

1 Zusammenfassung

In dem derzeitigen Run auf Lösungen aus dem Bereich Identity-Management und zentraler Provisionierungssysteme erlangen realisierbare und realitätsnahe Rollenmodelle eine neue Bedeutung. Dies obwohl das Thema der Rollenmodellierung absolut nicht neu ist und es diverse Konzepte und Lösungsansätze gibt. Ein in der Praxis wirklich sinnvoll nutzbares Rollenmodell muss jedoch weit mehr Zusammenhänge des IT-Managements abbilden, als die meisten angebotenen Systeme wirklich leisten. Eine in dieser Richtung positiv zu erwähnende Lösung wurde z.B. durch E-Plus realisiert.

In der bisherigen direkten und einzelnen Verwaltung der User und deren Berechtigungen auf den jeweiligen Zielsystemen ist es praktisch unmöglich, einen aggregierten Überblick über die Rechte der User und deren Entsprechung zu der ausgeübten Tätigkeit zu bekommen.

Je nach Ausrichtung des Unternehmens kommen massive externe Zwänge zu einer eindeutigen Nachvollziehbarkeit der Prozesse in der Useradministration aus verschiedenen Regularien hinzu (SOX, Basel II, 8. EU-Direktive, KONTRAG etc.). Dies führt z.B. zum regelmäßigen massenhaften Ausdruck der Berechtigungen aller User und der sog. Re-Zertifizierung durch deren Leiter, was schließlich nur ein formaler, zeitaufwendiger und nicht wirklich sinnvoller Vorgang ist.

Aus den Projekterfahrungen des Autors heraus, werden die Bereiche angesprochen, die sich in einem produktiven Einsatz als kritisch erwiesen haben. Ein weiterer Aspekt ist den Aufgaben der internen Revision gewidmet, wenn sie in die Produktevaluierung einbezogen ist und ein IPM¹-Projekt begleitet.

¹ IPM = Identity- und Provisioning-Management

2 Notwendige Security - Eigenschaften eines IPM-Systems

Um überhaupt eine qualifiziertes Security-Management eines IPM-Systems ausführen zu können, sind einige Systemeigenschaften bzw. –Funktionen unverzichtbar.

2.1 Differenziertes Rollenmodell

Das Rollenmodell eines IPM-Systems muss eine Differenzierung zwischen Fachrollen und Systemrollen ermöglichen. Wobei die Fachrollen die Systemrollen enthalten. Dies ist notwendig, um die eigentlichen Berechtigungen von der Steuerung der Fachrollen zu trennen.

Aus dieser Sicht, verfügt ein Leiter nur über die Zuordnung von Fachrollen zu seinen Mitarbeitern. Eine weitere Einschränkung der Sichten auf Rollen muss für den User so weit möglich sein, dass innerhalb eines Fachbereiches nur die für diesen Bereich relevanten Fachrollen überhaupt sichtbar und damit beantragbar sind. Das setzt die Möglichkeit einer Attribut-Referenzierung für Fachrollen voraus. Diese ist in der Regel auf die Struktureinheiten bezogen, sollte aber auch für andere Userattribute (Funktion, Standort etc.) möglich sein.

2.2 Rollenkonflikte

Von besonderer Bedeutung bei der Rollenmodellierung ist die Auflösung von Rollenkonflikten bzw. deren weitgehende Vermeidung. Ein Rollenkonflikt tritt dann auf, wenn ein User ein System jeweils über eine andere Rolle mit verschiedenen Ausprägungen der Berechtigungen zugewiesen bekommt und in der Systemeinstellung die Vereinigung der Profile definiert wurde. Diese Problematik stellt hohe Anforderungen an die interne Logik des IPM-Systems, da dieser Fall auch mehrfach auftreten kann und vor allem dann Probleme bereitet, wenn eine solche Rolle entfernt wird und genau das Profil aus den vorher vereinigten Profilen wieder logisch sauber herausgelöst werden muss. Um die möglichen Rollenkonflikte zu verringern sollte die Rollenmodellierung nicht *additiv* sondern *autonom* organisiert werden. Dies bedeutet, dass jede Fachrolle nur ein Berechtigungsprofil für ein System enthält. Ein Leiter hat dann z.B. alle Rechte, die er als Leiter braucht und nicht die Zusammensetzung der Rechte eines Mitarbeiters und der Differenz der Rechte des Leiters über je eine Systemrolle. Trotzdem kann es zu Rollenkonflikten über die Zuweisung von mehreren Fachrollen kommen, die dann durch das IPM sauber aufgelöst werden müssen. Weiterleitende Ausführungen zu dieser Problematik sind z.B. zu finden unter: <http://www.secu-sys.de/download.html>

