Identity Management in der Praxis

Identity Management des Rechenzentrums und der Verwaltung der Universität Freiburg auf Basis von HIS/OpenLDAP und eigenen Werkzeugen

Gerhard Schneider, Dirk von Suchodoletz

Lehrstuhl für Kommunikationssysteme
Rechenzentrum Universität Freiburg
Hermann-Herder-Str. 10, 79104 Freiburg

Zusammenfassung: Identitätsmanagement[1] stellt Organisationen vor neue Herausforderungen. Die Verwaltung von Benutzern und deren Zuständigkeiten erfolgt weitgehend durch EDV, meistens dezentral verteilt über eine ganze Reihe verschiedener Bereiche. Die meisten Vorgänge und Dienste greifen im Hintergrund auf die elektronisch gespeicherten Identitäten zurück. Damit Kosten nicht ausufern und die Sicherheit und Überblick gewährleistet bleiben, ist eine Zusammenführung erstrebenswert. Wegen der unterschiedlichen etablierten Systeme, verteilten Zuständigkeiten und Datenschutzbelangen sind generische Lösungen selten anwendbar. Da sich das Thema in den meisten größeren Einrichtungen stellt, gibt es eine Reihe kommerzieller Lösungen. Eine Alternative besteht in der Zusammenführung verschiedener Systeme unter dem Dach von freien Softwareprodukten kombiniert mit Eigenentwicklungen. Als zentrales Problem kristallisieren sich die notwendigen Konnektoren zu den verschiedenen Systemen heraus. Akzeptanz entscheidend sind die Komponenten der Benutzerselbstverwaltung. Das Rechenzentrum der Universität Freiburg realisiert basierend auf OpenLDAP, Webschnittstellen und selbstentwickelten Konnektoren seit 2001 ein eigenes Identity-Management. Dieses Konzept setzt ein Single-Password für die meisten Dienste um und definiert Flussrichtungen von Datensätzen und ihren Updates.

1 Identity-Management in der Praxis

Die meisten Verwaltungsakte finden an sehr unterschiedlichen Stellen unabhängig voneinander statt. Mit der Einführung von EDV ergab sich erst einmal keine wesentliche Änderung an diesem Konzept, es kamen lediglich neue Dienste hinzu. Die Abwicklung der traditionellen Arbeitsabläufe wurde elektronisch abgebildet. Heute stehen Universitäten und ihre Rechenzentren vor neuen Herausforderungen. Während im letzten Jahrzehnt die Durchsetzung der elektronischen Datenverwaltung an erster Stelle stand, liegt nun die Integration der verschiedenen heterogenen Datenbestände an. An dieser Stelle kommt das sogenannte „Identity Management“, eine zentralisierte Instanz zur Benutzerverwaltung und

[1] Nach Wikipedia.de: Verwaltung von Entitäten (Personen oder Dinge) in einem Unternehmen oder einer Behörde. Ziel ist es, den Vorgang des Zuordnes von systemweit eindeutigen Identifikatoren zu einer die Entität beschreibenden Attributen, wie etwa den Namen, so selten wie möglich (am besten nur ein einziges Mal) durchzuführen.

Authentifizierung, ins Spiel. Dieser Aufsatz beschreibt die praktische Umsetzung eines Identity-Managements mit selbstentwickelten Komponenten und Werkzeugen basierend auf Standardsoftware, wie OpenLDAP und den Tools der Betriebssysteme.

Eine Universität hat aufgabengemäß eine ganze Reihe von Angehörigen. Die nicht unerhebliche Zahl festangestellter Mitarbeiter wird in der Personalbuchhaltung[2] geführt. Diese Personengruppe hat größerenteils einen eigenen Telefonanschluss, verfügt über Schlüssel und Zugangsberechtigungen zu verschiedenen Bereichen. Die weit größere Zahl der Studierenden, die sich über mehrere Fakultäten verteilen, findet sich in der Studierendendatenbank.[3] Studierende müssen sich zu Prüfungen anmelden, arbeiten als Hilfskräfte, bekommen Bibliotheksausweise, Schlüssel zu speziellen Arbeitsräumen, Scheine über bestandene Leistungen ausgehändigt. Zudem ist die Fluktuation systembedingt ziemlich hoch. Die Anforderungen an ein Identitätsmanagement sind also erheblich.

