Föderiertes Identitäts-Management
Einführung auf einer Seite

Autor: Rainer Hörbe, 6.9.2010

Identitäts-Management (IDM) wird in der IT seit langem betrieben, indem Anwendungen ihre Benutzer verwalten und authentifizieren. Auch die Vereinheitlichung der damit verbundenen Dienste ist ein alter Hut, z.B. gibt es RACF seit 1976. Java und .Net-Anwendungen lagern die Authentifizierung in den Anwendungsserver bzw. das Framework aus. Ist nun IDM nur eine mit heißer Luft gefüllte Blase?

Es ist mehr als ein Hype: In vielen Unternehmen ist IDM bereits etabliert, und wo es noch nicht eingeführt wurde, stehen Architektur und ausgereifte Produkte zur Verfügung. Damit werden Mitarbeiter, z.T. auch externe Benutzer in der Unternehmens-IT zentral verwaltet und authentifiziert. IDM über diesen Bereich hinaus ist noch relativ neu. Um die Defizite des derzeitigen Status Quo zu erläutern, müssen einige aktuelle Trends genannt werden:

- Auflösung von physischen und technischen Unternehmensgrenzen: Mobile Arbeit, Outsourcing, Vernetzung mit Kunden und Lieferanten, etc. führen dazu, dass das bisherige Sicherheitsmodell mit dem Schwerpunkt auf SSL, Firewalls und Rechenzentrum nicht mehr greift. Identitäts-basierte Sicherheit muss in Zukunft die der Netzwerkgrenzen ergänzen.
- Skalierbarkeit von Web-Anwendungen: Mit der zunehmenden Menge der Anwendungen steigt der Aufwand für Benutzerverwaltung und Revision. Ein ökonomischer Betrieb vieler Anwendungen ist nur mit guter Organisation und redundanzfreier Verwaltung sinnvoll.
- Software-as-a-Service (SaaS) bietet ein Möglichkeit im Abo-Modell Anwendungen zu nutzen, ohne die IT-Abteilung bemühen zu müssen. Potentiell ermöglicht die Vernetzung verschiedener SaaS-Anwendungen untereinander und mit der internen IT neue Anwendungsfälle. Voraussetzung ist aber die Interoperabilität des IDM.
- Anwendungen in der Wolke (Cloud Computing) benötigen transparente und nachvollziehbare Sicherheitsmaßnahmen um das Risiko des Verlusts der direkten Kontrolle über die Daten auszugleichen. Als Folge davon werden sicherheitskritische Anwendungen in der Wolke meistens auch eine transparentes IDM benötigen.

Um diesen Herausforderungen entsprechen zu können, ist die Einrichtung eines föderierten IDM zweckmäßig, wobei bereits existierende Systeme weitgehend integriert werden können. Föderiertes IDM ist eine Erweiterung des unternehmensinternen IDM um ein rechtliches Rahmenwerk, dass eine Vielzahl bilateraler Verträge vermeidet und die technischen Schnittstellen vereinheitlicht. Durch die Bildung der Föderation entstehen folgende Rollen:

- Identitäts-Provider (IdP) registrieren Benutzer und bestätigen die Authentizität ihrer Attribute in einer *Assertion* (Zusicherung).
- Benutzer oder Geräte werden durch ihre Attribute identifiziert, wie Name oder eMail-Adresse.
- Service-Provider (SP) vertrauen IdP Benutzer zuverlässig zu identifizieren und authentifizieren.
- Ein Depositar verwaltet und publiziert die registrierten SP, IdP und Prüfer entsprechend der Rahmenvereinbarung der Föderation.

Fügt man zu diesen Rollen eine interoperable technische Infrastruktur hinzu (SAML, OpenID, WS-Federation) und schafft definierte Vertrauensstellungen durch eine Rahmenvereinbarung und kann so diese Rollen unterschiedlichen Anbietern zuweisen, die somit eine Föderation bilden.

Daraus ergeben sich erhebliche Vorteile in der Verwaltung der Benutzer, der Einhaltung von Sicherheitsrichtlinien, der Umsetzbarkeit starker Authentifizierung, und Effizienzgewinne beim Rollout neuer Anwendungen. Potentiell kann durch diese Beseitigung von Barrieren ein explosives Wachstum von Anwendungen für neue Geschäfts- und Anwendungsfälle entstehen.