

Ein Werkzeugkasten für IDM: Erfahrungen aus der Praxis

Bei der Umsetzung eines Identitätsmanagements (IDM) müssen hohe Hürden genommen werden. Bereits mittelgrosse Unternehmen verwenden in der Regel die unterschiedlichsten Applikationen, Plattformen, Benutzerdaten und Policies. Deren Abbildung und Integration in ein IDM-System ist sehr anspruchsvoll. IDM-Pakete ab der Stange können nur Teilaspekte dieser Aufgaben abdecken und weisen zudem meistens fehlende oder ungeeignete Sicherheitsstrukturen auf. Letzteres verletzt bereits eine fundamentale Anforderung eines robusten, modularen IDM-Systems.



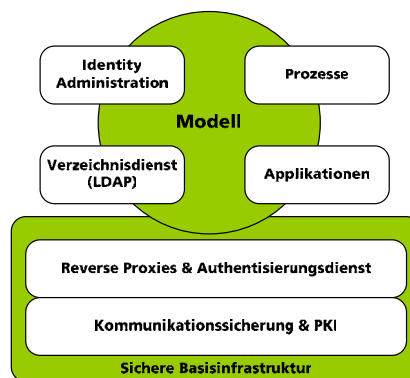
Philipp Färber

Philipp Färber, Dr. sc. techn. ETH, ist Senior Security Engineer bei der AdNovum Informatik AG, www.adnovum.ch.

philipp.farber@adnovum.ch

Die Einführung eines IDM-Systems ist eine komplexe Aufgabe. Die Komplexität lässt sich aber signifikant reduzieren, wenn "IDM" nicht als Programmpaket, sondern als modulares System verstanden wird. Dieses setzt sich aus mehreren, zum Teil unabhängigen Komponenten zusammen. Die Aufschlüsselung in einzelne Module öffnet die Sicht auf die typischen Problemstellungen und erlaubt ein schrittweises und priorisiertes Vorgehen bei der Spezifikation und Umsetzung.

Folgende Abbildung illustriert die modulare Sicht auf ein mögliches IDM-System:



Der Werkzeugkasten

Die wichtigsten Komponenten eines IDM-Systems lassen sich effizient und kostengünstig realisieren, wenn ein Werkzeugkasten mit bewährten Lösungen eingesetzt wird. In der Praxis erweisen sich dabei vor allem vier IDM-Module von zentraler Bedeutung.

1. Sichere Basisinfrastruktur

Der durchgängige Einsatz von Verschlüsselung und Knoten-Authentisierung ist im Intranet noch immer keine Selbstverständlichkeit. Ohne entspre-

chende Massnahmen gegen triviales „Sniffing“ von Passwörtern oder einfache „Man-in-the-Middle“-Attacken ist jedes IDM-System wertlos. Als weit verbreitetes Werkzeug bietet sich hier die Kommunikationssicherung über SSL an. Gemeinsam mit einer möglichst einfach wartbaren PKI für das Zertifikatsmanagement werden damit – unabhängig von einem IDM-System – die Grundpfeiler für eine sichere Basisinfrastruktur gelegt.

Neben der Kommunikationssicherung sollte auch das Problem des Delegierens, also der Weitergabe von Identitätsinformationen, bereits innerhalb der Infrastruktur gelöst sein. Als verbreitete Variante empfiehlt sich hier der Einsatz von sicheren

Reverse Proxies, die zusammen mit einem zentralen Authentisierungsdienst Identitäten verifizieren und

auf sichere Art transparent an jeden Request binden.

Der Einsatz eines Authentisierungsdienstes erlaubt zudem die saubere Trennung von Authentisierung und Autorisierung. Denn ein IDM-System sollte sich nur mit Autorisierung, der Zu-

IDM muss als modulares System verstanden werden.

ordnung von Benutzern und Berechtigungen, und allenfalls mit dem Mapping von Benutzern zu Credentials befassen. Die Feststellung von Identitäten, wie sie Aufgabe der Authentisierung ist, sollte an die Infrastruktur delegiert werden können. Die Vermischung der beiden Aspekte macht nicht nur das IDM-System komplizierter, sondern behindert auch einen Single-Signon (SSO), bei dem Benutzer unabhängig von den aktuell gebrauchten Credentials (wie Passwort, Kerberos, Zertifikat) erkannt werden.