Die globalen Probleme stellen sich in abgewandelter Form auch in Teileinrichtungen, wie dem Rechenzentrum. Die im folgenden geschilderte Ausgangslage trifft sicherlich auf eine ganze Reihe ähnlicher Institutionen mit hohen Mitgliederzahlen und hoher Fluktuation zu. Erschwerend kommt eine dezentrale Verteilung der Aufgaben über die gesamte Institution hinzu. Ein Universitätsrechenzentrum bietet anders als zu Mainframe-Zeiten eine breite Palette verschiedener Dienste basierend auf verschiedenen Plattformen und Systemen an. Hierzu zählen eine ganze Reihe öffentlicher Windows- und Unixsysteme, Emailservices, zentrales Backup, öffentlicher Netzwerkzugang mit Laptop per WLAN, Ethernet, Modem- bzw. ISDN-Einwahl sowie diverse Webservices, wie E-Learning oder elektronische Vorlesungsverzeichnisse. Das Ergebnis hiervon: die Daten sind oft redundant, aber niemals konsistent.

Es ist inzwischen klar geworden, dass die Sicherstellung einer Konsistenz der Datenbestände bereits in einfachen Fällen hohe Kosten verursacht. So ist der Personalaufwand, um beispielsweise einen Studierenden zu exmatrikulieren und damit überall die noch vorhandenen Rechte zu löschen, nicht zu unterschätzen.

2 Rezentralisierung der Datenbestände und Informationsflüsse

Im Rechenzentrum der Uni Freiburg[4] gab es bis zum Jahr 2001 vier verschiedene Nutzerverwaltungen. Die gleiche Situation findet sich auch in anderen Bereichen der Universität. Keine dieser Implementierungen konnte sich gegenüber ihren Konkurrentinnen durchsetzen. Keine kann ohne weiteres aufgegeben werden, da oft wichtige Dienste mit ihr verknüpft sind. Ein Bestandsschutz muss daher gewährleistet sein. Aus den Erfahrungen mit Benutzer- und Datenverwaltung aus allen Universitätsbereichen wurde klar, dass es eine alles umfassende zentrale Lösung nicht trivial geben kann. Dazu sind die Schnittstellen der einzelnen Systeme zu unterschiedlich, und zukünftige Entwicklungen zu wenig vorhersagbar.

[2] Häufig kommt hier das POS-Modul vom HIS (Hochschulinformationssystem), http://www.his.de zum Einsatz.

[3] Die Verwaltung der Studenten erfolgt im SOS-Modul der HIS-Suite.

[4] Webauftritt: http://www.rz.uni-freiburg.de

Das Anheuern externer Experten und die Anschaffung sehr teurer kommerzieller Softwarepakete kam aufgrund der Komplexität und Kosten ebenfalls nicht in Frage. Deshalb realisierte das Rechenzentrum eine Lösung mit eigenen Mitteln. Dazu wurde zuerst eine zentrale Hierarchie definiert und dann in einer hierarchischen, verteilbaren Datenbank nach dem LDAP-Standard umgesetzt. Konzeptionell ist der Aufbau der Zentralinstanz zwar an diesem Modell orientiert, wenn auch nicht überall übernommen oder erzwungen. Anstelle dessen wurden einige verbindliche Festlegungen getroffen:

- Der Fluss der Daten erfolgt von der Spitze an untergeordnete Hierarchien.
- Personen können nur an der Spitze der Datenbank angelegt werden. Jede Hierarchiestufe importiert nur die für sie wichtigen Daten. Der Export von Daten wird gefiltert, so dass keine unnötigen Daten an niedrigere Hierarchiestufen gelangen. Damit wird den Belangen des Datenschutzes Rechnung getragen.
- Betriebs- und systemwichtige Daten werden auf der Hierarchiestufe angelegt, auf der sie benötigt werden. Jede Hierarchiestufe darf importierte Datensätze erweitern, aber keine neuen Datensätze, die äquivalent zu den importierten sind, anlegen.

Organisatorisch ist damit eine Zentralisierung erreicht. Die Zentralinstanz verfügt aber nicht über alle Daten, sondern nur über die für ihre Aufgaben wichtigen. Jedes untergeordnete System kann, wenn die Datensätze ausreichen, direkt mit der Datenbank kommunizieren. Wenn zusätzliche Daten benötigt werden, benutzt eine nachgelagerte Ebene eine eigene Datenbank. Hierbei entscheiden die Betreiber selbst, welche Daten sie benötigen und importieren. Umgekehrt erhalten sie nur für sie relevante Daten.

