Anlage 1

Universitätsspezifischer Teil des Sicherheitskonzepts Alma

Humboldt-Universität zu Berlin (HU Berlin),

Dr. Michael Voß

Inhaltsverzeichnis

3. Verantwortlichkeiten

3.1 IT-System der Bibliothek der HU Berlin

- Gesamtverantwortung für den Betrieb von ALMA:
  - Verfahrensverantwortung Prof. Dr. A. Degkwitz, Direktor der UB
  - Stellvertretung: Dr. M. Voß, Leitung der EDV-Abteilung der UB
- Verantwortung für die Systemadministration (VSA) ALMA
  - Dr. M. Voß, Leitung der EDV-Abteilung der UB
  - Stellvertretung: U.Wassermann, Stv. Leitung der EDV-Abteilung der UB
- Die Systembibliothekare erhalten die Rechte des Verwaltungssystemadministrators und legen nach Vorgabe der Abteilungsleiter/Fachvorgesetzten die Benutzungsrollen der Mitarbeitenden an.
- Die Abteilungsleiter / Fachvorgesetzten erhalten die Rechte auf Analytics.

5. Angaben zu Abhängigkeiten von anderen Systemen / von diesem System abhängige Systeme

5.1.1 Das Bibliothekssystem ist abhängig von folgenden Systemen:

- *IDM der HU Berlin*
  - Datenübernahme von Daten der HU-Angehörigen, die Leser der Bibliothek sind;
  - Authentifizierung über Shibboleth in Primo zur Nutzung der Ausleihfunktionen (Bestellungen, Verlängerungen, Vormerkungen etc.) in Alma;
  - Authentifizierung der UB-Beschäftigten über Shibboleth in ALMA;

  Steht das IDM nicht zur Verfügung, können die externen Benutzerdaten in Alma nicht aktualisiert werden. Die Authentifizierung gegen Shibboleth ist ebenfalls nicht möglich. Die UB-Beschäftigten können nicht in ALMA arbeiten. Insbesondere können keine Medien entliehen oder zurückgebucht werden.
- *Verbuchungsautomaten / RFID (ID)*
  - Zum Verbuchen von Ausleihen und Rückgaben eines Mediums und zur Bezahlung ausstehender Gebühren in Alma. Authentifizierung über Barcode auf dem Studierendenausweis / Bibliotheksausweis bzw. Eingabe von Login/Passwort bzw. Nutzung der HU-Card mit Password.

Stehen die Verbuchungsautomaten nicht zur Verfügung, kann die Ausleihe und Rücknahme nur an den Theken erfolgen, die Bezahlung von Gebühren ist dann nur über EC-Kartenzahlung in 2 Zweigbibliotheken möglich.

- *Mailrelay*
    - Die Kommunikation von Alma mit der Umgebung erfolgt über Mail. Darüber werden sowohl Mahnungen und Benutzerbenachrichtigungen abgewickelt sowie auch Listen, Quittungen und alle anderen Schreiben erzeugt.

Fällt der Mailrelay oder das Mailsystem der HU Berlin aus, können keinerlei Schreiben oder Drucke aus Alma erfolgen.

- *IT-Umgebung Einzelplätze*
    - Nutzung von Alma nach Authentifizierung durch Mitarbeitende des Bibliothekssystems

Fallen die Einzelarbeitsplätze in den Bibliotheken aus, sind partiell oder vollständig keine dienstlichen Arbeiten mehr möglich. Ein großes Problem tritt dann auf, wenn davon Ausleihplätze betroffen sind, da keine Ausleihen und Rückbuchungen möglich sind.

5.1.2 Vom Bibliothekssystem sind abhängig:

- *Digitalisierungsserver der UB*

Es können keine neuen Vorgänge angelegt werden. Bei diesem Vorgang werden bibliographische Daten aus ALMA geladen.

- *Vscout*
    - Die Bibliographischen Daten von Beständen des Grimm-Zentrums und der ZwB Campus Nord werden aus ALMA regelmäßig exportiert, um das elektronische Leitsystem (Vscout) mit aktuellen Daten zu versorgen.

Fällt Vscout oder die Schnittstelle aus, können keine Daten in Vscout aktualisiert werden.

