

Mit Sicherheit mehr Effizienz

Identity Management ermöglicht:

- ▶ **Nachvollziehbarkeit:**
- ▶ **Daten- und Systemintegrität**
- ▶ **Datenschutz**
- ▶ **Durchsetzung der Richtlinien**

Die entscheidenden Fragen bei all diesen Aspekten beziehen sich auf die Identitäten von Personen und Rollen:

- ▶ Wer hat Zugang zu kritischen Daten, Anwendungen und Prozesse?
- ▶ Wer ist für die Erteilung einer Zugriffserlaubnis zuständig?
- ▶ Wer definiert die Regeln?

Vorteile für Ihre Unternehmen

- ▶ Prozessoptimierung
- ▶ Schaffung von Datenkonsistenz beim User-Management
- ▶ Kostensenkungspotentiale durch Administrationsvereinfachung und Optimierung des Datenaustauschs
- ▶ Minimierung von Sicherheitsrisiken
 - ➔ Schutz vor unberechtigten Zugriffen
- ▶ Geringere Komplexität durch Konsolidierung und/oder Verknüpfung von Identitätsinformationen
- ▶ Verlässliche Betreuung einer digitalen Identität über ihren ganzen Lebenszyklus hinweg

Allgemein kontrolliert Identity Management Anwendungen und Daten in Bezug auf Zugriffsberechtigungen innerhalb des Unternehmens. Durch die einfachere Bereitstellung und Sperrung von Daten basierend auf Zugriffsrechten wird es dem Unternehmen ermöglicht, Datensicherheit und Datenschutz in den Griff zu bekommen.

Situation.

Angebots zahlreicher Applikationen, Portale und Dienste, auf die Mitarbeiter innerhalb und Kunden ausserhalb von Unternehmen zugreifen, wird die Frage der effizienten und sicheren Verwaltung von Zugriffsrechten für die Organisationen zu einer immensen Herausforderung. Zudem muss sich ein Anwender meist eine Vielzahl von Benutzernamen und Passwörtern (Passwort Changes) merken, um auf „seine Dienste“ zugreifen zu können. Abhilfe schaffen hier Lösungen für das Identity Management (IdM): Dabei werden Informationen zu einzelnen Benutzern zentral verwaltet. Automatisierte Prozesse sorgen hierbei für eine einfache Verwaltung, komfortable Nutzung für den Anwender sowie maximale Sicherheit und die Gewährleistung rechtlicher Grundlagen in Bezug auf die Datenhaltung.

Warum Identity Management?

In Unternehmen sind Daten meist auf verschiedene Datenpools mit jeweils unterschiedlichen Zugriffsverwaltungen verteilt. IdM-Lösungen sorgen hier für ein zentralisiertes Management und bieten sowohl Unternehmen als auch Anwendern gravierende Vorteile.

Fazit.

IdM ist für Unternehmen in der Regel mehr, als eine reine Software-Lösung. Es ist eine strategische Komponente, um Kunden und Partner in Workflows und Prozesse zu integrieren, die technische Infrastruktur zu vereinheitlichen und Wettbewerbsvorteile zu schaffen oder auszubauen.

Fachliche Anforderungen.

IdM-Lösungen adressieren konkurrenzierende Ziele



Grafik: Sun Microsystems (Schweiz) AG

Mit Sicherheit mehr Effizienz

Die wichtigsten Komponenten einer IdM-Lösung.

User Provisioning

Der Identity Manager ersetzt bislang fragmentierte manuelle Prozesse durch das vollständig automatische Management des User Lifecycle Prozesses. Das Provisioning auf der Basis von Rollen und Regeln bietet weitreichende Flexibilität bei der Handhabung der Provisioning-Regelungen für Nutzer, Unternehmen, Ressourcen, Rollen und Gruppen. Der dynamische Workflow unterstützt mehrstufiges, komplexes Provisioning; Änderungen der Identitätsdaten werden automatisch vorgenommen. Die Verantwortlichen können die Zugangsberechtigung der Nutzer komplett einsehen und kontrollieren.