So erreicht man eine problemlose Integration neuer Dienste, da die zentrale Instanz deren Eigenarten nicht berücksichtigen muss. Die einzelnen organisatorischen Knoten und Abläufe, wie verschiedene Abteilungen der Universität oder abteilungsinterne Aufgaben, werden entflochten.

3 LDAP als zentrale hierarchische Datenbank

Das Prinzip der hierarchischen, verteilten Datenbank ist nichts Neues – viele kennen noch X.500. Eine einfache Lösung ist LDAP (Lightweight Directory Access Protocol). LDAP ist bezogen auf sein Einsatzgebiet nicht einfach aus der Luft gegriffen. Es gibt eine Reihe kommerzieller und OpenSource-Produkte, die auch für diese Aufgabenstellung eingesetzt werden. Viele Systeme bringen eine native LDAP-Unterstützung mit. Microsofts aktuelle Betriebssysteme arbeiten mit einem Active Directory. Dieses ist eine Abwandlung von LDAP, aber in vielen Bereichen direkt kompatibel.

Linux-Systeme sind im Bereich der Benutzerverwaltung LDAP-enabled. Es existiert eine Vielzahl von LDAP-Clients. So können fast alle Browser mit ihren Adressbüchern direkt LDAP als Backend benutzen. Fast alle Programmiersprachen besitzen LDAP-Schnittstellen. Der populäre Webservser Apache kann ebenfalls gegen LDAP authentifizieren.

Ein LDAP-basiertes System zur Daten- und Benutzerverwaltung ist dabei nicht auf kommerzielle Software angewiesen. Für fast alle Aufgabenstellungen existieren Werkzeuge der beteiligten Betriebssysteme oder OpenSource-Implementierungen. Anpassungen können mit freien Softwarewerkzeugen erstellt werden. Die Einbindung kommerzieller Produkte stellt ebenfalls kein Problem dar.

