Identity Management – vom Prozess zur Implementierung

Björn Bröhl – OPITZ CONSULTING Gummersbach GmbH

In vielen Medien ist zur Zeit verstärkt die Rede von Identity Management oder kurz IDM. Der Artikel zeigt, was sich dahinter verbirgt.

Schaut man bei Wikipedia nach, findet man unter anderem folgende Antwort: „Identity Management befasst sich vornehmlich in der Netzwelt der Datenverarbeitung mit der Verwaltung von Benutzerdaten, die einzelnen Personen zugeordnet sind. Eine Person kann dabei durchaus mehrere Identitäten besitzen, während eine Identität gewöhnlich nur einer Person zuzuordnen ist. Dabei ist die Identität eine Sammlung von personenbezogenen Attributen, die die Person, die sich dieser Identität bedient, individualisiert."

Da dies noch ziemlich abstrakt klingt, hier ein konkretes Beispiel: Ein Benutzer meldet sich am Morgen an seinem Arbeitsplatz an. Dort verwendet er Daten aus seiner digitalen Identität, um sich zu authentifizieren (Benutzername und Passwort). Darüber hinaus besitzt er vielleicht weitere Identitäten wie ein Datenbank-Login, ein Login für das E-Mail-System, für den Proxy-Server und so weiter. Diese Aufzählung lässt sich beliebig erweitern – es ist keine Seltenheit, dass eine Person bis zu 50 und mehr digitaler Identitäten besitzt.

Daraus ergeben sich für einen Anwender verschiedene Probleme: Er muss sich diese Identitäten inklusive Benutzernamen und Passwörter merken. Für Unternehmen oder Administratoren entstehen dadurch ebenfalls Probleme: Oft ist nicht nachvollziehbar, welcher Anwender zu welchem Zeitpunkt bestimmte Rechte besaß, oder es kann nicht sicher gestellt werden, dass alle Accounts deaktiviert werden, wenn ein Mitarbeiter das Unternehmen verlässt.

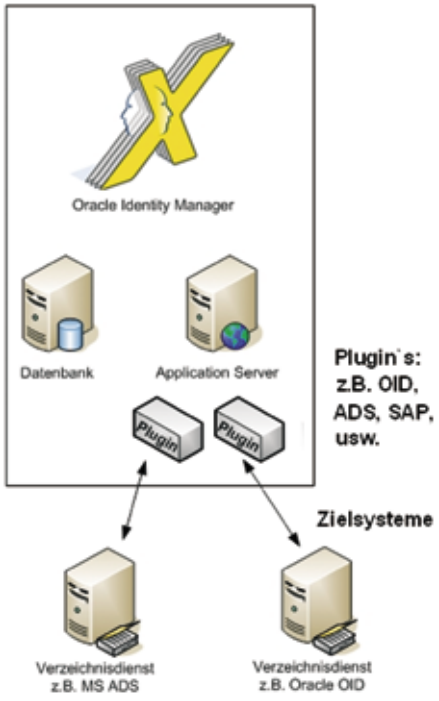

Abbildung 1: Aufbau eines IDM-Systems

Technische Herausforderungen

Zur Vermeidung oder Lösung dieser Probleme gibt es verschiedene Strategien. Meist wird in kleineren Umgebungen versucht, Single-Sign-On-Lösungen einzuführen. Dies scheitert in der Regel jedoch an technischen Problemen, weil verschiedene Systeme auch verschiedene Methoden zur Authentifizierung verwenden.

Ein besserer Lösungsansatz kann die Implementierung eines IDM-Systems sein. Die Architektur dieser Systeme ist bei allen Herstellern ähnlich. Sie bestehen meist aus einem zentralen Verzeichnis (beispielsweise LDAP) zur Speicherung von Benutzerdaten und Konnektoren für verschiedene Zielsysteme.