Access Management

Das Access Management verwaltet alle Zugriffsrechte auf Applikationen und Dienste. Dezentrale Dienste für Authentisierung und Autorisierung, die rollenbasierte Zugangskontrolle und Single Sign-On (SSO) liefern ein effizientes, skalierbares Sicherheitsmodell für alle web-basierten Applikationen. Access Manager verbessert die Sicherheit und vereinfacht nicht nur das Management, sondern auch die Transaktionen und den Datenaustausch. Zugleich sorgt er für den Schutz und die Sicherheit wichtiger Identitätsdaten, schützt die Ressourcen vor Missbrauch sowie unbefugten Zugriffen. Sorgfältig definierte, mehrfach einsetzbare und für Audits geeignete Sicherheitsabläufe können unternehmensweit eingesetzt werden.

Federation

Unter Federation versteht man Unternehmens-übergreifende IdM-Systeme. Identitäten werden hier gemeinsam mit Partnern genutzt und verwaltet. Das Access Management ist somit nicht mehr nur auf die eigene Infrastruktur begrenzt, sondern mit externen Angeboten und Diensten verbunden.

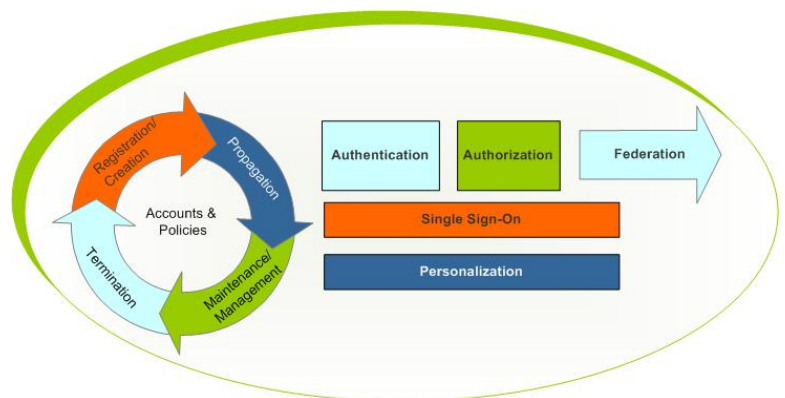
Auditing + Reporting

Verantwortliche erhalten durch die umfassende Auditing- und Reporting-Funktionen schnell einen Überblick (Audit) über Zugriffsrechte und Veränderungen an den einzelnen Identitäten. Die manipulationssicheren Audits ermöglichen dabei Dokumentationen, die den zahlreichen rechtlichen Vorgaben entsprechen.

openX Beratungsdienstleistung.

Um unsere Kunden optimal auf den Einstieg ins Identity Management vorzubereiten oder bestehende Lösungen zu überprüfen, bietet openX Consulting individuelle Bestandsaufnahmen. Unsere Spezialisten analysieren die vorhandenen Zugriffsberechtigungsmodelle, die einzuhaltenden Prozesse und Vorgehensweisen, die Zielsetzungen und vor allem den Bedarf des Unternehmens. Dadurch ist es möglich, eine objektive Einschätzung des Geschäftswerts einer IdM-Lösung für ein Unternehmen zu erhalten. Über eine abschließende Analyse können die IdM-Fachleute den Weg zur erfolgreichen Einrichtung einer prozessorientierten Identity-Management-Lösung detailliert aufzeigen.

IdM Portfolio von openX Consulting.



Unsere Vorgehensweise baut auf einem bewährten Modell auf, bei dem die einzelnen Phasen sinnvoll aufeinander abgestimmt sind und somit so früh wie möglich ein ROI erreicht werden kann.

Identity Management gehört zu den wichtigsten Komponenten einer erfolgreichen Infrastruktur. Unsere Consultants unterstützen Sie bei der Planung, Implementierung und Verwaltung Ihrer Identity Management Lösung. Umfassendes Services und Methoden für Architektur, Implementierung sowie Management sorgen dafür, dass Sie alle Vorteile unserer Identity Management Lösung voll ausschöpfen können.

Sprechen Sie mit uns! Wir freuen uns auf Ihre Kontaktaufnahme.