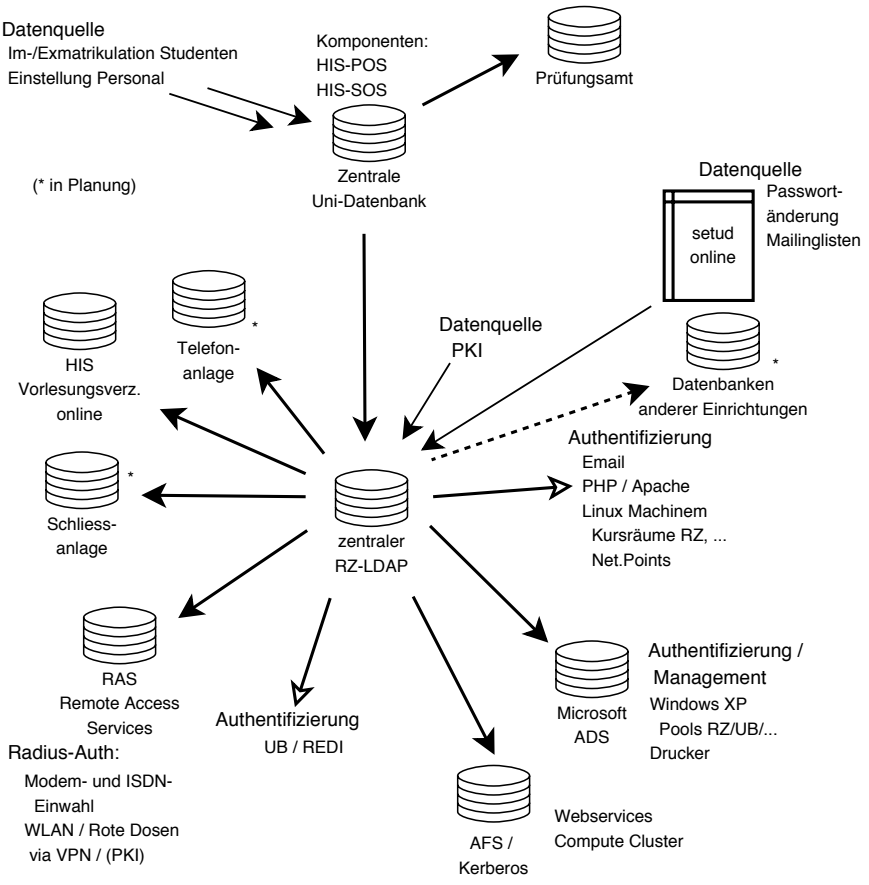

Abbildung 1: Datenflüsse des Identity-Management-Systems in Freiburg

4 Administrative Seite

Dieses Konzept ließ sich naturgemäß nicht „einfach so“ durchsetzen. Die Widerstände waren zu Beginn nicht unerheblich, da Accounts auf lokalen Systemen nur angelegt werden dürfen, wenn sie in der zentralen Instanz vorhanden sind. Die Funktionalität für Benutzer und Administratoren verschlechterte sich anfangs, bis die notwendigen Export- oder Importfunktionen zur Verfügung standen. Die oft mangelnde Kooperation der Betriebssysteme stellte ein weiteres Problem dar. Der Vorzug dieses Ansatzes ist, dass Systeme dabei nicht aufgegeben werden müssen, sondern nur deren Datenbanken aus einer neuen Quelle bestückt werden.

Ziel der Umstellung im Bereich des Rechenzentrums war die Erreichung eines „single-password“. Eine der zentralen Fragen bei der Entscheidung über kommerzielle Lösungen oder Eigenentwicklungen ist die Verfügung von Konnektoren zu verschiedenen Systemen. Kommerzielle Lösungen bringen üblicherweise viele Standardkonnektoren mit. Es gibt

jedoch immer wieder lokale Besonderheiten die in einzelnen Bereichen zu beachten sind. Einige Systeme können direkt gegen LDAP authentifizieren, andere nur gegen einen Export der LDAP-Daten in eine eigene Datenbank.

Zudem gibt es traditionell viele Eigenentwicklungen einzelner Institute, seltene Spezialsoftware oder recht historische Betriebssysteme. Kommerzielle Produkte lohnen sich aus Sicht der Autoren nur, wenn sie eine schnelle AdHoc-Umstellung ermöglichen. Sind Eigenentwicklungen unumgänglich stellen sich offene Systeme und Architekturen als die bessere Grundlage heraus. Dann ist auch der Personal- und Zeitaufwand ein nicht unerheblicher Faktor. Kann dieser nicht weitgehend durch ein kommerzielles Produkt absorbiert werden, sind die oft recht hohen Initial- und Anpassungskosten solcher Produkte langfristig problematisch. Ergibt sich zudem noch ein hoher dauerhafter Betreuungsaufwand, spricht mehr für freie Lösungen mit Eigenentwicklung.

Für viele Organisationen besteht bei der Entscheidung über ein Identitätsmanagement zudem eine politische Dimension. So können zentrale Vorgaben bestehen oder die Bindung an einen speziellen Anbieter aufgrund besonderer Konditionen gefordert sein. Die Arbeitsgruppe am Rechenzentrum in Freiburg beschloss eine zentrale Benutzerverwaltung in Open-LDAP zu realisieren. Abgelehnt wurde eine (teure) kommerzielle Speziallösung, da zu hoher Einführungs- und laufender Aufwand erwartet wurde. Die Anpassung für alte auslaufende Systeme und ausstehende neue Herausforderungen wurde als zu kostenintensiv angesehen.

Trotzdem verzichtete die Arbeitsgruppe nicht auf externe Berater. Diese richteten jedoch nicht das von einem Anbieter propagierte Modell ein, sondern evaluierten die bestehenden Anforderungen zur Umsetzung in OpenLDAP. Dieses diente zur Beschleunigung der Anwendung und Auflösung interner Widerstände. So wurde eine lockere Kopplung der verschiedenen Systeme mit klarer Datenflussrichtung als erstrebenswertes Ziel propagiert. Auf eine umfassende Synchronisation aller Systeme, wie sie oft versprochen, aber selten erreicht wird, wurde bewusst verzichtet. Ebenfalls blieb die zentrale Datenbank frei von starren Rechenzentrumsspezifika. Dadurch liessen sich überschaubar einfache Datenstrukturen in der Zentrale erreichen. Das Ziel wurde mit Erreichung eines „single sign-on“ definiert. Erreicht wurde zumindest ein zentrales Passwort für alle Systeme und Dienste. Die üblicherweise mangelnde Kooperation unterschiedlicher Betriebssysteme und Applikationen macht zwangsläufig Kompromisse notwendig.

Deshalb erfolgt die Passwort-Vergabe nicht mehr auf der Ebene der einzelnen Systeme, sondern direkt auf der für alle Systeme zentralen Datenbank. Das Interface für solche Aufgaben ist am besten eine Webmaske, damit es von einer Großzahl der Plattformen aus bequem aufgerufen werden kann.