5.1.3 Durch die Bibliothek erhobene Daten, in Alma gemäß den Bedingungen in Spalte 6 gespeichert:

	1. Daten	2. Inhalte	3. Erforderlichkeit	4. Datenaustausch / mit wem	5. Speicherdauer	6. Löschung / Anonymisierung	7. Zugriffsrechte
1	Benutzerdaten (Nicht HU-Angehörige)	Name, Vorname Geb.-datum Heimat-/ Privatadresse E-Mail-Adresse Gültigkeitszeitraum des Benutzerkontos	Im Rahmen der Benutzerverwaltung ist die Speicherung der persönlichen Meldeadresse notwendig. Diese Notwendigkeit ergibt sich aus Vorschriften der Benutzungsordnung, die den amtlichen Nachweis eines Wohnsitzes vorsehen, bzw. die Ausleihe von Medien außer Haus verweigern, wenn ein amtlich festgestellter Wohnsitz in der Bundesrepublik Deutschland nicht nachgewiesen werden kann. Hintergrund dieser Vorschriften der Benutzungsordnung ist die verwaltungsrechtliche Bestimmung, dass in einem öffentlich-rechtlichen Nutzungsverhältnis offene Forderungen wie nicht gezahlte Gebühren,	Primo	2 Jahre nach der letzten Kontoaktivität bei ausgeglichenem Benutzerkonto oder auf Verlangen des Benutzers bei ausgeglichenem Benutzerkonto	Anonymisierung nach der angegebenen Frist bzw. nach Ausgleich des Benutzerkontos; eine Löschung erfolgt nicht, da die Daten für statistische Zwecke erforderlich sind	Autorisierte Mitarbeitende der Bibliothek

	1. Daten	2. Inhalte	3. Erforderlichkeit	4. Datenaustausch / mit wem	5. Speicherdauer	6. Löschung / Anonymisierung	7. Zugriffsrechte
			Auslagen und Schadenersatzforderungen im Verwaltungsvollstreckungsverfahren beigetrieben werden.				
6	Ausleihdaten	Bestellung/ Vormerkung von Medien: Vormerker, Zeitpunkt der Bestellung/ Vormerkung, Zeitraum des Interesses Ausleihe: Ort, Zeitpunkt, Medium, Entleiher_in Rückgabe: Ort, Zeitpunkt, Medium	Die anonymisierten Daten werden für die Erstellung von Statistiken benötigt. Die Statistiken bilden die Grundlage für die Zukunftsplanung der Bibliothek (Personaleinsatz, Benutzungsdienste, Medienbeschaffung usw.)		Unbegrenzte Speicherung der anonymisierten Daten	Anonymisierung: 8 Wochen nach Abschluss der Vormerkung/ Bestellung oder 8 Wochen nach Rückgabe (Anonymisierung des Ausleihe- und des zugehörigen Rückgabe-Satzes)	alle für die Benutzung autorisierten Mitarbeiter_innen der Bibliothek

5.2 Maschinell von anderen System nach Alma übermittelte Daten

	Art der Daten	Quellsys-tem	Inhalte	Erforderlichkeit	Speicherdauer	Rechtliche Grundlage	Datenschutz des Quellsystems	Verant-wort-licher
2	**Benutzer-daten (HU-Angehöri-ge)**	Identi-täts-manage-ment der HU Berlin	Name, Vor-name Geb.-datum Heimat-/ Pri-vatadresse E-Mail-Adresse Gültigkeits-zeitraum des Benutzerkon-tos	Im Rahmen der Benutzer-verwaltung ist die Speiche-rung der persönlichen Mel-deadresse notwendig. Diese Notwendigkeit ergibt sich aus Vorschriften der Benutzungsordnung, die den amtlichen Nachweis eines Wohnsitzes vorse-hen, bzw. die Ausleihe von Medien außer Haus ver-weigern, wenn ein amtlich festgestellter Wohnsitz in der Bundesrepublik Deutschland nicht nachge-wiesen werden kann. Hintergrund dieser Vor-schriften der Benutzungs-ordnung ist die verwal-tungsrechtliche Bestim-mung, dass in einem öf-fentlich-rechtlichen Nut-zungsverhältnis offene Forderungen wie nicht ge-zahlte Gebühren, Auslagen	2 Jahre nach der letzten Kontoaktivität bei ausgegli-chenem Benut-zerkonto Oder auf Ver-langen des Be-nutzers bei ausgegliche-nem Benutzer-konto; an-schließend er-folgt die Ano-nymisie-rung;eine Lö-schung erfolgt nicht, da die Daten für sta-tistische Zwe-cke erforderlich sind	Benutzungs-ordnung ZE CMS und ZE UB (amtl. Mit-teilungsblatt der HU Berlin 23/2004)	- Sicherheitskon-zept des HU_IAM-Konnektors ALMA - Sicherheitskon-zept zur Einfüh-rung eines HU-einheitlichen Identitätsmana-gements (HU-IAM-Kern)	Michail Bach-mann (CMS)

	Art der Daten	Quellsys-tem	Inhalte	Erforderlichkeit	Speicherdauer	Rechtliche Grundlage	Datenschutz des Quellsystems	Verant-wort-licher
				und Schadenersatzforde-rungen im Verwaltungs-vollstreckungsverfahren beigetrieben werden.				

