Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

RECHENZENTRUM

6 Jahre Identity Management an der Julius-Maximilians-Universität Würzburg

Sylvia Wipfler
Rechenzentrum, Universität Würzburg

Projektstart

- Projektstart: 1. Oktober 2006
- Einführungsphase 3 Jahre
- Gründe: Wunsch nach einem ldap-basierten Verzeichnis, das umfangreiche und korrekte Benutzerdaten bereitstellt; Vereinheitlichung und Vereinfachung und Automatisierung der Benutzerverwaltung
- Produkt: Novell Identity Manager

Ausgangssituation

- Ldap-Server nur im eDirectory für File und Print vorhanden
- Nur sehr wenige Daten per Ldap verfügbar (Nachname, Vorname, Account-Name, E-Mail-Adresse)
- Benutzerdaten in Oracle-Datenbank
- Zugriff auf die Daten für die Benutzerverwaltung über MS Access (Formulare, Code) und Datenbank-Skripte auf weiteren Systemen
- Zwei weitere Anwendungen, Ticket-System und Web-Shop verwenden diese Daten
- Auch bei Einführung eines Verzeichnisdienstes müssen Benutzerdaten weiterhin in der Datenbank vorhanden sein; Benutzerverwaltungs-Frontend kann zunächst weiter verwendet werden

Stand Benutzerverwaltung 2006

- Erfassung der Daten teilweise automatisiert
- Täglicher Datenaustausch mit der Studentenkanzlei
- Speicherung der Personen- und Account-Daten bei Studierenden automatisch, aber Aktivierung durch einen Mitarbeiter in der Beratung
- Erfassung der Daten von Beschäftigten und Sonstigen (Gäste) von Hand mit Antragsformular
- Automatische Verlängerung der studentischen Accounts semesterweise
- Alle anderen Accounts mussten jeweils am Jahresende verlängert werden
- mehrere Accounts pro Benutzer

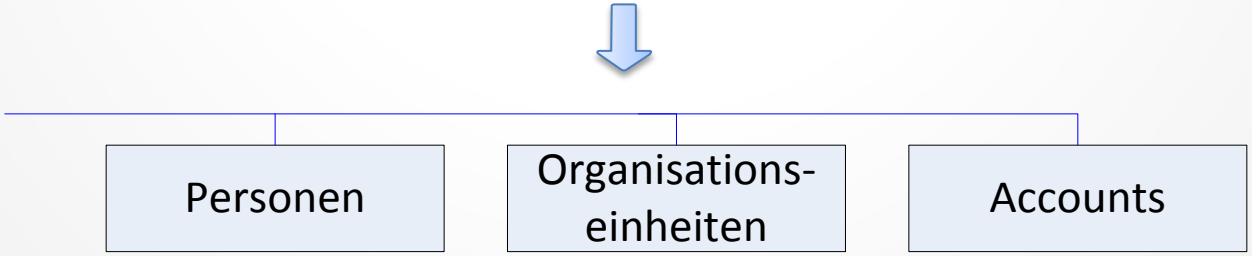
Erste Schritte

- Grundsätzliche Überlegungen zu
  - Umfang der speichernden Daten,
  - Datenquellen,
  - Struktur des zukünftigen Verzeichnisdienstes (flach oder hierarchisch),
  - Planung der einzelnen Schritte
- Vorstellung des Projekts in der Universität (Datenschutz, Personalrat, Studentenkanzlei, Personalabteilung)
- Erfahrungsaustausch mit anderen Rechenzentren

Erste Anforderung

- Beschluss der Hochschulleitung auf gedrucktes Vorlesungsverzeichnis und Personalverzeichnis zu verzichten
- Anforderung: Telefon- und Emailverzeichnis im Intranet/Internet

- Start des Identity Management zunächst nur mit Personendaten und Organisationseinheiten
- Entscheidung für Verzeichnisdienst mit einer flachen Struktur