5 Die zentrale Komponente

Die zentralen „Objekte“ der zentralen verteilten Datenbank sind die Mitarbeiter und Studenten der Universität. Sie werden durch HIS-POS / HIS-SOS bei der Einstellung oder Immatrikulation erfasst. Mit der Existenz dieser Datensätze werden alle Berechtigungen dieser Person verknüpft. Alle Datensätze bereinigt um sensible Daten werden an den

RZ-LDAP exportiert. In diesem Zuge wird eine zentrale Benutzer-ID generiert. Der RZ-LDAP-Server ist die zentrale Instanz einer ganzen Reihe abgeleiteter Dienste. Mit dem Ausscheiden eines Universitätsmitglieds werden dessen Einträge in der zentralen Datenbank deaktiviert und nach Ablauf einer Frist gelöscht. Dieses setzt sich „nach unten“ durch den RZ-LDAP über die realisierten Schnittstellen ohne aufwändige Eingriffe auf alle Bereiche durch.

Das Rechenzentrum selbst benutzt diese Datenbank, um eine Reihe von Systemen und Diensten direkt zu authentifizieren. Hierzu gehört der zentrale Email-Service, der allen Mitgliedern der Universität angeboten wird. Ebenfalls nutzen alle Linux-Maschinen LDAP direkt zur Authentifizierung von Benutzern. Dieses sind mehrere hundert Geräte in den Pool-Räumen, öffentliche Internet-Terminals und betreute Rechner an anderen Fakultäten. Parallel erfolgt ein Export an einen zentralen Microsoft-ADS. Dieser authentifiziert Benutzer in den Windows-Pools des Rechenzentrums und angeschlossenen Fakultäten. Ebenfalls erfolgt die Freigabe von Druckjobs auf diesem Wege. Gemeinsam mit einem Webinterface zum Management der Account-Daten erreicht das Konzept ein „single-password“ für fast alle Dienste. Zukünftige Migrationspfade zu einem später möglichen „single-sign-on“, basierend beispielsweise auf Kerberos 5, sind eingeplant.

Ein weiterer Export von Daten zur Authentifizierung erfolgt an die RAS-Datenbank. Es gibt eine ganze Reihe Remote Access Services, die einen generellen Zutritt zum Universitätsdatennetz erlauben. Hierzu zählen die Einwahl per ISDN oder Modem und der Zugriff auf das Uni-Netz über WLAN oder ein speziell geschütztes öffentlich zugängliches Ethernet. Diese Zugriffe reguliert ein Cisco-VPN-System. Alle drei Dienste benutzen hierfür ein Radius-Backend. Dieser Radius-Server bildet gleichzeitig die Grundlage für den Aufbau einer BelWü-[5] und DFN-weite Roaming Funktion.

6 Benutzerselbstverwaltung mittels Webschnittstelle

Die Benutzerselbstverwaltung ist eine zentrale Komponente der Freiburger Lösung. Passwortänderung erfolgen nicht innerhalb der einzelnen Systeme, sondern über eine WWW-Maske. Neue Passwörter wirken auf direkt angeschlossene Betriebssysteme und Applikationen sofort. Allen anderen werden sie „beigebracht“. Diese Aufgabe übernehmen an der Universität Freiburg entwickelte Konnektoren. Diese Konnektoren müssen dabei nicht von der Identity-Management-AG erstellt werden. Die Verlagerung an die einzelnen System- und Applikationsadministratoren erlaubte „einfache“ Lösungen. Einige Synchronisationen laufen nachts als Batch-Jobs im Hintergrund.

Ein möglichst eleganter Zugang zu den gespeicherten Daten ist Voraussetzung für die Akzeptanz seitens der Nutzer. Deshalb fiel die Wahl der Schnittstelle auf ein Webinterface. Dieses ist ausreichend plattformunabhängig und hinreichend sicher durch SSL/TLS. Die Maske ist direkt von der RZ-Homepage zugänglich. Sie ergänzt damit das Serviceangebot und verbessert die Wahrnehmung der weiteren WWW-Angebote. Die Authentifizierung

[5] Bezeichnet das Badenwürttemberg extended LAN (http://www.belwue.de). Dieses verbindet die Hochschulen und Forschungseinrichtungen des Landes untereinander und mit dem DFN.