5.3 Aus Alma maschinell an andere Systeme übermittelte Daten

	Art der Daten	Zielsystem	Inhalte	Erforderlichkeit	Speicherdauer	Rechtliche Grundlage	Datenschutz des Ziel-system	Verantwortlicher
	Bibliographische Daten	Digitalisierungs-server	Bibliogr. Daten, von Medien, die digitalisiert wer-den sollen	Die bibl.Daten werden zur Identi-fikation der Digi-talisate benötigt	unbegrenzt			
	Bibliographische Daten und Standortangaben	Vscout	Bibliographische Daten und Standortangaben des Grimm-Zentrums und der ZwB Campus Nord	Die Daten dienen der Orientierung der Leser über die Standorte der Me-dien; personenbe-zogene Daten werden nicht übergeben;	Vscout: für das Leitsys-tem solange dies einge-setzt wird			
	Benutzerdaten	Primo	ALMA-ID, E-Mail-Adresse Name, Vorname	Nur über Primo können die Benut-zerinnen der Bibli-othek Bestellun-	Solange, wie die Benutzer-Daten in Alma gespeichert sind		Primo-Datenschutzverfahren	Leiter EDV der UB

	Art der Daten	Zielsystem	Inhalte	Erforderlichkeit	Speicherdauer	Rechtliche Grundlage	Datenschutz des Zielsystem	Verantwortlicher
				gen zu Medien der Bibliothek erstellen; Einblick in ihre Kontodaten nehmen, und Leihfristen verlängern.				

6. Schutzbedarfsfeststellung – universitätsspezifische Ergänzung

Die Schutzbedarfsfeststellung der abhängigen Systeme wird hier nicht dargestellt.

8. Rechtemanagement

8.1 Benutzerinnen und Benutzer in Alma

8.1.1 Interne und externe Benutzer_innen in Alma (internal/external user)

In Alma werden externe und interne Benutzerinnen und Benutzer unterschieden.

Interne Benutzerinnen und Benutzer werden komplett in Alma verwaltet. Für diese Benutzer werden auch die Passworte verschlüsselt in Alma gespeichert.

Externe Benutzerinnen und Benutzer werden in anderen DV-Systemen geführt und gepflegt und über das IDM der HU Berlin nach ALMA überführt. (Beschreibung des Verfahrens unter 7.6).

Interne und externe Benutzergruppen werden wie folgt unterschieden:

1. Interne Alma Benutzerinnen und Benutzer - alle nicht universitären Benutzerinnen und Benutzer, Kontaktdaten von Lieferanten und Fernleihbibliotheken,
2. Externe Alma Benutzerinnen und Benutzer - alle Studierende der HU Berlin und die Mitarbeitenden der HU, die Leser der Bibliothek sind und alle staff-user der Bibliothek

8.3 Rollen- und Rechtekonzept in Alma

8.3.5 Festlegungen der Bibliothek für die Rollenvergabe

Die Mitarbeiter der Medienbearbeitung sind für den Bereich der Medienerwerbung und -erschließung zuständig. Im Bereich der Medienerwerbung müssen sie Bestellungen erstellen und verwalten, Rechnungen bearbeiten und prüfen sowie Etats verwalten und belasten. Im Mittelpunkt der Medienerschließung stehen die Katalogisierung, Bestandsbearbeitung (Lokaldaten und Exemplardaten) sowie die physische Bearbeitung von Medien.

Im Rahmen der Rechte muss nicht zwischen Mitarbeitern in verschiedenen Tarifgruppen unterschieden werden, da die Aufgaben grundsätzlich von allen Medienbearbeitern erledigt werden und die Unterscheidung im Bereich des Schwierigkeitsgrades der Titel und der Höhe der Bestellsummen liegt. Die allermeisten Aufgaben sollen standortübergreifend zu leisten sein, müssen also im Bereich der Rechte nicht auf Standorte eingeschränkt werden. Die Übersichtlichkeit der jeweiligen Arbeitsumgebung ergibt sich aus der Konfiguration der einzelnen Erwerbungsabteilungen der Standorte in Alma.

Die Mitarbeiter_innen, die mit der Medienbearbeitung/Erwerbung betraut sind, benötigen zum Verfügbarmachen der erworbenen Medien das Recht, sich an der Leihstelle anzumelden, die das Medium im Benutzungsprozess verwaltet.

Wenn ein Medium auf Wunsch eines Benutzers beschafft wird, müssen die Mitarbeiter_innen Zugriff auf die Leser-daten der UB haben, damit auf das erworbene Buch eine Vormerkunge erstellt werden kann.

Die Mitarbeiter_innen in den Benutzungs-Bereichen Auskunft und Ausleihe benötigen Lese- und Schreibrechte auf die personenbezogenen Daten der Leser_innen:

- Namen, Geburtsdatum
- Adressen
- E-Mail-Adresse
- Ausleih-Daten
- Gebühren-Daten

8.4 Aktionen in Alma im Hinblick auf personenbezogene Daten

Da Alma personenbezogene Daten nur im Hinblick auf interne Benutzer_innen bzw. externe Benutzer_innen speichert und zur Auswertung bereithält, sind die weiteren Aktionen den folgenden beiden Kapiteln zu entnehmen

8.5 Verwaltung der internen ALMA-Benutzer_innen

Die Bibliothek der HU verwaltet folgende Benutzer_innen als ALMA-interne Benutzer_innen:

- Leser, die nicht HU-Angehörige sind
- Fernleihbibliotheken.

