Unternehmensweites Rollen-Management

Karsten Müller-Corbach, ORACLE Deutschland GmbH

Eine rein manuelle Verwaltung von Zugriffsrechten auf die Unternehmens-IT macht die Einhaltung von Compliance-Vorschriften nahezu unmöglich. Die Lösung sind automatisierte Verfahren, die Zugriffsrechte und Privilegien provisionieren und auch wieder entfernen können. Um eine inhaltliche Ausgestaltung der Automatisierung zu erlangen, ist der Einsatz eines unternehmensweiten Rollenkonzepts äußerst zielführend.

In der Regel sieht die Realität in Unternehmen folgendermaßen aus:

- *Viele Mitarbeiter haben Zugriff auf Daten und Ressourcen, die sie nicht haben sollten.*
  Abteilungswechsel, virtuelle Teamänderungen, wechselnde Projektmitgliedschaften und Beförderungen führen zu Überschneidungen in Kompetenzen. Wenn die IT-Systeme nicht genau verfolgen, wer welche Rechte hat, diese Änderungen auditieren und berichten, verlieren Administratoren sowie die Benutzer selbst schnell die Übersicht.

- *Provisionierung von Benutzern wird meist noch manuell durchgeführt.*
  Die manuelle Provisionierung von Benutzern und die Vergabe von Rechten hilft nicht beim Erreichen von Compliance, da keine übergeordnete Instanz diese Vergabe dokumentieren kann. Die Dokumentation muss leider dezentral geschehen. Auditoren wie auch interne Kontrollstellen müssen zuerst mühevoll Daten sammeln und dann erst auswerten. Zudem wirken sich manuelle Änderungen negativ auf eine gewünschte Skalierung aus.

- *Benutzer werden nicht zeitnah gelöscht.*
  Mitarbeiter, die das Unternehmen verlassen, können nach zwei Wochen immer noch auf die meisten Applikationen zugreifen. Oft werden Benutzer nicht automatisch gelöscht oder deaktiviert. Dadurch enthalten viele Systeme Benutzer, die längst gelöscht sein sollten. Ein Bereinigungsprozess ist nach einiger Zeit nur schwer durchzuführen.

- *Interne Kontrollen wie Beglaubigungsvorgänge können nicht nachvollzogen werden.*
  Compliance-Vorschriften sehen vor, dass Beglaubigungsvorgänge in re-