Aufbau IDM

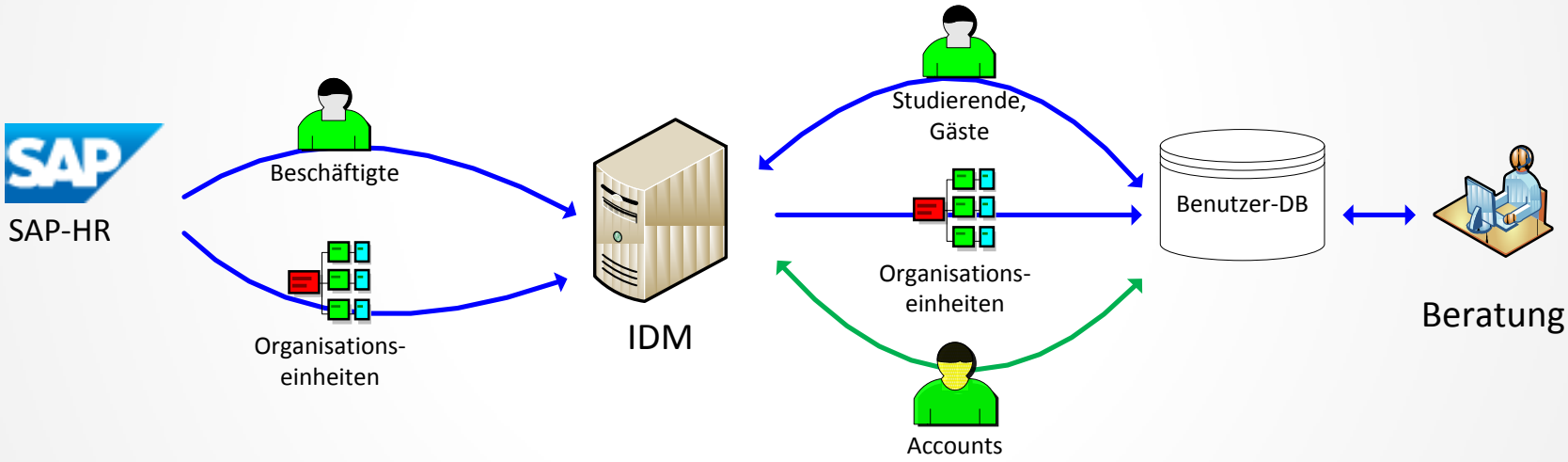
- Anbindung des Personalverwaltungssystems SAP-HR (csv-Files) und Import von Personendaten und Organisationseinheiten
- Programmierung der Web-Anwendung Telefon- und Email-Verzeichnis und Veröffentlichen der ersten Version
- Datenschutzfreigabe, Dienstvereinbarung
- Abfrage des Geburtsdatums bei der Account-Verlängerung 2007/2008
- Anbindung der Benutzerdatenbank
- Datenabgleich (matching) SAP-Daten mit bisher vorhandenen Daten und Aktualisierung der Personendaten in der Datenbank
- Import aller weiteren Personendaten (Studierende, Gäste) aus der Datenbank
- Daten der Gäste werden auch in Zukunft von Hand erfasst

Accounts

Ziel: Alle Accounts sollten möglichst schnell im IDM vorhanden sein, um das Anlegen und Aktualisieren in Zielsystem zu vereinfachen

- Verwaltung der Accounts (Anlegen, Sperren, Löschen) weiter über bestehende Benutzerverwaltung, da es eingespielte Abläufe gab
- Import der Accounts aus der Benutzerdatenbank in das IDM und von da aus weiter in die Zielsysteme

Anbindung Benutzerdatenbank



Anbindung Zielsysteme

- Nachdem alle Accounts im IDM verfügbar waren, konnten Zielsysteme angebunden werden:
- eDirectory File- und Print

  Voraussetzung: Einführung Universal Passwort mit neuer Passwort-Policy

  Entscheidung für „weichen Übergang“, alte Passwörter wurden übernommen, Passwort-Policy nur bei neuen Passwörtern
- Ldap-Adressbuch für E-Mail-Clients
- Moodle Systeme
- VoIP Datenbank