Die Daten werden von den Beschäftigten der Bibliothek in ALMA eingegeben. Es erfolgt kein maschineller Abgleich mit anderen Datenbanken. Diese Benutzer müssen sich an einer Theke der Bibliothek anmelden und bei Bedarf ihren Bibliotheks-Account verlängern lassen. Persönliche Benutzer müssen einen amtlichen Lichtbildausweis und eine Meldebescheinigung, mit der ein Wohnsitz in Deutschland nachgewiesen wird, Benutzer unter 18 Jahren zusätzlich die Einwilligungserklärung ihrer Erziehungsberechtigten, institutionelle Benutzer die Bestätigung der Institutsleitung vorlegen.

Für Patron werden folgende Daten erfasst:

- Vorname
- Nachname
- Anrede
- Titel
- Geburtsdatum
- Sprache (deutsch, englisch)
- Privat-Anschrift in Deutschland (Kommunikationsadresse): a) Stadt b) Straße und Hausnr. c) PLZ
- E-Mail-Adresse

- Tel.nr. privat oder dienstlich (fakultativ)
- Beginn der Gültigkeit des Benutzerausweises/ Start des Benutzungsverhältnisses
- Benutzergruppe in der Bibliothek
- fakultativ: Alternativadresse: a) Stadt b) Straße und Hausnr. c) PLZ

8.6 Verwaltung der externen ALMA-Benutzer_innen

Die Bibliothek verwaltet folgende Benutzer-Gruppen als externe ALMA-Benutzer:

- Beschäftigte der UB (staff-user in ALMA)
- HU-Angehörige (Leser_innen der UB)

Die Daten der externen ALMA-Benutzer werden aus dem IDM der HU bezogen.

Die Daten der Studierenden werden in xxx in der Studierenden-Verwaltung, die Daten der HU-Beschäftigten werden in yyyy von der Personal-Abteilung gepflegt.

Die Softwaresysteme der Studierenden-Verwaltung und der Personal-Abteilung werden hier nicht betrachtet, da ALMA nur Daten mit dem IDM austauscht.

Die Veränderungen der Daten in der Studierenden-Verwaltung und in der Personal-Abteilung werden in kurzen Abständen an das IDM der HU Berlin geliefert.

Die Daten der HU-Studierenden werden einmal pro Tag aus dem IDM an ALMA geliefert. Dabei werden die Daten aller Studierenden an ALMA geliefert, deren Konto in der UB nicht anonymisiert wurde.

Wenn ein HU-Angehöriger (nicht Student) Leser werden möchte, muss er dies auf einer Web-Seite der UB mitteilen. Auf dieser Web-Seite stimmt er der Datenübergabe aus dem IDM nach ALMA zu. Alle Daten, die ALMA benötigt, aber vom IDM nicht bereitgestellt werden, muss der HU-Beschäftigte auf dieser Web-Seite selbst eingeben. Der HU-Beschäftigte muss dann zu einer Ausleihtheke gehen, damit seine Angaben geprüft und ihm ein Leser-Ausweis ausgehändigt werden kann. Ab diesem Zeitpunkt werden täglich die Daten der Leser, die HU-Angehörige und nicht HU-Studenten sind, zwischen ALMA und dem IDM abgeglichen.

Der Datenabgleich endet, wenn

- der Leser sein Benutzungsverhältnis zur UB beenden möchte, sein Konto ausgeglichen ist (keine Vormerkungen/Bestellungen auf Medien vorliegen, alle Ausleihen beendet sind und keine offenen Gebühren existieren) und sein Konto anonymisiert wurde;
- der Account im IDM abgelaufen ist.

Im letzteren Fall wird das Bibliothekskonto als gesperrt gekennzeichnet, damit der/die Leser/Leserin an einer Ausleihtheke seinen Status klären muss.

Das IDM liefert einmal pro Tag alle Daten von allen Beschäftigten der UB - besitzen eine OKZ 92xxx - nach ALMA. Wenn bei dieser Datenlieferung Daten von neuen Beschäftigten enthalten sind, werden diese mit dem Rollen-Template „NOLOGON" ausgestattet. Erst, wenn die korrekte Rollenzuweisung erfolgt, kann sich der neue Beschäftigte in ALMA anmelden.

Das IDM der HU Berlin liefert bei externen Benutzerinnen und Benutzern (Leser der Bibliothek)

- Name, Vorname
- Account-ID
- private Post-Adresse
- dienstliche, persönliche E-Mail-Adresse
- Ablaufdatum des Accounts im IDM (bei unbefristet Beschäftigten ein festes Datum in der Zukunft)
- Status im IDM (Student, nicht-wiss. Beschäftigter, wiss. Beschäftigter, Professor)

Das IDM der HU Berlin liefert für die staff-user der Bibliothek:

- Name, Vorname
- dienstliche, persönliche E-Mail-Adresse
- Account-ID
- Ablaufdatum des Accounts im IDM (bei unbefristet Beschäftigten ein festes Datum in der Zukunft)

Alma-spezifische Daten wie Benutzergruppe und PIN werden in Alma gepflegt und nicht überschrieben.

