Das Identity Management an der Universität Konstanz – eine Chronologie

Michael Längle
Andreas Schnell

Was ist eigentlich Identity Management?

IT-Anwendungen speichern Daten unabhängig, ob diese in Form von Dateien auf einer Festplatte oder zum Beispiel als Prüfungsdaten in einer Datenbank vorliegen. Nicht jeder soll aber das Recht haben unbeschränkt auf diese Daten zuzugreifen oder sie auch noch verändern zu können. Deshalb muss jede Anwendung genau verwalten, welche Person berechtigt ist, welche Daten zu sehen, zu verändern oder auch löschen zu dürfen. Die Verwaltung dieser Berechtigung nennt die IT „Autorisierung". Bevor aber Rechte verwaltet werden können, muss die Anwendung wissen, wer sie eigentlich benutzt. Die Person muss sich also bei der Anwendung anmelden oder authentifizieren.
In einer Organisation wie der Universität können die Personen aber nicht nur eine Anwendung nutzen, sondern viele unterschiedliche. So können sich MitarbeiterInnen an ihrem Arbeitsplatz anmelden, haben Zugang zu Mails, können mit mobilen Geräten das WLAN nutzen usw. Neben MitarbeiterInnen nutzen auch weitere Personengruppen die Anwendungen, z.B. Studierende, Gäste, Externe, Kooperationspartner usw. Um sicherzustellen, dass alle Personen jederzeit, die für sie notwendigen Anwendungen nutzen können, bedarf es einer zentralen Verwaltung all der Personendaten. Diese Aufgabe übernimmt das Identity Management.

Identity Management an der Universität Konstanz begann vor mehr als 15 Jahren. Damals wurden in der Beratung des Rechenzentrums die Personendaten neu immatrikulierter Studenten für einen E-Mail-Account zusätzlich neu in einer Maske von Hand erfasst, weshalb sich in der ersten und zweiten Semesterwoche regelmäßig eine Personenschlange vom Beratungsraum bis ins V5-Foyer hinzog.

Einem Kollegen aus dem Netzwerkbereich ist es zu verdanken, dass sich das umständliche Vorgehen optimieren ließ: Er hatte als Erster die Idee, die Systeme so zu vernetzen, dass Prozesse automatisiert werden konnten. Denn die notwendigen Attribute zur Erzeugung einer E-Mail-Adresse (primär Vorname und Nachname) waren ja bereits in den Systemen der Verwaltung vorhanden. Das Ziel war, diese zu nutzen, damit Daten nicht doppelt von Hand erfasst werden mussten. Mit einem täglichen elektronischen Abgleich der Daten aus der Verwaltung wurde dieser Prozess automatisiert.
In einem weiteren Schritt wurden die Account-Daten für Studierende direkt auf den Leporello gedruckt und mit diesem versandt. Damit war die erste Form eines Identity- Management-Systems geboren zu einer Zeit, als es den Begriff dafür noch gar nicht gab.

Die automatisierte Bereitstellung der Zugangsdaten (E-Mail-Adresse + Passwort), die anfänglich nur für das E-Mail-System gedacht war, erfolgte frühzeitig auf Basis von allgemeinen technischen Standards. Dadurch konnten ohne große Änderungen an der IDM-Infrastruktur weitere Anwendungen angeschlossen werden, eine eigene Nutzerverwaltung blieb dadurch erspart. Inzwischen machen mehr als vierzig Anwendungen Gebrauch davon.

Die Herauslösung einer eigenen Nutzerverwaltung für die jeweilige Anwendung warf die Frage auf, ob dieser Schritt nicht auch über den Campus hinaus möglich wäre.
Die Technik dazu heißt Shibboleth - der Name stammt vom hebräischen Wort Schibboleth und bedeutet wörtlich „Getreideähre", wird aber im übertragenen Sinn heute auch in der Bedeutung von „Kennwort" oder „Codewort" verwendet - und wurde zuerst im Bibliotheksbereich eingesetzt. Dank dieser Technologie konnten Elektronische Journale erstmals nicht mehr mit einem separaten Registrierungsprozess, sondern mit den Zugangsdaten der Uni Konstanz genutzt werden.