Abbildung 1 zeigt ein Beispiel mit einem Microsoft Active Directory und einem Oracle Application Server auf dem das Oracle Internet Directory (OID) als LDAP-Server betrieben wird. Auf beiden Systemen sind die entsprechenden Adapter installiert. Nun lässt sich zum Beispiel über das IDM-System ein definierter Prozess starten, wenn in dem Active Directory ein Benutzer angelegt oder bearbeitet wird. Über den Prozess kann man nun den Benutzer in dem OID anlegen oder aktualisieren.

Dieses Beispiel ist nicht besonders komplex, und sicherlich ist bekannt, dass man dieses Szenario auch ohne ein IDM-System mit einer LDAP-Synchronisation hätte lösen können. Stelle man sich nun aber vor, es existieren mehr als zwei Systeme (was normalerweise die Regel ist), und man möchte diese untereinander abgleichen. Im Extremfall kommen ein SAP-System, mehrere Datenbanken, eigene Anwendungen und vieles mehr zusammen. Eine solch komplexe Umgebung lässt sich vielleicht nicht mehr durch Replikationen lösen und erfordert den Einsatz eines IDM-Systems (zum Beispiel den Oracle Identity Manager).

Abbildung 2: Arbeitsweise eines IDM-Systems (Provisioning = Verteilen von Informationen, Reconciliation = Auslesen von Informationen)

Aufnahme der Prozesse und Arbeitsabläufe

Ist es ausreichend, ein IDM-System zu implementieren, wenn man die im ersten Abschnitt beschriebenen Probleme lösen möchte? Die Antwort lautet: vielleicht …

Denn neben den technischen Herausforderungen, ein komplexes System zu implementieren, besteht eine weitere Herausforderung in der Aufnahme und Dokumentation der zugrunde

liegenden Prozesse und Arbeitsabläufe. Kennt man die Prozesse und Abläufe nicht, besitzt man „nur“ ein System, das Benutzer-Informationen verteilen kann. Weitere Anforderungen – wie die Dokumentation, welcher Benutzer wann welche Rechte hatte – sind mehr oder weniger wertlos, da nicht dokumentiert wurde, welche Systeme wie integriert sind.

Beispiel für einen Prozess kann die Einstellung eines Mitarbeiters sein. Sicherlich kennt der eine oder andere das Szenario, dass am ersten Arbeitstag nicht alle benötigten Ressourcen (Schreibtisch, Telefon, PC, Zugangsdaten etc.) zur Verfügung stehen. Ein anderer Prozess wird zum Beispiel benötigt, wenn ein Anwender selbst weitere Rechte beantragen (und natürlich auch erhalten) möchte oder einen Benutzer-Account beantragen will. Dazu muss zuerst ein Antrag gestellt werden, der dann von einem berechtigten Benutzer (zum Beispiel Vorgesetzter) genehmigt wird. Ist dieses erfolgt, wird die Anfrage meist an einen weiteren Genehmiger (zum Beispiel in der IT) weitergeleitet. Stimmt dieser ebenfalls zu, wird durch das IDM-Tool die entsprechende Ressource (Benutzer-Account oder Zugriffsrecht) dem Zielsystem zugewiesen.