Das Passwort wird nicht nach ALMA übertragen, die Authentifizierung erfolgt über Shibboleth. Alma kennt das Passwort nicht.

Externe Nutzer können auf zwei Arten in Alma geladen werden,

a.) per Synchronisation
b.) per Import. Import ist für einmalige Vorgänge, z.B. im Rahmen der Migration, relevant, während die Synchronisierung permanent läuft.

Das einmalige Laden erfolgt mittels der Definition eines Importprofils. Das Benutzerprofil wird gemäß den Installationsempfehlungen als öffentlich gekennzeichnet und importiert. Nach dem Import werden die rollengemäßen Rechte zugewiesen.

Geladen werden diese Daten in Form von XML-Dokumenten.

Import, Abgleich und Synchronisierung erfolgen anhand einer ID, an der HU die Immatrikulationsnummer der Studierenden bzw. der Personalnummer der HU Beschäftigten. Bei der Synchronisierung werden alle Felder überschrieben, mit Ausnahme von Benutzergruppe, Prozess-Titel, PIN-Nummer und Benutzer-Sprache, daher müssen alle Dateilieferungen die vollständige Feldbelegung enthalten.

8.7 Anonymisierung/Löschung von Benutzer_innen in ALMA

Wenn externe Benutzer nicht mehr im IDM der HU nachgewiesen werden, wird der entsprechende Bibliotheks-Account gesperrt. Aus dem externen Benutzer wird ein interner Benutzer gemacht. Ab diesem Zeitpunkt gelten die Abläufe für den internen Benutzer.

Ein staff-user-Konto wird gelöscht, wenn im IDM das Merkmal OKZ 92xxx entfernt wurde oder der Account im IDM gelöscht wurde.

Interne Benutzer, deren Konten die Gültigkeitsdauer überschritten haben, werden auf gesperrt gesetzt.

Eine endgültige Löschung eines Nutzers geschieht 2 Jahre nach Sperrung, wenn das Benutzerkonto ausgeglichen ist. Damit ist gewährleistet, dass Benutzer, die deutlich nach Ablauf des Gültigkeitszeitraums ihres Kontos eine Verlängerung beantragen, leicht wieder ein aktives Konto erhalten können und nicht neu angelegt werden müssen.

Wenn ein Benutzer-Konto folgende Merkmale aufweist:

- ausstehende Bestellungen/Vormerkungen,
- ausstehende Ausleihen,
- offene Gebühren (auch befristet oder unbefristet niedergeschlagene Gebühren)

wird der Account erst gelöscht, wenn das Benutzerkonto bereinigt ist.

Bewegungsdaten gelöschter Benutzer sind anonymisiert in Analytics auswertbar (Vollständig ausweisbar beibehalten)

9. Beschreibung der IT-Komponenten (Seite Bibliothek)

Beim Betrieb von ALMA sind folgende IT-Komponenten einbezogen:

1. PCs der UB-Mitarbeiter; Peripherie (Drucker)
2. öffentliche Computerarbeitsplätze (UB und CMS)
3. Ausleih-, Rückgabe-, Ausgabe-Automaten
4. Server zur Übergabe der Kassen-Logs an das Studentenwerk Berlin
5. Rechner, der die Kassen-Logs abholt (Studentenwerk Berlin)
6. Rechnernetz der Humboldt-Universität
7. Firewall der Humboldt-Universität
8. Identitäts-Management der HU
9. Active Directory (Windows-Domain)
10. ALMA (Cloud Betrieb)
11. B3KAT (Verbund-Katalog)

