Titel:
Identitätsmanagement für Cloud-, mobile und soziale Umgebungen,

Autor:
Christian Patrascu, Director of Product Management – Oracle Fusion Middleware

Datum:
20.11.2013, 10:00 - 10:45 Uhr, Raum 19

Stream:
Middleware & SOA

Zielgruppe:
Fortgeschrittene

Abstract:

Oracle Identity Management 11g Release 2 erlaubt es Unternehmen, Cloud-, Social-Web- und mobile Infrastrukturen sicher einzusetzen. Damit erreichen Unternehmen neue Zielgruppen und können so ihre Geschäftsfelder erweitern.
Muss dafür jedoch das Rad neuerfunden werden ?
Wie gewährleistet man "End to End Security" ?
Wie werden diese Themen vom Markt akzeptiert ?

Einführung & Manuskript:

Datenzugriff, jederzeit, überall - die Mega-Trends Cloud, Mobile und "Social" stellen Unternehmen vor enorme Herausforderungen in Sachen Sicherheit. Insbesondere dann, wenn die Identitäts- und Zugangskontrolle (Identity und Access-Management, IAM) auch beim Zugriff via Soziale Netzwerke möglich sein soll. Die mobilen Geräte sollen sich möglichst nahtlos in die Unternehmenslandschaft integrieren lassen, ohne die bestehenden Sicherheits-Workflows zu unterlaufen.

Das **"mobile Identitätsmanagement"** wird deshalb zur **Schlüssel-Technologie**, wenn es darum geht, Social Networking im Unternehmensbereich richtig zu etablieren. Wie steht es um Single-Sign-On (SSO) beim browser-basierten Zugriff auf und native mobile Geschäftsanwendungen? Wie lässt sich eine Hochsicherheits-Authentifizierung und Autorisierung des Mobilgeräts per kontext-basierter "Fingerabdruck-Kontrolle" etablieren? Und wenn das Unternehmen den **Zugriff auf Unternehmensanwendunge**n und -daten **via Google- oder Facebook-Konto** ermöglicht, weil es längst selbst eine eigene Präsenz in sozialen Netzwerken aufgebaut hat: Wie lässt sich da noch eine **Single-Sign-On-Strategie** des Unternehmens durchsetzen?

Die **Authentifizierung des Endnutzers** und die **Validierung des Mobilgeräts**, die Integration des Datenzugriffs in bestehende Verzeichnisse, entsprechende Nutzer-Profil-Dienste, die **Provisionierung von SSO für mobile Applikationen**, das **Zugangs- und Zugriffsmanagement**, der **Schutz** mobiler Anwendungen und von **Web-APIs**, das Regelwerk für den Fall des

Geräteverlusts oder -Diebstahls, das Loggen und die **Überwachung mobiler Transaktionen**: Ein sicheres, mobiles Identitätsmanagement wird scheinbar zur Sisyphos-Aufgabe.

- Müssen Unternehmen die Themen "Mobile & Social" für das Identitätsmanagement berücksichtigen?
- Welche Services muss Identitätsmanagement in Zeiten von Cloud, Mobile und Social Networking berücksichtigen?
- wie lassen sich diese Services nahtlos in die bestehende ID-Management-Infrastruktur des Unternehmens integrieren?