2009 wurde in einem Artikel „Auth/Aut/Sig, IDM, LDAP und Shibboleth: Ein KIM-Projekt", das Potential dieser Technologie aufgezeigt:
„...Vielleicht ist es noch zu früh, um zu prophezeien, dass zukünftig Studenten unserer Partneruniversität Tongji vom fernen Shanghai aus Online-Seminare der Universität Konstanz besuchen, elektronisch Prüfungen ablegen und in ihrer Heimat diese Leistungen

anrechnen lassen können. Jedoch die organisatorischen und technischen Vorbereitungen für eine internationale Authentifizierungs- und Autorisierungsinfrastruktur sind bereits in vollem Gange."

Nach weiteren drei Jahren formulierten die vier Universitäten Karlsruhe, Ulm, Freiburg und Konstanz gemeinsam einen Antrag an das Ministerium für Wissenschaft und Kunst mit dem Ziel, auch komplexeren landesweiten Diensten dieselbe einfache Art der Authentifizierung und Autorisierung, basierend auf Shibboleth, zu ermöglichen. Dazu gehören u.a. der UniCluster, der ForschungsCluster sowie bwsync&share.
Das Projekt wurde durch das MWK bewilligt, nannte sich bwIDM und wurde 2013 erfolgreich abgeschlossen. Komplizierte, selbst für Fachpersonal nur schwer verständliche Registrierungsprozesse gehörten von da an der Vergangenheit an.

IT-Systeme unterliegen einem ständigen Wandel. Hardware, Betriebsysteme, Datenbanken, Anwendungen, alles verändert sich mit dem stetigen Wunsch nach weiteren Funktionalitäten und mehr Leistungen. Im Jahr 2011 (und vermutlich schon davor) war klar, dass das bisherige BIS (BenutzerInformations-System) weitere Funktionen braucht. Das System war mit 18 Jahren Laufzeit allerdings nicht volljährig geworden, sondern hat eher das IT-Rentenalter erreicht. Gleichzeitig wurde die Basissoftware für das BIS vom Hersteller abgekündigt. Damit war klar, dass eine weitere Entwicklung auf dieser Basis nicht mehr möglich sein wird. Es musste also was Neues her.

Aber was? In solchen Fällen ist es gut einmal Bestandsaufnahme zu machen. Was hat bisher gut funktioniert, was brauchen wir nicht mehr, was können wir besser machen, welche Systemarchitektur wollen wir einsetzen, usw.? Ein Projektteam wurde gegründet und ein Ziel formuliert. Das Identity Management speichert selbst vergleichsweise wenig Daten, sondern verteilt und synchronisiert Daten von unterschiedlichen Systemen. Diese Datenstrukturen wurden erfasst und dienen heute noch als Basis für andere Projekte. Darauf basierend wurde ein Datenmodell erstellt, Schnittstellen zu den unterschiedlichen Systemen beschrieben und Prozesse aufgestellt (wie kommt eine Person zu einem Account, welche Daten können sich z.B. durch Heirat ändern, was passiert, wenn die Personen die Universität wieder verlässt). Dazu wurden Geschäftsregeln erstellt, wie zum Beispiel ein Loginname automatisch aus dem Vornamen und Nachnamen generiert wird, was passiert, wenn zwei Personen den gleichen Namen haben oder der Name einfach sehr lang ist, usw. Und natürlich wollen die Daten auch verwaltet werden und müssen irgendwo angezeigt werden, zum einen für den Support, zum anderen aber auch für eine Person, um zum Beispiel das Passwort ändern zu können.

Also wurde am Anfang ziemlich viele Dokumente geschrieben, um das zu dokumentieren und festzulegen. Parallel dazu haben wir uns beraten lassen, um eine neue Systemarchitektur zu finden. Hier konnten wir eine sehr moderne Software-Plattform auf Open Source Basis finden. Im Laufe des Projektes haben wir hier auch das Betriebskonzept ausgearbeitet: wie sieht die Hochverfügbarkeit aus, welche Systeme brauchen wann ein Backup, was passiert, wenn ein System ausfällt usw?
Insgesamt sind an der gesamten Architektur über 10 einzelne Systeme beteiligt (parallel zum Produktivsystem gibt es das vergleichbar auch noch als Testsystem). Also insgesamt sehr komplex.