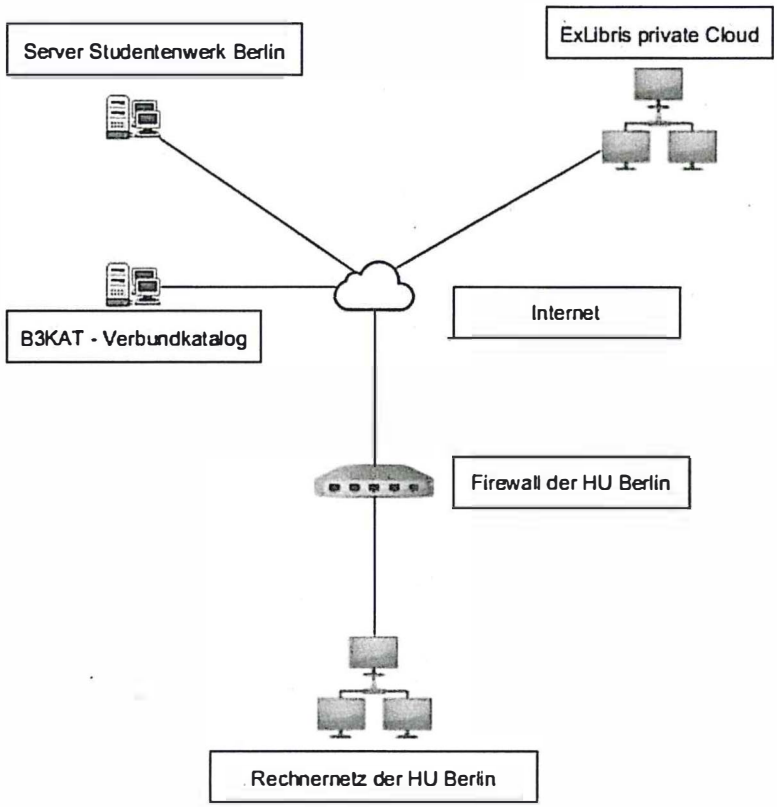

Abb. 1: Gesamtüberblick IT-Komponenten, die in ALMA involviert sind

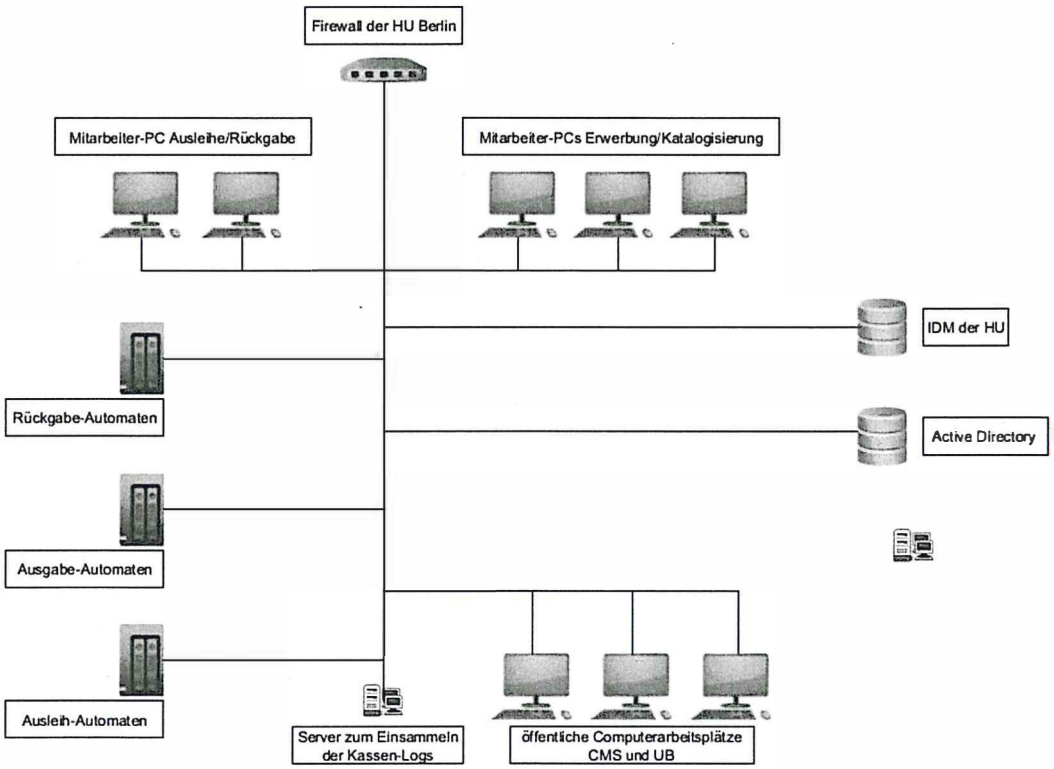

Abb.2: Überblick über die IT-Komponenten der UB, die in ALMA involviert sind

9.1 PCs der Mitarbeiter

Die Mitarbeiter-PCs sind per Gruppenrichtlinien so abgesichert, dass sich nur Mitarbeiter der UB an diesen PCs anmelden können. Die PCs sind mit einem aktuellen Windows-Betriebssystem und aktuellem Virenscanner ausgestattet. Sicherheits-Patche und Programm-Aktualisierungen werden zentral durch die Abteilung EDV der UB installiert.

9.2 Öffentliche Computerarbeitsplätze (UB, CMS)

Die öffentlichen Computerarbeitsplätze sind Thin-Clients oder Windows-PCs, die im Kiosk-Modus betrieben werden. Zum Teil kann ohne Anmeldung ein Browser genutzt werden, der über ein Proxy auf Web-Server der Humboldt-Universität zu Berlin und auf einzelne Web-Kataloge (Online-Katalog der UB, Regionaler Katalog des KOBV) beschränkt sind. Über RDP-Clienten kann auf die Terminalserver-Farm des CMS zugegriffen werden. Dazu ist ein CMS-Account oder ein Bibliotheks-Account erforderlich.

