis der Bibliotheken hinsichtlich ihrer Risikoeinschätzung für die Schutzbedarfskategorie „Server-Sicherheit“.

3. Erstellung des Alma-Sicherheitskonzepts

Das Alma-Sicherheitskonzept der Berliner Universitätsbibliotheken besteht aus einem allgemeinen Teil und drei institutsspezifischen Teilen, jeweils für die Freie Universität, die Humboldt-Universität und die Technische Universität / Universität der Künste (beide haben eine gemeinsame Alma-Installation). An der Erstellung des Sicherheitskonzepts waren eine Reihe von Personen und Gruppen beteiligt:

- Die Erarbeitung des Sicherheitskonzepts lag in der Hand der Bibliotheken der vier Berliner Universitäten; die Federführung hatte die Autorin dieses Artikels, die auch die Alma-Projektleitung an der Universitätsbibliothek der TU Berlin innehatte. Aus den Bibliotheken waren fünf Personen – jeweils aus der Leitungsebene – an der Erstellung des Konzepts beteiligt: zwei Personen aus der Freien Universität, jeweils eine Person aus Humboldt-Universität, Technischer Universität und Universität der Künste.
- Unterstützt wurden die Bibliotheken durch einen externen Sachverständigen mit spezifischer datenschutzrechtlicher Expertise für universitäre Einrichtungen.
- Die Firma Ex Libris lieferte umfassende, auch vertrauliche, Informationen zu ihren Sicherheitsmaßnahmen.
- Begutachtet wurde das Sicherheitskonzept durch die behördlichen Datenschutzbeauftragten der vier Universitäten, die dazu untereinander eng zusammengearbeitet und zudem die Beauftragte für Datenschutz und Informationsfreiheit des Landes Berlin einbezogen haben.

Die Erstellung des Alma-Sicherheitskonzepts war ein iterativer Prozess mit einem kontinuierlichen Hin und Her zwischen den Beteiligten: Ersterstellung durch die Bibliotheken unter Einbeziehung des externen Datenschutzexperten und der Informationen von Ex Libris > Begutachtung und Nachbesserungswünsche durch den externen Datenschutzexperten > Vorlage bei den Behördlichen Datenschutzbeauftragten > Begutachtung und Nachbesserungswünsche > Rückkopplung der Nachbesserungswünsche mit Ex Libris und Einarbeitung weiterer Informationen von Ex Libris > Rückkopplung des neuen Standes mit dem externen Datenschutzexperten > … – bis Ex Libris alle im BSI-Eckpunktepapier aufgelisteten Schutzmaßnahmen[21] im Detail und für die behördlichen Datenschutzbeauftragten zufriedenstellend beantwortet und entsprechende Unterlagen geliefert hatte. Angemerkt sei, dass der gesamte Prozess in einer sehr konstruktiven Atmosphäre stattgefunden hat. Alles in allem dauerte der Prozess bis zur abschließenden Zustimmung der Personalräte hinsichtlich der auf das Bibliothekspersonal bezogenen datenschutzrelevanten Teile gut 9 Monate.