Nach den Dokumenten ging es dann an die Umsetzung. Die stellte sich als schwierger heraus, als wir uns das vorgestellt hatten. Hauptproblempunkt war die Datenqualität der führenden Systeme. Hier gab es immer wieder Überraschendes zu entdecken, zu lernen und dann entsprechend mit dem System umzusetzen. Häufig mussten neue Lösungen gesucht und dann erst auf die Machbarkeit geprüft werden. Das machte eine Abschätzung „wo stehen wir im Projekt?" nahezu unmöglich. Es war sehr viel Detailarbeit zu leisten, viele Systeme mussten neu aufgesetzt und betrieben werden. Die unterschiedlichen Daten aus den führenden Systemen immer wieder eingespielt und getestet werden. Das Team veränderte sich während des Projektes. Wir hatten immer wieder Begleitung durch einen externen Consultant, der uns in vielen Bereichen beraten und helfen konnte. Ein Kollege aus dem FB Informatik unterstützte uns tatkräftig (und tut das immer noch) bei der Prüfung der Datenqualität. Seine automatisierten Skripte prüfen regelmäßig die Konsistenz von tausenden von Datensätzen auf unterschiedlichen Systemen und zeigen, wo noch Schwächen oder Probleme liegen.

Im letzten Jahr hatten wir uns dann einen GoLive-Termin im November gesetzt, da die Datenqualität und die Tests der Datenmigrationen sehr erfolgversprechend aussahen. Auf der Zielgeraden machten uns die Zielsysteme technische Probleme, so dass wir entschieden, in den Pilotbetrieb einzusteigen, um die Systeme beobachten und die Probleme lösen zu können. Mit Hilfe des Software-Herstellers konnten die Probleme gelöst werden und im Februar war es dann soweit, dass wir das Kernsystem live nehmen

konnten. Einzig sichtbare Änderung für den Nutzer ist die Webseite zum Anzeigen der persönlichen Daten und zum Ändern des Passwortes.

Aktuell betreiben wir das neue IDM-System und noch Teile des alten BIS-Systems parallel. In den nächsten Wochen werden rund 40 Anwendungen von den alten Zielsystemen auf neue Zielsysteme umziehen. Dann können auch die letzten Überreste des bisherigen BIS-Systems abgeschaltet werden.

Lange haben wir gezweifelt, ob das neue System in Betrieb gehen kann. Viele, viele Probleme waren zu lösen, doch am Ende war der Übergang zur Version 1.0 des neuen Identity Management sehr unspektakulär und lief dank der super Vorbereitung einfach durch. Ein großes Lob und Dank an das gesamte, tolle Projektteam, das diesen Erfolg so möglich gemacht hat.

Es wurden rund 18.000 Accounts migriert, 3.000 - 4.000 pro Jahr kommen neu dazu, es werden Daten über neun sehr unterschiedliche Datenschnittstellen synchronisiert, es authentifizieren sich Nutzer über viele tausend Zugriffe auf die Zielsysteme pro Woche, viele IT-Arbeitsplätze autorisieren sich über die Zielsysteme, usw.

Mit der Version 1.0 wurde die Basis für ein neues Rückgrat für Authentifizierung und Autorisierung aller elektronischen Dienstleistungen an der Universität geschaffen. Wie beim Fussball gilt aber auch hier, „nach dem Spiel, ist vor dem Spiel“. Nach Abschluss der Restarbeiten für die Version 1.0 haben wir bereits eine große Anzahl an Wünschen und Ideen für die Version 2.0. Mit diesem Team werden wir auch das sicher erreichen.

1 Bericht in Bibliothek Aktuell 89/2009,
https://ojs.ub.uni-konstanz.de/ba/article/view/3181/2983