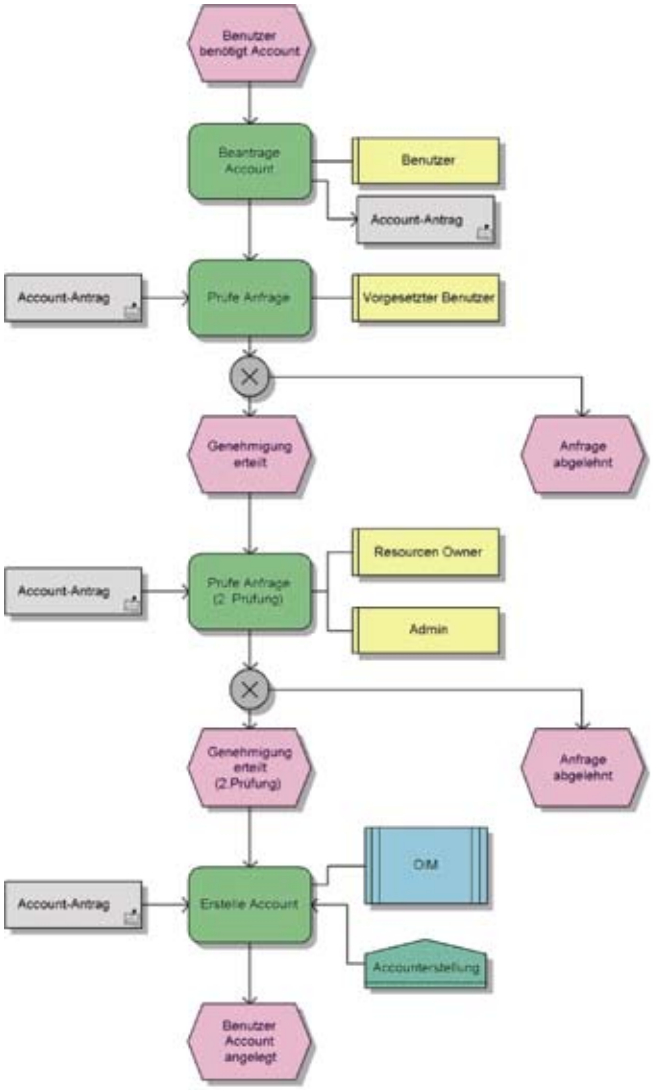

Abbildung 3: Darstellung eines IDM-Prozesses, der in einem Prozessmodellierungs-Werkzeug (zum Beispiel Aris Toolset von IDS Scheer) dargestellt wird.

Implementierung

Größe und Komplexität für ein IDM-Projekt ergeben sich aus verschiedenen Faktoren, unter anderem aus der Anzahl der zu integrierenden Systeme und umzusetzenden Prozesse. Die Dokumentation der Prozesse sollte am Anfang eines IDM-Projekts erfolgen. Erst auf Basis dieser Dokumentation wird deutlich, welche Lösung mit welchem Anpassungs- und Implementierungs-Aufwand geeignet ist, um die Anforderungen zu erfüllen. Die Vorgehensweise zur Umsetzung eines solchen Projekts lässt sich in mehreren Stufen realisieren (siehe Abbildung 4).

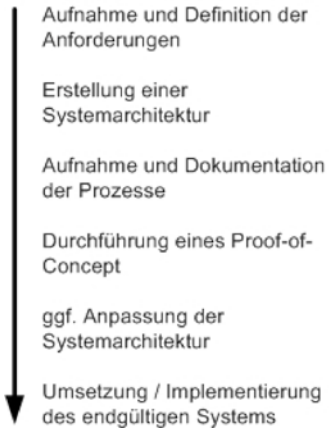

Abbildung 4: Beispiel für den Ablauf eines IDM-Projektes

Fazit

Es ist kein Geheimnis, dass viele Projekte an einer schlechten Planung scheitern oder mehr Zeit erfordern als geplant und damit natürlich mehr Budget benötigen. Bei der Umsetzung von Identity-Management-Projekten sind meist mehrere Abteilungen oder gar Unternehmen beteiligt, die alle ihre eigenen Prozesse einsetzen.

Die Erfahrung zeigt, dass durch die Dokumentation von Abläufen und Prozessen die „reine Realisierung“ deutlich stressfreier verläuft. Sonst könnte es vorkommen, dass mitten in der Abnahme eines IDM-Systems die Personalabteilung mitteilt, bestimmte Anwendungen oder Systeme seien vergessen worden …

Quellen und Links

- http://www.wikipedia.de
- http://otn.oracle.com
- http://www.oracle.com/technology/products/id_mgmt/index.html

Kontakt:
Björn Bröhl
bjoern.broehl@opitz-consulting.de