Eine besonders wichtige Regel sei hier aber explizit erwähnt, da sie eine sanfte Migration von der direkten Systemzuweisung zu einer rollenbasierten ermöglicht. Sie besagt, dass eine Systemzuweisung über eine Rolle immer eine direkte Zuweisung überschreibt.

2.3 Prozesssteuerung

Diese Eigenschaften eines Rollenmodells sind die Voraussetzung für die Automatisierung der IPM-Prozesse. Hierzu gehören vor allem:

- Mitarbeiter-Eintritt, Mitarbeiter-Austritt und sein Status-Wechsel
- Wechsel in der Organisationseinheit, im Team, Projekt etc.
- Wechsel zwischen Unternehmen eines Konzerns
- Antrag und Genehmigungsverfahren eines User auf eine Fachrolle
- Antrag eines Leiters auf eine Fachrolle für einen seiner Mitarbeiter
- Allgemeiner Antrag auf Basis eines Formblatts

Die wahre Komplexität von Rollenmodellen

Sitzung endet in: 179:39 min

Hier können Sie für sich oder jemand anderen eine Rolle beantragen.

Service Center

- ZIC Passwort ändern
- LAN PW Service
- Objektverwaltung
- Abwesenheiten
- Userverwaltung
- Antrag stellen
- Urlaubsantrag
- Rollenantrag
 - Eigener Antrag
 - Antrag für andere
- Taskmanager
- Info-Übersichten
- Vertragsverwaltung

1. Berechtigungsstatus für Katrin Mustermann

[?]

Bereits zugewiesene Rollen

- Noch mögliche Rollen**
 - iSM-Informationstechnologie
 - Chef-Programmer CSE**
 - S-Chef-Programmer CSE
 - Z- Demo

2. Informationen zur Rolle

Rolle: Chef-Programmer CSE
(fachliche Rolle ohne Berechtigungen)

3. Rollen zuweisen/löschen

Kommentar:

Gültigkeit der Zuordnung:
gültig ab 31. 1. 2006
gültig bis . . .

Folgende Rollenzuweisungen beantragen:

Chef-Programmer CSE

Bild 1: Beispiel für ein Rollen-Antragsverfahren des IPM-Systems **bi-Cube**® IPM

Für diese Prozesse muss im Reporting die Möglichkeit der Nachvollziehbarkeit für den gesamten Ablauf gegeben sein. Es geht nicht nur darum, wer welche Berechtigung (Rolle) wann bekommen hat, sondern auch wer diese beantragt, begründet und dann genehmigt oder auch abgelehnt hat.