Authentifizierungs-Server

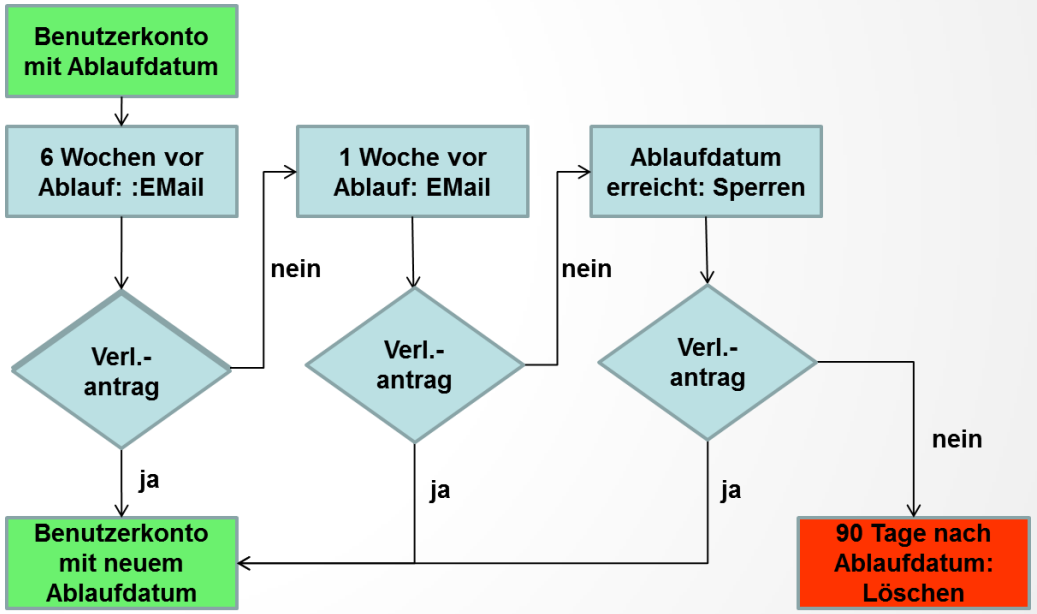
- Aufbau Authentifizierungs-Server für ldap- und Shibboleth-Anwendungen
- Weiteres eDirectory
- Nur Accounts und Gruppen werden synchronisiert
- Nur Accounts mit gültigem Passwort wurden übernommen
- Benutzer mit altem Passwort wurden aufgefordert ihr Passwort zu ändern
- Umzug der ldap-Dienste auf den Authentifizierungs-Server (Webmail, Imap, WLAN/VPN, sb@home …)

Workflow für Accounts

- Prozesse zur Accountverwaltung wurden neu definiert und vereinheitlicht
- Beschäftigte (Personalabteilung) und neu immatrikuliert Studierende erhalten automatisch einen unbefristeten Account mit Standard-Berechtigungen (Mailbox, Home-Directory, WLAN/VPN, VoIP-Telefonnr. für Beschäftigte)
- Verliert ein Mitarbeiter den Status Beschäftigter bekommt der Account ein Ablaufdatum und kann als Gastaccount weitergeführt werden
- Studentische Accounts bekommen nach der Exmatrikulation ein Ablaufdatum, bleiben aber noch ein Jahr für die Dienste E-Mail, sb@home, eLearning freigeschaltet