2. Prozess- und Applikationsanalyse

Das Bedürfnis nach einem IDM-System wird erst dann virulent, wenn eine bestehende Benutzerverwaltung aus dem Ruder zu laufen droht oder den Anforderungen (Security Compliance, Nachvollziehbarkeit) nicht mehr genügt. Deshalb sind 'auf der grünen Wiese' gebaute Lösungen, für die ein Produkt ab der Stange durchaus genügen kann, in der Realität selten. Eine Umsetzung (und Einführung) von IDM in Form eines eigenen, mehrere Phasen umfassenden Projekts erlaubt dagegen die Rücksichtnahme auf spezifische Anforderungen und lokale Gegebenheiten.

Durch die Analyse der existierenden Benutzerdaten und Verwaltungsprozesse als erste Aufgabe des Projektvorhabens entsteht ein Anforderungskatalog, der sowohl Applikations- als auch Prozess-Integration berücksichtigt. Eine solche Analyse und Dokumentation des "Status Quo" ist für ein

Unternehmen an sich schon ein lohnendes Unterfangen, da sie immer auch eine kritische Begutachtung der bestehenden Prozesse nach sich zieht und deren Vereinheitlichung und Optimierung erlaubt. Hinsichtlich Applikationsintegration sind Probleme wie technische Anbindung und Abbildung von neuen auf alte Benutzerdaten von Bedeutung. Das "Werkzeug" für eine solche Analyse ist eine detaillierte Studie, die sich vor allem auf Interviews mit den Applikationsverantwortlichen und -benutzern stützt. Dank direkter Befragung betroffener Mitarbeiter entsteht nicht nur ein Abbild eines aktuellen Zustands, sondern es wird auch klar, wie die Prozesse im Alltag konkret umgesetzt werden und wo allfällige Mängel behoben werden müssen.

3. Flexibles Modell

Sobald ein Anforderungskatalog erstellt ist, muss ein Modell zur Zuordnung von Benutzern und Berechtigungen definiert werden. Aus Gründen der Einfachheit empfehlen wir ein rollenbasiertes Modell (Role-Based Access Control, RBAC), das auf möglichst wenigen, unternehmensweit gültigen Enterprise-Rollen aufbaut. Die Alternative

eines regelbasierten Systems erlaubt zwar ein dynamischeres Mapping, führt

aber bezüglich Administrierbarkeit leicht zur Unübersichtlichkeit. Falls auf applikationsspezifische Rollen nicht verzichtet werden kann, können diese als generische Zusatzberechtigungen aufgenommen werden.

4. Erweiterbares Verzeichnis und Administration

Der eigentliche Kern eines IDM-Systems beschränkt sich auf einen hoch verfügbaren Verzeichnisdienst, in dem alle im Modell definierten Informationen auf flexibel abrufbare Art abgelegt sind. Als verbreitete Schnittstelle bewährt sich hier LDAP (bzw. LDAP/S) - wobei hier oft schon ein bereits existierender Verzeichnisdienst benutzt werden kann. Zukünftigen Modell-Erweiterungen kann durch eine Erweiterung des LDAP-Schemas Rechnung getragen werden. Die Administration der Daten hängt stark vom Modell und den definierten Prozessen ab, so dass hier durchaus der Einsatz einer selbst gebauten Applikation sinnvoll ist. Dadurch ergibt sich eine hohe Flexibilität bei der Einbindung existierender Prozessschnittstellen (HR-System oder andere Workflows). Auch kann das Ausmass, in dem Prozesse automatisiert (bzw. durch die Benutzer selbst) ausgeführt werden, auf diese Weise dynamisch gewählt werden.

Erweiterungen

Wird ein IDM-System mit den Modulen des Werkzeugkastens und unter konsequenter Verwendung von offenen Standards und Schnittstellen aufgebaut, kann es auf einfache Weise um zusätzliche Module erweitert werden. Zum Beispiel für die Einbindung weiterer Applikationen, Föderation verschiedener Benutzer-Domänen, Unterstützung von Pseudonymen für den Datenschutz oder komplexere Berechtigungsverwaltungen.