9.3 Ausleih-, Rückgabe- und Ausgabe-Automaten

An der UB werden Ausleih-, Rückgabe- und Ausgabe-Automaten der Firmen Lygnsoe, Bibliotheca und MK-Sorting eingesetzt. Die Automaten kommunizieren mit dem unverschlüsselten Protokoll SIP2 mit dem Bibliothekssystem ALMA. Damit die Kommunikation nicht verfolgt werden kann, wird sie über einen secure-Tunnel (stunnel) verschlüsselt.

Bei der Bezahlung von Gebühren durch die Leser an den Ausleihautomaten entstehen Kassen-Logs, die an das Studentenwerk Berlin täglich übergeben werden. Dies erfolgt über einen gesonderten Server, den die UB betreibt. Damit hat das Studentenwerk nur Zugriff auf die Kassen-Logs. Das Studentenwerk hat keinen Zugriff auf die Ausleihautomaten.

9.4 Server zur Übergabe der Kassen-Logs an das Studentenwerk Berlin

Die UB betreibt einen gesonderten Server zum Sammeln der Kassen-Logs zur Übergabe an das Studentenwerk Berlin. Dieser Server ist nur per ssh zugänglich. Der ssh-Zugang ist auf das HU-Netz und eine IP-Adresse des Studentenwerks Berlin beschränkt. Einmal täglich (um 0:30 Uhr) werden alle Kassen-Logs von den Ausleihautomaten per script (Windows-Freigabe) geholt und für einen UNIX-Benutzer bereitgestellt. Das Studentenwerk Berlin hat einen UNIX-Account für diesen Server. Mit Key-basierter Anmeldung holt das Studentenwerk die Daten ab und löscht diese nach erfolgreicher Übertragung. Die Zugriffe des Studentenwerks (auch aller anderen Unix-Benutzer) werden protokolliert.

9.5 Rechner, der die Kassen-Logs abholt (Studentenwerk Berlin)

Das Studentenwerk betreibt u.a. einen Rechner, der täglich die Kassen-Logs von einem Server der UB abholt (siehe: „Server zur Übergabe der Kassen-Logs an das Studentenwerk Berlin").

9.6 Rechnernetz der Humboldt-Universität

Die PCs und Server der UB sind Bestandteil des Rechnernetzes der Humboldt-Universität zu Berlin, das vom CMS betrieben und abgesichert wird. Es wird nicht weiter beschrieben.

9.7 Firewall der Humboldt-Universität

Die Firewall, die das Rechnernetz der Universität absichert, sichert alle Rechner von Zugriffen aus dem Internet, wenn nicht von den Betreibern andere Regeln aufgestellt werden. Die Firewall wird hier nicht weiter beschrieben.

Für die IT-Komponenten der UB, die im Rahmen des ALMA-Betriebs genutzt werden, sind nur die hier beschriebenen Zugänge von außen definiert. Für die PCs der UB sind

keine Zugänge von außen erlaubt. Alle Kommunikation muss von den PCs ausgehen. Soweit aktuell absehbar gibt es keinen Anpassungsbedarf hinsichtlich der HU-Firewall, um den Betrieb von Alma zu gewährleisten. Sollte Anpassungsbedarf entstehen, wird dieser in diesem SIKO ergänzt.

9.8 Identitäts-Management der HU

Das Identitätsmanagement der Humboldt-Universität (IDM) wird vom CMS betrieben. Es wird hier nicht weiter beschrieben. Der Datenfluss wurde in 7.6 beschrieben.

9.9 Active Directory (Windows-Domain)

Die UB betreibt für ihre Mitarbeiterinnen und Mitarbeiter eine Windows-Domain (die Domain UB). Die Leser der UB, die nicht Angehörige der UB sind, erhalten einen Windows-Account (aus dem Bibliotheks-Account und an diesen gebunden), wenn sie auf den Web-Seiten der UB ihr Password ändern. Damit ist gesichert, dass kein Bibliotheks-Mitarbeiter das Windows-Passwort eines Lesers kennt und missbrauchen kann.

III. Darstellung Universität

10.2. Maßnahmen zur Absicherung der Endgeräte

Mitarbeiter-PCs

Auf den Mitarbeiter-PCs ist Windows-7 installiert. Die Programme und das Betriebssystem werden mit den aktuellen Sicherheits-Patches versorgt. Alle PCs sind Mitglieder der Windows-Domain ub.hu-berlin.de. Über Gruppenrichtlinien werden Veränderungen der Konfiguration der PCs durch die Nutzer unterbunden.

öffentliche Computerarbeitsplätze (UB und CMS)

Die öffentlichen Computerarbeitsplätze (öCAPs) sind nicht direkt in die Verarbeitung von ALMA einbezogen. Über das Discovery-System Primo können sich Leser Daten aus ALMA anzeigen lassen. Sie können an den öCAPs - wie von allen Rechnern der Welt auch - über Primo Leihfristen der von ihnen entliehenen Medien verlängern oder Bestellungen/Vormerkungen auf Medien in ALMA speichern.