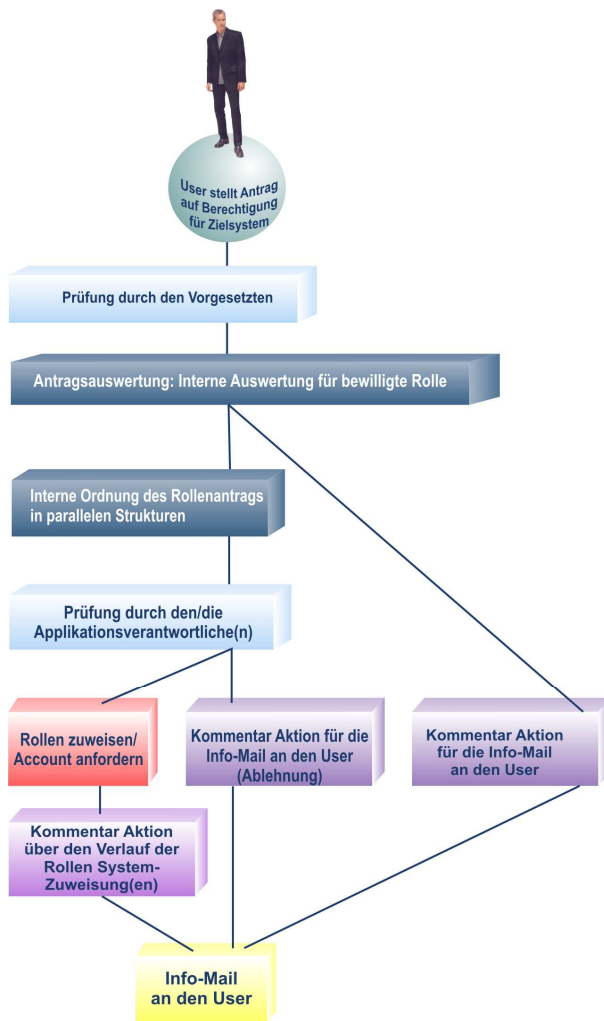


Bild 2: Antragsverfahren für eine Berechtigung im Zielsystem

2.4 Automatisierte Prozesse verringern deutlich die Risiken

Besondere Verantwortung haben in einem zentralen System natürlich die Administratoren. Um das hier objektiv gegebene Risiko deutlich zu verringern, sind möglichst umfassend automatische Prozesse zur Anwendung zu bringen, die eine aktive Beteiligung der Administratoren im regulären Ablauf nicht erforderlich macht bzw. sogar unterbindet.

Damit wird die direkte Berechtigungszuordnung durch den Administrator nur auf Ausnahmefälle beschränkt.

Allein aus dieser Security-Sicht, sollte jede Interne Revision ein IPM-System daraufhin überprüfen, ob es hinreichende Möglichkeiten zur Automatisierung hat. Über die SoP - Prozesse² können (nachweisbar) bis zu 80% der Admin-Tätigkeit automatisiert werden. Das Maß der möglichen Automatisierung hängt natürlich von den Möglichkeiten des jeweiligen IPM-Systems ab. Das hier betrachtete System **bi-Cube**[®] unterstützt die Prozessautomatisierung bei gleichzeitiger Revisionssicherheit sehr umfangreich. Es ist wichtig, dass die Prozessmodellierung von vollautomatisch für Basisrollen (Win 2000, Mailssystem etc.) bis zu mehreren Genehmigungen (z.B. Leiter, Bereich Security,) inkl. einer Bestätigung einer User-Richtlinie, ohne die der User das System nicht final zugewiesen bekommt, alle Möglichkeiten einer Modellierung bietet.

² SoP = Selbstorganisierendes Provisioning

2.5 Security-Classification

Eine weitere Notwendigkeit besteht darin, in der Vielfalt der Objekte eines IPM-Systems (User, Rollen, Applikationen,...) die Möglichkeit zu haben, diese Objekte und Attribute mit einer Security-Classification (SC) zu versehen. So kann z.B. über die Classification generell festgelegt werden, dass bestimmte Rollen nur internen Mitarbeitern zugeteilt werden können oder eine Rolle, die den Zugang zu vertraulichen Unternehmensdaten ermöglicht, nur der Geschäftsführung mit der Classification: Top Secret, zugänglich gemacht wird. Gleichzeitig ist diese Classification die Basis des IKS³, um z.B. auffällige Einzelvorgänge zu ermitteln.

2.6 Schnittstellen und Datenflüsse

Eine möglichst umfassende automatische Kopplung mit vorgelagerten Systemen zu den User- und Organisationsdaten (HR-, Finanz-, und Facility-Systeme) verringert die Möglichkeit der bewussten und unbewussten Datenmanipulation. Deshalb sollten diese Daten weitgehend aus vorgelagerten Systemen übernommen werden.