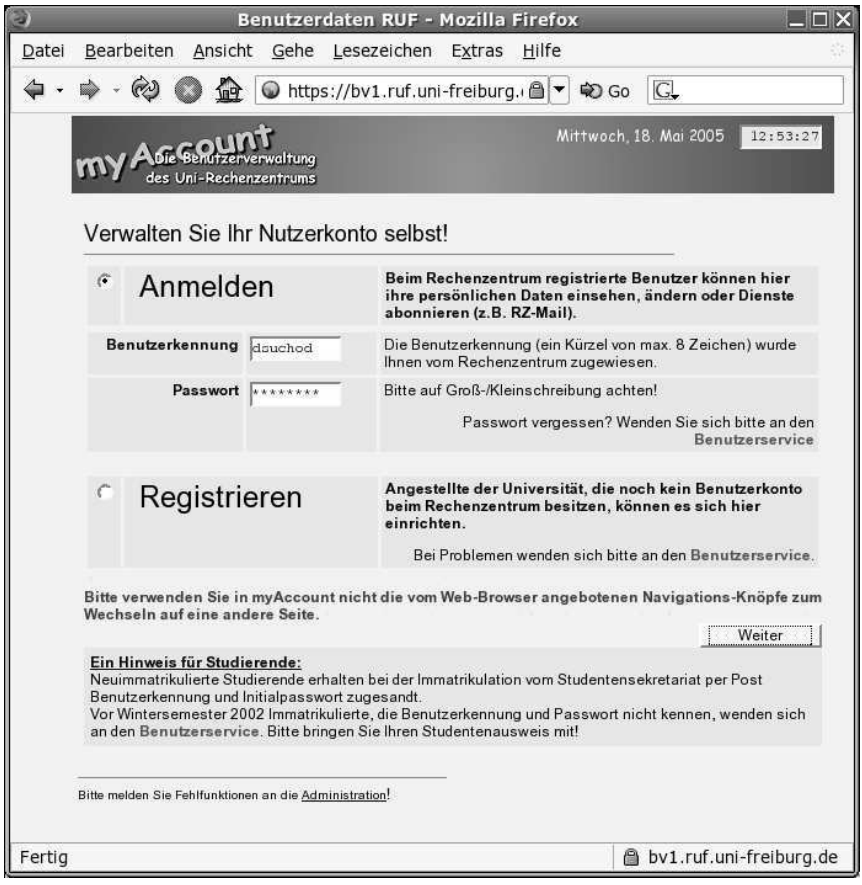

Abbildung 2: Anmeldung an der Account-Selbstverwaltungsschnittstelle mit RZ-Benutzername und Passwort

über die RZ-Userid und das Passwort wurde als ausreichend befunden. Spätere Erweiterungen und Verfeinerungen sind jedoch nicht ausgeschlossen. Ein Webinterface für solche Zwecke ist eigentlich ein uralter Hut, aber erprobt und breit im Einsatz. Es ersetzt die Passwortdialoge und ID-Management-Tools der einzelnen Systeme. Das Ergebnis ist nicht gerade „state-of-the-art“, aber funktional. Es schafft die Grundlage für die weiteren Lösungsansätze:

- Neue oder weitere Dienste lassen sich unproblematisch einbinden.
- Die Accountvergabe erfolgt möglichst im do-it-yourself-Verfahren oder automatisch. Studierende werden bei der Immatrikulation automatisch aus HIS-SOS importiert. Mitarbeiter können sich selbst einen Account erstellen, da sie in der Personaldatenbank bzw. HIS-SOS bekannt sind.
- Je mehr Daten ein Benutzer selbst eingeben kann, desto geringer ist der Gesamtaufwand für das Rechenzentrum.

Zur Datenvervollständigung werden alle relevanten und unkritischen Daten aus den hierarchisch „höher liegenden“ Datenbanken HISPOS/SOS importiert. Zur Absicherung des Verfahrens und Kontrolle seitens der Nutzer erhalten alle Account-Neuinhaber einen Brief mit dem Erstpasswort.