Die öCAPs sind entweder Thin-Clients auf der Basis von Linux oder Windows. Sofern von den Herstellern Betriebssystem- und Programm-Patches geliefert werden, werden diese zeitnah auf den öCAPs installiert. Die öCAPs können zum Teil ohne persönliche Anmeldung genutzt werden. Dann ist die Nutzung auf einen Browser beschränkt, der nur Web-Seiten aus dem HU-Rechnernetz anzeigen kann. Wenn weitergehende Internet-Recherche oder andere Programme genutzt werden sollen, muss der Nutzer sich an einer Terminal-Serverfarm des CMS über die Windows-Domäne der HU-Berlin anmelden.

Ausleih-, Rückgabe-, Ausgabe-Automaten

Die Ausleih-, Rückgabe- und Ausgabe-Automaten werden durch Windows-Steuerrechner betrieben. Im Normalbetrieb wird durch ein Programm, das die Kommunikation zwischen dem Leser und ALMA vermittelt, gesichert, dass der Leser nur die Funktionen, Ausleihe, Rückgabe und zum Teil Gebührenbezahlung durchführen kann. Ein Zugriff der Leser auf das Betriebssystem ist nicht möglich. Die an diesen Geräten vorhandenen Tastaturen besitzen keine Funktionstasten. Den Service-Betrieb kann man nur durch die Eingabe von Passwörtern erreichen. In diesem Betriebsmodus ist der Zugriff auf das Betriebssystem in vollem Umfang möglich. Die Passwörter zum Umschalten auf den Service-Mode sind nur den Systemadministratoren der EDV-Abteilung bekannt.

Die Kommunikation dieser Geräte wird über das Protokoll SIP2 geführt. Das Protokoll SIP2 ist unverschlüsselt. Damit die Kommunikation zwischen den Geräten und ALMA nicht abgehört werden kann, wird das SIP2-Protokoll über einen stunnel verschlüsselt.

Die Windows-Betriebssysteme auf den Steuerrechnern werden in Absprache mit den Hersteller-Firmen aktualisiert. Durch die Konfiguration der Windows-Firewall und Ab-

schalten nicht benötigter Prozesse wird ein nicht-autorisierter Zugriff über das Netz unterbunden.

Die Wartung der Ausleih-, Rückgabe- und Ausgabe-Automaten erfolgt zum Teil über Remote-Zugriff. Die Firewall der Humboldt-Universität ist so konfiguriert, dass ein Zugriff nur von autorisierten IP-Nummern erfolgen kann. Der Zugriff auf die Automaten ist auf je eine IP-Nummer der jeweiligen Herstellerfirma (MK-Solutions Systems, Bibliotheca, Lyngsoe) beschränkt. Der Zugriff auf die Geräte erfolgt nur im Wartungsfall.

Server zur Übergabe der Kassen-Logs an das Studentenwerk Berlin

Der Server zur Übergabe der Kassen-Logs an das Studentenwerk Berlin ist ein Linux-Server, der nur mit den Ausleih-Automaten und dem Rechner des Studentenwerks, der die Kassen-Logs abholt, kommuniziert. Das Betriebssystem wird automatisiert mit Sicherheits-Patches versorgt. Der Zugang zu diesem Server ist nur per ssh aus dem Rechnernetz der HU Berlin möglich (Ausnahme: der Rechner des Studentenwerks Berlin, der die Kassen-Logs abholt).

Rechnernetz der Humboldt-Universität, Firewall der Humboldt-Universität, Identitäts-Management der HU und Active Directory (Windows-Domain)

Rechnernetz der Humboldt-Universität, Firewall der Humboldt-Universität, Identitäts-Management der HU und Active Directory (Windows-Domain) werden vom CMS der HU Berlin betrieben und hier nicht weiter beschrieben. *(hier sollen Verweise auf die entsprechenden Sicherheitskonzepte des CMS eingefügt werden - diese sind angefragt)*

10.3. Organisatorische Maßnahmen

Alle Mitarbeiterinnen und Mitarbeiter werden verpflichtet und unterschreiben Verpflichtungen zur Wahrung der Dienstgeheimnisse.

Alle Mitarbeiterinnen und Mitarbeiter werden vor Arbeitsaufnahme in die Funktionen und die Handhabung von ALMA eingewiesen. Bei wesentlichen Updates werden die Schulungen erneut durchgeführt. Bei kleineren Aktualisierungen werden die Mitarbeiterinnen und Mitarbeiter über einen Newsletter über Veränderungen informiert.

Regelmäßig werden Konsistenzprüfungen der Daten durchgeführt, um fehlerhafte Eingaben frühzeitig zu erkennen und zu korrigieren.

Durch die Passwort-Bildungsrichtlinien des CMS werden die Mitarbeiter gezwungen, sichere Passwörter zu bilden und zu nutzen. Alle 12 Monate müssen die Passwörter geändert werden.