Die Zielsysteme in denen die Berechtigungen aus dem Zentralsystem gesteuert werden, dürfen keine eigene Administration durchführen. Es muss an dieser Stelle für einen strengen top-down-Fluss gesorgt werden. Es geht dabei nicht nur um das Auseinanderlaufen der Berechtigungen, sondern vor allem um das „Unterlaufen“ des Rollenmodells, wenn im Zielsystem die Berechtigungen am User direkt geändert werden. Aus dieser Sicht, ist der von einigen Anwendern gewünschte bidirektionale Abgleich strikt abzulehnen.

Trotzdem muss die Übereinstimmung der Berechtigungen der User zwischen IPM und Zielsystem ein Prüfungsziel der Revision sein. Diese Aufgabe kann durch eine selektive Migration oder Software-Agenten unterstützt werden, indem diese die Differenzen aufdecken und die Auflösung unterstützen.

2.7 Frühwarnsystem / Internes Kontroll- und Sicherheitssystem

Ein IKS mit integrierter Frühwarnfunktion muss von einem qualifizierten IPM angeboten werden, um den immer strenger werdenden Sicherheitsanforderungen zu genügen.

Das IKS überwacht die Prozesse auf Zulässigkeit, steuert Security-Komponenten (wie vier-Augen-Prinzip und Weiterleitung) ein und entdeckt auf Basis eines internen Regelsystems auffällige Vorgänge. Ein integriertes SSO unterstützt das IKS durch die Überwachungsmöglichkeit dynamischer Informationen, z.B. eine hohe Nutzungsrate kritischer Applikationen bzw. die Nutzung dieser Systeme zu bestimmten Tagesszeiten.

Security-lastige Einzelvorgänge

Dies können beispielsweise die direkten Zuweisungen von Systemen oder Rollen mit $SC = 5^4$ sein, wenn diese Systeme eigentlich nur über ein Antragsverfahren zugeteilt werden sollten. Genauso muss verhindert werden, dass ein Administrator, der Rollen mit einer hohen Security-Classification im Zugriff hat, diese sich selbst zuordnen kann.

Für diesen Bereich gilt die Regel: was nicht verhindert werden kann (oder soll) muss zumindest beobachtet werden.

Ein leistungsfähiges IPM-System bietet die Möglichkeit Regeln zu definieren, nach denen mit bestimmten Attributwerten Zuordnungen von Rollen gesteuert werden. Damit sind diese -aus Sicht der Revision- kritische Attribute, weil an ihren Werten bestimmte Berechtigungen „hängen“. Eventuelle Änderungen dieser User-Attribute sind besonders zu beobachten.

Auffällige Koinzidenzen

Auffällige Zustände sind z.B.

- User mit hoher Zahl kritischer Systeme / Rollen.
- Administratoren, mit Vergabeberechtigung kritischer Objekte (System oder Rolle) und eigener

³ Internes Kontroll- und Sicherheitssystem

⁴ Security-Class: 0=Unmarket, 1=Unclassified, 2=Restricted, 3= Confidential, 4=Secret, 5=Top Secret

Die wahre Komplexität von Rollenmodellen



- Berechtigung an diesem Objekt.
- Nur kurzzeitige Berechtigungen an kritischen Objekten

Risikoreiche Tendenzen

Risikoreiche Tendenzen deuten auf ein erhöhtes Mißbrauchsrisiko hin. Dies kann z.B. die häufige direkte Zuordnung kritischer Objekte sein. Im Ergebnis dieser Erkenntnis sollte hier das Rollenmodell und das Antragverfahren auf diese Objekte ausgedehnt werden, um das genannte Risiko systemintern zu verringern. Die Zahl kritischer Applikationen oder Rollen, die ein Administrator im Zugriff hat, sollte möglichst gering gehalten werden (1 bis max. 2). Das IKS muss diese Vorgänge im Rahmen des Frühwarnsystems intern überwachen.