Die Benutzerselbstverwaltung umfasst:

- das Setzen und Verteilen von Passwörtern Abonnieren verschiedener RZ-Dienste, wie Login und Homeverzeichnis, Webdienst (AFS), RAS / WLAN
- Mail-Adressenverwaltung mit Hauptadresse und weiteren
- TSM-Steuerung[6]
- Verwaltung von Zusatz- und Rollenaccounts

Das beschriebene Webfrontend mit der LDAP-Datenbank im Hintergrund schaffte die Voraussetzungen für eine breite Akzeptanz. Inzwischen erfolgt ein Export der Daten an die Microsoft ADS,[7] an die Universitätsbibliothek, den Mailserver, die AFS/Webservices.[8] Eine direkte Authentifizierung erfolgt für die Linux-Maschinen (Login, Kurs- und Pool-Räume). Zusätzlich erlaubt das Konzept einfache Webauthentifizierung für vielfältige Dienste wie CMS[9] oder Raumverwaltung. Eine Verbindung mit Telefonanlagenfunktionen ist geplant und eine Integration mit der Siemens-Schliessanlage beauftragt.

Für die Webschnittstelle wird eine eigene Linuxmaschine betrieben. Diese ist im Augenblick ein P4 1.8 GHz System unter SuSE-Linux 9.0. Installiert sind OpenLDAP, ein Apache-Tomcat-Server und Java. Das Webinterface umfasst inzwischen ca. 15.000 Zeilen Code, 50 eigene Klassen, Format-Output ...

Seit der Einführung gibt es eine zunehmende Nutzung der zentralen Benutzerverwaltung. Mit dem Import der Daten in die Microsoft ADS erlaubt dieses eine Übernahme von Nutzerdaten in die Verwaltung von Instituts-ADS-Inseln. Eine lokale Nutzerverwaltung ist nicht mehr nötig. Accounts müssen vor Ort nur noch „freigeschaltet“ werden. So erfolgt beim Ausscheiden eines Nutzers eine automatische Löschung auch an den beteiligten Instituten. Für viele Administratoren ergab sich die Erkenntnis: Man kann offenbar eigene Daten authentifiziert selbst verwalten, ohne dafür einen großen Aufwand selbst treiben zu müssen. Zukünftige Bereiche könnten sich beispielsweise auf die Verwaltung der eigenen Telefonnummer erstrecken.

Damit ergeben sich klarer Datenfluss und Zuständigkeiten bei überschaubaren Abhängigkeiten. Zwei wesentliche Arbeitsbereiche lassen sich abgrenzen: Wartung und Pflege der LDAP-Datenbank und Weiterentwicklung der Webschnittstelle. Beide Aufgabenbereiche entsprechen im Arbeitsumfang einer knappen halben Stelle. Interessenten an einer Benutzerverwaltung müssen Konnektoren selbst erstellen. Sie können dabei aber auf einen umfangreichen Pool frei verfügbarer Lösungen und Entwicklungen des Rechenzentrums zugreifen. Die Kosten fallen durch diese Form der Delegation bei den späteren Nutzniessern

[6] Tivoli Storage Manager – Backup/Archiv Dienst

[7] Der Active Directory Server wurde mit Windows2000 eingeführt.

[8] Das Rechenzentrum Freiburg bietet seinen Nutzern das Andrew Filesystem als Grundlage zum Einstellen der Web-Inhalte an.

[9] Content Management Systeme gewinnen auch an Universitäten für die zunehmenden Mengen von Webinhalten an Bedeutung.

an. Ungeachtet dessen ergibt sich eine hohe Kostenentlastung bei Poolbetreibern durch die Vereinfachung des eigenen Betriebes. Dieses gilt ebenfalls für den deutlich reduzierten Aufwand, den Webadministratoren für zugriffsbeschränkte Dienste treiben müssen. Die Übernahme der RZ-Accounts entlastet sie von der Benutzerverwaltung. Es muss lediglich die Freischaltung des Dienstes selbst übernommen werden.

Die gut funktionierende Benutzerverwaltung schafft bedienbare „Begehrlichkeiten“. So wurde die Integration mit dem HIS-Vorlesungsverzeichnis erfolgreich realisiert. Ein Selbsteintragen von Studierenden in Seminar- und Kurslisten wird möglich. Die Verbindlichkeit durch Authentifizierung steigt: Spasseinträge und Einträge auf Verdacht werden unterbunden. Die Verwaltung von Leihgeräten (Laptop-Pool) könnte vereinfacht und eine Integration mit einem Webshop in vertretbarem Aufwand programmiert werden. Eine Integration der bestehenden Benutzerverwaltung mit der Uni-PKI wird derzeit evaluiert. Der Aufwand sollte im vertretbaren Rahmen bleiben. Alles in allem wurde eine solide Grundlage für ein noch anzustrebendes „single-sign-on“ geschaffen.