Workflow für Accounts

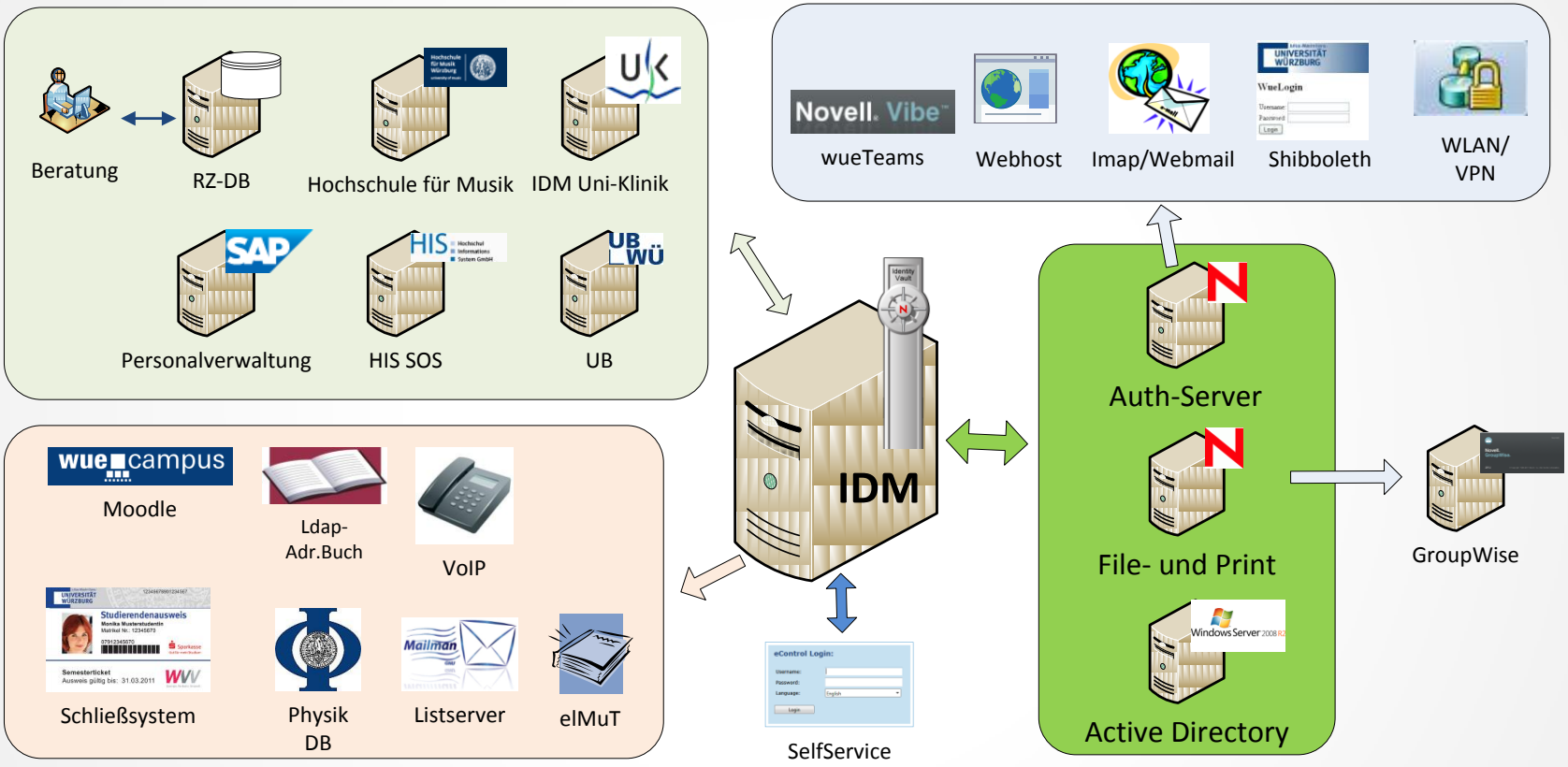
- Gäste bekommen auf Antrag einen zeitlich befristeten Account (max. 1 Jahr), der verlängert werden muss



- Neu: Funktions-Accounts gehören keiner Person sondern der Organisationseinheit
  Ansprechpartner (Verwalter) ist im Account hinterlegt
  Verwalter darf Accounts weitergeben und Passwort ändern

Optimierung und neue Systeme

- Neuanbindung SAP-HR, von Text-Treiber zu SAP-Treiber
  bessere Verarbeitung zukünftiger Ereignisse und mehrerer Beschäftigungsverhältnisse
- Direkte Anbindung HIS-SOS
  zusätzliche Attribute (dfnEduPerson), Erleichterung Datenexport in die Studentenkanzlei
- Einführung einer neuen Chip-Karte für Studierende
- UB Stadtbenutzer
- Hochschule für Musik, IDM der Uni-Klinik
- Neue Version Telefon- und E-Mail-Verzeichnis
- Aufbau SelfService



2006 Projektstart

2007 Projektvorstellung, Datenschutz, Personalrat, Anbindung SAP-HR, Email- und Telefonverzeichnis

2008 Anbindung Benutzerdaten-Bank, Datenabgleich, Mailinglisten

2009 Universal Passwort, eDirectory (File und Print), Authentifizierung-Server, Ldap-Adressbuch, Moodle, VoIP Datenbank, Mail-Systeme

2010 Accountverwaltung Zutrittskontrolle CiP-Pools

2011 Neuanbindung SAP HR und HIS SOS Chip Karte für Studierende, Neues Schließsystem, Webhost-Server, HfM, Uni-Klinik, UB Stadtbenutzer

2012 Active Directory, SelfService, Alumni,

Fazit

- Es ist von Vorteil möglichst schnell ein vorzeigbares Ergebnis zu haben
- Bewährt hat sich die Aufteilung in überschaubare Teilschritte
- Für Änderungen von denen viele Benutzer betroffen sind (Passwort) längere Zeiträume einplanen
- Enge Zusammenarbeit mit anderen Abteilungen ist notwendig
- Organisatorische Abläufe müssen klar definiert sein

Fragen ?