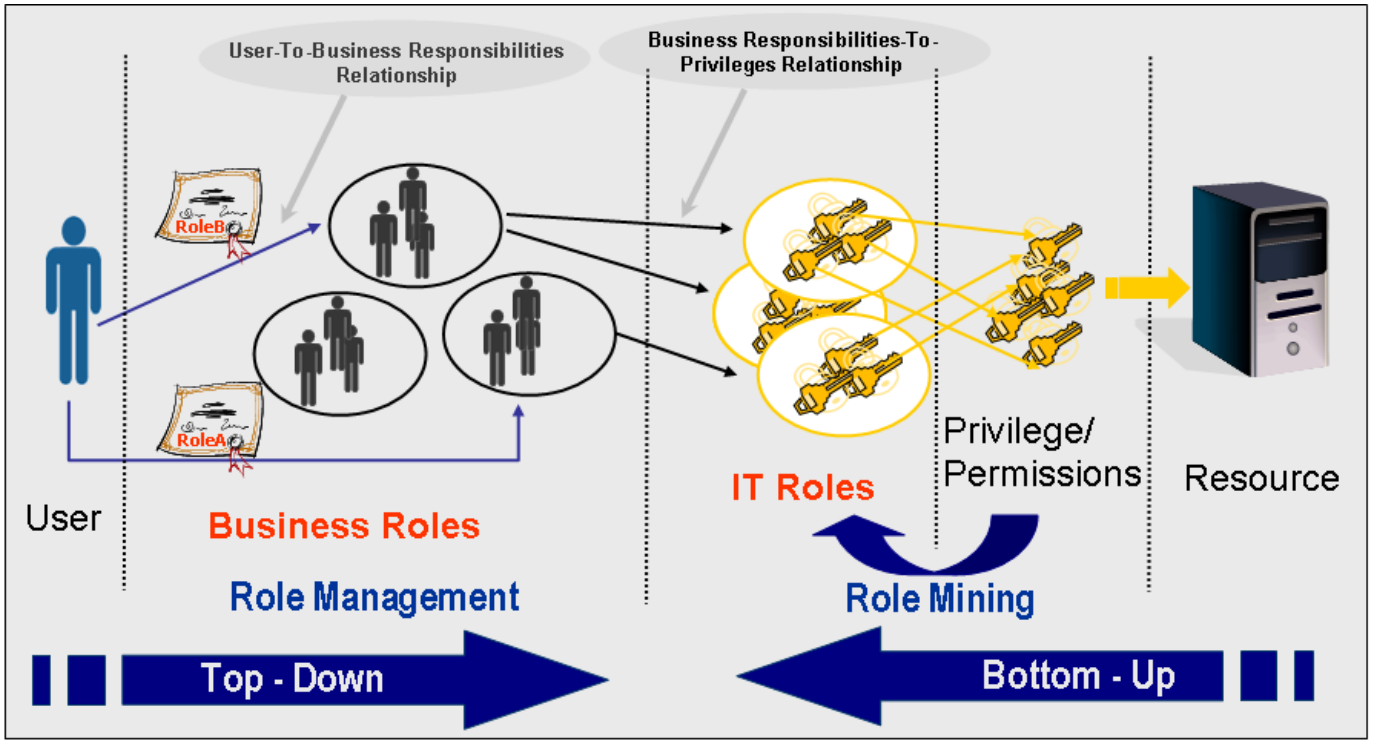

Abbildung 1: Rollen-Management mit Top-down- und Bottom-up-Planung

gelmäßigen Abständen durchgeführt werden. Nur so ist nach manuellen Änderungen, wie einen genehmigten Antrag, nachzuvollziehen, ob Ressourcen oder Berechtigungen noch aktuell sind und ob die vordefinierten Provisionierungsprozesse einwandfrei funktionieren.

Identity-Management

Durch die manuelle Vergabe von Accounts, Berechtigungen und Rollen, besteht die Gefahr von Inkonsistenzen und Sicherheitslücken. Eine Antwort darauf geben Identity- und Access-Management-Systeme (IAM-Systeme). Der Begriff Identitäts-Management (IDM) entwickelte sich aus einfachen Verzeichnis-Diensten und wurde schnell in Meta-Directories erweitert. Seit einigen Jahren verdrängen nun Provisioning-Suiten diese Meta-Directories.

Schon früh hat man festgestellt, dass Meta-Directories leider nur auf der Daten-Ebene arbeiten, Unternehmen jedoch Prozess-Anforderungen haben, die in einem Provisionierungs-Kreislauf einfließen müssen. Der zwingend folgende Trend beinhaltet umfassende Lösungen, die nicht nur das Identitäts-, sondern auch das Zugriffs-, Prozess- und Sicherheitsmanagement abdecken. Eine moderne Provisioning-Suite enthält auch den offenen Zugang für und in eine serviceorientierte Architektur (SOA).

Ein Identity- und Access-Management bietet eine Vielzahl von Diensten an, die in die IT-Infrastruktur eines Unternehmens eingreifen und dadurch integriert sein müssen.

Vor der Entscheidung für die Integration und Implementierung eines IAM-Systems stehen weitreichende Planungen an. Die Auswirkungen sind die automatische Vergabe von Zugangs- und Zugriffsrechten an Tausende oder eine nahezu unbegrenzte Anzahl von Mitarbeitern. Klar definierte Prozesse sind erforderlich, um diese automatischen Vergaben zu garantieren.

Der Lebenszyklus eines Mitarbeiters wird vom IAM-System verwaltet – von der Anlage des Mitarbeiters im Personal-System, über Änderungen seines Profils, Beantragungen von neuen Ressourcen, Genehmigungen von Privilegien bis zur sofortigen Löschung oder Deaktivierung aller Accounts beim Ausscheiden. Auf Rollen basierte Regeln helfen bei der fortlaufenden Pflege, Verwaltung und Überwachung. Ein strukturiertes Rollenkonzept ermöglicht eine größtmögliche Automatisierung innerhalb eines IAM-Systems.

Rollen-Management

Der Aufbau eines unternehmensweiten Rollen-Konzepts bedingt eine C-Level-Unterstützung, da mehrere bestehende Rollen-Konzepte zu vereinheitlichen sind. Verschiedenste Bestandssysteme wie Datenbanken oder Verzeichnisdienste enthalten eigene Rollenkonzepte

in Form von Rollen in Datenbanken oder Gruppen in Verzeichnisdiensten. Die einzelnen Rollen-Konzepte lassen sich nicht direkt gegeneinander abbilden.