7 Fazit

Die vorgestellte Lösung entspricht sicherlich nicht in allen Punkten dem, was man sich üblicherweise von einer Identitätsverwaltung verspricht oder von dieser fordert. Hierin besteht jedoch häufig ein nicht zu unterschätzendes Problem: Hohe Anforderungen, erstellt von einer vielzahl verschiedener Interessengruppen und organisatorischen Teilstrukturen, verhindern sehr oft eine zeitnahe Umsetzung. Allein zwischen der Definition und der ersten prototypischen Umsetzung vergeht soviel Zeit, dass alte Forderungen obsolet wurden und neue auftauchen. Das verhindert, dass ursprünglich ehrgeizige Projekte zu ihrem anvisierten Ziel geführt werden.

Die Umsetzung am Rechenzentrum Freiburg wurde zu einer Erfolgsgeschichte. Der „große Wurf“ wurde von vorneherein vermieden und Maximalforderungen abgewehrt. Auf diese Weise konnte die Migration in sinnvollen Zeiträumen abgeschlossen werden. Teure Experten halfen beim Projekt-Anschub, implementierten aber keine kommerzielle Lösung die nur sie selbst pflegen können. Modularität und Simplizität waren wesentliche Erfolgsfaktoren. Der Verzicht auf überkomplexe Synchronisationsprozesse vermied die Fallen, in die ambitionierte Projekte immer wieder geraten.

Die Nachteile sollen aber keineswegs verschwiegen werden: Anders als bei den meisten kommerziellen Lösungen funktioniert die Passwortverteilung nicht für alle Dienste in Echtzeit. Alle Systeme, wie Linux oder Webschnittstellen, die direkt LDAP ansprechen werden sofort bedient. Für eine ganze Reihe weiterer wichtiger Server, wie die Microsoft-ADS läuft die unidirektionale Synchronisation zeitverzögert.

Die unidirektionale Flussrichtung der Information und die Wahl einer offenen Datenbank erlaubt es Konnektoren recht einfach zu erstellen. Dabei mussten besondere Wünsche und Anforderungen von den jeweiligen System-Administratoren lokal realisiert werden. Durch diese Festlegung bleibt auch die Größe der Datensätze überschaubar. Für ein bestimmtes Betriebssystem oder eine Applikation nichtnotwendige Daten werden gar nicht erst importiert. Das vereinfacht den Datenschutz, da eine „allwissende“ Zentralinstanz vermie-

den wird. Nur notwendige Daten wandern an untergeordnete Einheiten. Applikationsspezifische Informationen und Einstellungen hingegen existieren nur im System vor Ort. Die zentralen Datensätze lassen sich bereits durch eingebaute LDAP-ACLs schützen, so dass auch hier aufwändige Speziallösungen unterbleiben.

Von der verwaltungsrechtlichen Seite her wurde in großen Teilen der Umsetzung auf „Kann-Regelung“ gesetzt und „Zwang“ vermieden. Das beförderte die langfristige Akzeptanz und baute Widerstände ab. Die Betreuung und Administration des laufenden Systems halten sich in Grenzen. Bekannte Software-Komponenten, die von vielen Admins beherrscht werden, verbessern die Wartungssituation. Ebenfalls müssen sich die Administratoren der Zentralinstanz nicht um die „Betreuung fremder Daten“ kümmern. Dieses erledigen die Zuständigen vor Ort.

Verschiedene Lösungsansätze werden im Rahmen von Praktika und Studienarbeiten am Institut für Informatik erprobt. Das erlaubt zum einen realistische Aufgabenstellungen für die Studierenden, zum anderen kann es dazu beitragen den Entwicklungsaufwand im eigenen Haus zu reduzieren. Die laufenden Software-Kosten sind gering, da keine Lizenzgebühren für die zentralen Komponenten anfallen. Vermutlich muss der geleistete Aufwand mit OpenLDAP etwas höher angesetzt werden, als mit einer kommerziellen hierarchischen Datenbank. Das freie LDAP erlaubt dafür den Betrieb auf kostengünstiger Standard-Hardware und kostenlosem Betriebssystem wie Linux. Eine feste Anbieterbindung unterblieb. Aus strategischer Sicht wird zentrales Know-How im Rechenzentrum selbst aufgebaut und muss nicht teuer zugekauft werden. So kann die zentrale Einrichtung Rechenzentrum selbst wieder als Dienstleister für Beratung und Umsetzung gegenüber Instituten und der Universitätsverwaltung auftreten.