21 Siehe Eckpunktepapier, 23–77 und das Beispiel in Abbildung 4.

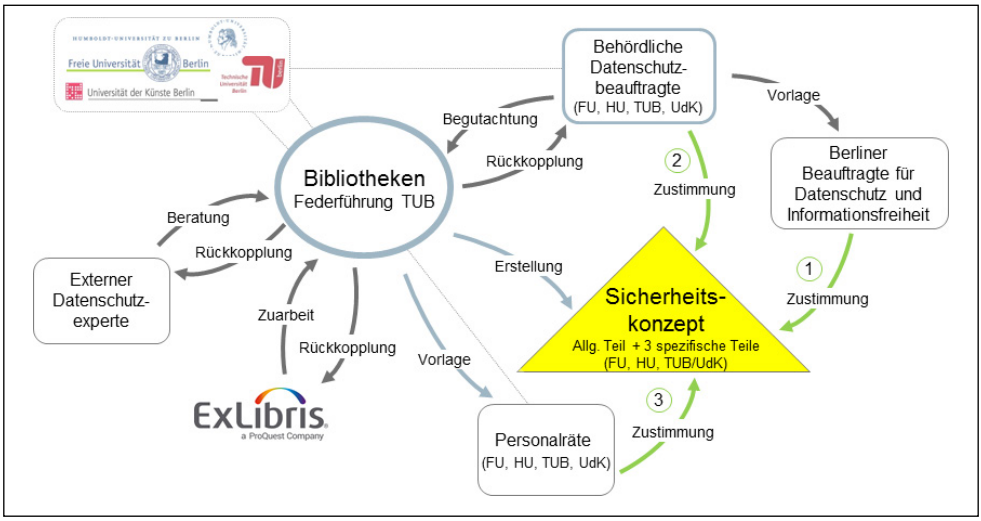

Abb. 5: Beteiligte an der Erstellung des Alma-Sicherheitskonzepts

Insgesamt wurde das Alma-Sicherheitskonzept intensiven datenschutzrechtlichen Prüfungen unterzogen. Nachdem es einen für die Behördlichen Datenschutzbeauftragten zufriedenstellenden Stand hatte, wurde es der Berliner Beauftragten für Datenschutz und Informationsfreiheit zur Begutachtung und Prüfung vorgelegt. Erst nach deren positiver Begutachtung haben die universitären Datenschutzbeauftragten ihre Zustimmung gegeben. Im Anschluss an diesen Prozess haben die vier Universitätsbibliotheken das Alma-Sicherheitskonzept ihrem jeweiligen Personalrat zur Zustimmung vorgelegt.

Was sind die Erfahrungen aus dem Verfahren zur Erstellung des Alma-Sicherheitskonzepts? Es empfiehlt sich, die behördlichen Datenschutzbeauftragten bereits in die Vertragsverhandlungen mit einzubeziehen, um den grundlegenden vertraglichen Rahmen für die datenschutzrechtlichen Maßnahmen sicherzustellen. Nicht unterschätzen sollte man weiterhin den zeitlichen Aufwand für die Erstellung des Sicherheitskonzepts, für Analyse und Beschreibung zum einen, insbesondere aber auch für die Rückkopplung zwischen den beteiligten Gruppen – daher sollte man so früh wie möglich mit der Erstellung des Sicherheitskonzepts beginnen. Auch zeitliche Abhängigkeiten gilt es frühzeitig zu berücksichtigen und einzuplanen: So war das Sicherheitskonzept die Voraussetzung für den Abschluss der Dienstvereinbarung zum Betrieb von Alma mit dem jeweiligen Personalrat, wobei in der Universität der TU Berlin die beiden Personalräte (Personalrat der Beschäftigten und Personalrat der studentischen Beschäftigten) einzubeziehen waren – auch hier wieder der Ratschlag, das Sicherheitskonzept so früh wie möglich anzugehen.

Der Aufwand zur Erstellung des Alma-Sicherheitskonzepts war hoch, zumal es keine Vorbilder gab, an denen die Berliner Universitätsbibliotheken sich hätten orientieren können. Angesichts der sensiblen Thematik Informationssicherheit und Cloud-Computing war der Aufwand andererseits angemessen und die vier Berliner Universitätsbibliotheken betreiben ihr neues Bibliothekssystem in der Ex Libris

Private Cloud in der Gewissheit, dass es den hohen datenschutzrechtlichen Standards in Deutschland entspricht. Von den Erfahrungen können sicher andere Bibliotheken in Deutschland, bei denen in den nächsten Jahren der Umstieg auf ein neues cloudbasiertes Bibliothekssystem ansteht, profitieren.

Literaturverzeichnis

- „Beschluss der Kommission vom 31. Januar 2011 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus im Staat Israel im Hinblick auf die automatisierte Verarbeitung personenbezogener Daten". Brüssel, 31. Januar 2011. Zuletzt geprüft am 06.10.2017. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:027:0039:0042:DE:PDF.

- Bundesamt für Sicherheit in der Informationstechnik, Hrsg. „Dossier Anwender-Management". Zuletzt geprüft am 06.10.2017. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Zielgruppen/Anwender/AnwenderManagement/AnwenderManagement.html.

- Bundesamt für Sicherheit in der Informationstechnik, Hrsg. „Eckpunktepapier. Sicherheitsempfehlungen für Cloud-Computing-Anbieter – Mindestanforderungen für die Informationssicherheit," Stand: Februar 2012. Zuletzt geprüft am 06.10.2017. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Eckpunktepapier/Eckpunktepapier_node.html.

- „Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz – BlnDSG) in der Fassung vom 17. Dezember 1990. Zum 30.09.2017 aktuellste verfügbare Fassung der Gesamtausgabe". Zuletzt geprüft am 06.10.2017. http://gesetze.berlin.de/jportal/?quelle=jlink&query=DSG+BE&psml=bsbeprod.psml&max=true

- Kende, Jiři. „Software as a Service – Herausforderungen bei der Einführung des Bibliothekssystems Alma in der Freien Universität Berlin". *o-bib* 2, Nr. 4 (2015): 134–139. https://doi.org/10.5282/o-bib/2015H4S134-139.