Modernes Rollen-Management bricht die Berechtigungen der angeschlossenen Systeme in Privilegien herunter. Eine Datenbank-Rolle oder Verzeichnisdienst-Gruppe entspricht einem einfachen Privileg. Die Methodologie des Rollen-Managements besteht aus folgenden Schritten:

- *Rollen-Discovery*
  Der Prozess des Rollen-Discoveries sammelt Privilegien und deren Mitgliedschaften aus Systemen und Ressourcen.
- *Rollen-Mining*
  Das Rollen-Mining berechnet IT-Rollen. Privilegien mit deren Mitgliedschaften werden miteinander in Kombination gebracht und deren Relation als IT-Rollen vorgeschlagen. Diese IT-Rollen sind eine Sammlung von IT-Privilegien. Rollen-Mining-Werkzeuge helfen bei der Analyse und der Berechnung der IT-Rollen.
- *Rollen-Modellierung*
  Auf der Business-Ebene müssen Business-Rollen definiert sein. In Business-Rollen werden Verantwortlichkeiten aus dem Unternehmen definiert und Benutzer zugeordnet. Um die Rollen-Management-Methodologie zu vervollständigen, müssen IT-Rollen und Business-Rollen aufeinander abgestimmt werden.
- *Rollen-Administration*
  Rollen können durch eine dynamische oder statische Zuordnung erfolgen. Bei der dynamischen Zuordnung erhält ein Anwender eine Rolle durch Mitgliedschaft in einer Hierarchie-Ebene, eines Projekts oder durch Eigenschaften seines Benutzerprofils. Eine statische Zuordnung kann durch Manager-Zuweisung oder durch Beantragung und anschließenden Genehmigungsprozess erfolgen.

Nur wenn IT- und Business-Perspektive in Einklang gebracht werden,

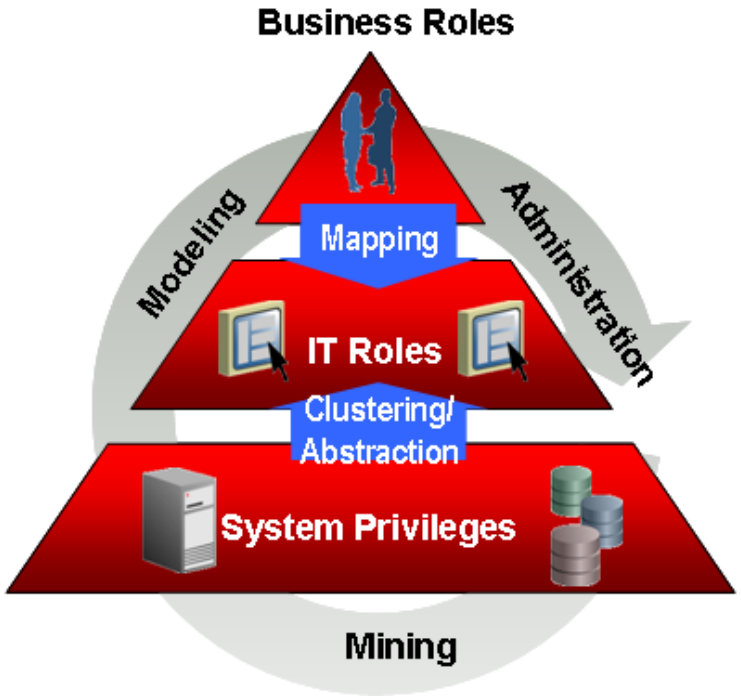

Abbildung 2: Prozesse des Rollen-Managements

kann ein Rollen-Konzept erstellt werden, das den Belangen aller Beteiligten entspricht. Die so für das Unternehmen gewonnenen Rollen-Definitionen können anschließend im IAM-System übernommen werden. Einem Mitarbeiter müssen nun keine Rechte mehr manuell vergeben werden. Eine einfache Rollen-Zuordnung veranlasst das IAM-System, Privilegien oder Rechte in den angeschlossenen Zielsystemen zu provisionieren, zu ändern oder zu deprovisionieren.

Das Rollen-Management-System ergänzt das IAM-System durch ein unternehmensweites Rollen-Konzept, da es alle bestehenden Rollen-Konzepte vereinigt. Der Prozess des Rollen-Managements umfasst die wiederkehrenden Schritte des Rollen-Minings, Rollen-Modelings und der Rollen-Administration.

Fazit

Die Herausforderung jedes Unternehmens ist eine ganzheitliche Betrachtung des Identity- und Access-Management, das viele Facetten beinhaltet. Durch seine heterogene und komplette Suite kann Oracle vieles vereinfachen. Die Stärke, auch eigene Applikationen im Produktportfolio zu haben, hat das Thema IAM reifen lassen. Oracle sieht sich wie jeder andere Kunde vor dieselbe Herausforderung gestellt: Mit fast 40 horizontalen und vertikalen, eigenen Applikationen ist es undenkbar, die Sicherheitsschicht immer wieder neu zu erfinden, da Silos entstehen, wie jedes Unternehmen sie leider kennt. Daher geht der Trend in Richtung „Identity as a Service“. Dabei nutzt die Applikation über definierte heterogene Schnittstellen IAM-Dienste. Oracle ist wie kein anderer Wettbewerber gezwungen, diesen Weg schnell und konsequent zu gehen. Und Oracle IAM ist fester Bestandteil dieser Strategie.

Kontakt:
Karsten Müller-Corbach
karsten.mueller-corbach@oracle.com