2.8 Gesichertes Betriebskonzept

Ein IPM-Betriebskonzept, das insbesondere die Systemsicherheit weit besser unterstützt und vor allem den Anforderungen der Internen Revision und solchen Regularien wie SOX, Basel II, usw. entspricht. Das Ziel besteht hierbei darin, die Modellierung von dem Produktiv-System zu trennen. Die Modellierungsmöglichkeiten sind so vielfältig und komplex, dass es ohne ausgiebige Tests nicht ratsam ist, Modellierungen gleich nach jedem Schritt in der Produktion wirksam werden zu lassen. Außerdem lässt sich auf diesem Weg eine „freigebende Instanz“ einschalten, die bestimmte Modellierungen freigibt, bevor diese produktiv wirksam werden. Kern dieser Struktur ist das Entwicklungssystem.

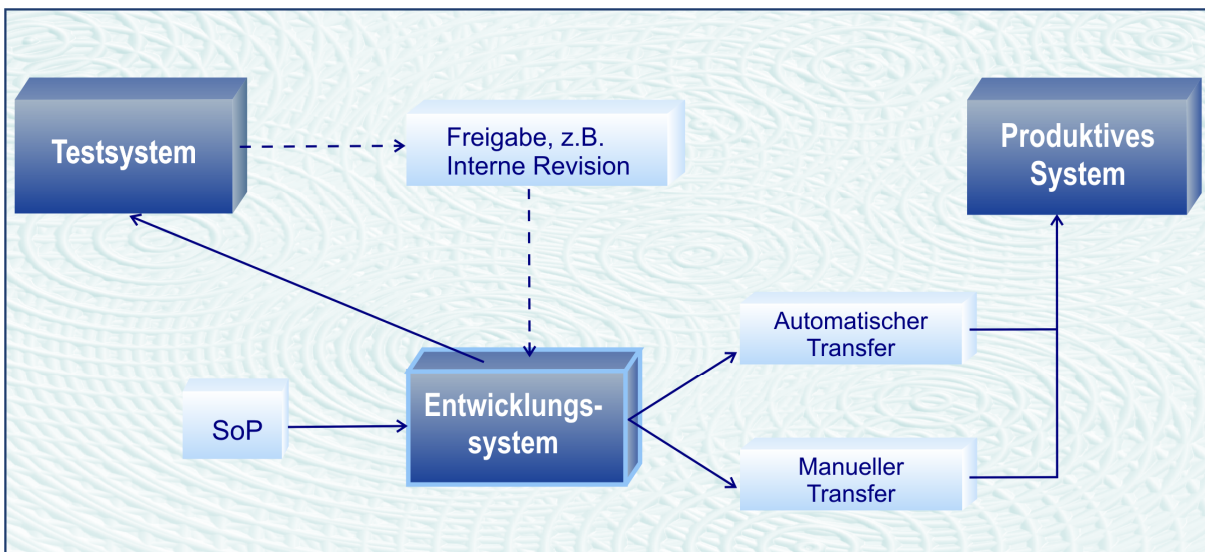


Bild 3: Entwicklungssystem

Die Generierung der synthetischen Rollen mittels des SoP erfolgt im Entwicklungssystem. Der schrittweise und evtl. auch nur teilweise Transfer in das Produktivsystem erfolgt dann nach Prüfung und Freigabe. Die Interne Revision sollte im Rahmen des Betriebskonzeptes darauf dringen, dass im Ansatz die oben dargestellte Betriebsweise umgesetzt wird. Im laufenden Prozess sollte sie in folgende Prozesse (evtl. in Kooperation mit dem Security-Team) als Freigabeorgan fungieren:

1. Festlegung der Security-Classification von Anwendungen und bestimmten Rollenausprägungen.
2. Freigabe von Rollen für das Produktiv-System
3. Kontrolle von Änderungen in der Modellierung im Produktivsystem

3 SOX und Interne Revision

3.1 Nachvollziehbarkeit

Das reguläre Reporting ermöglicht eine Analyse über dem System, zum aktuellen Zeitpunkt und über definierte Zeiträume. Wobei der Ausgangspunkt jeweils der User, das System, die Rolle oder ein Prozess sein kann.

In diesen Bereich fällt auch das Reporting über den Life-Cycle eines Users. Dieser wird in einer Liste dargestellt, die alle Aktivitäten zu einem User vom Usereintritt beginnend, enthält.

3.2 Änderungen in der Modellierung

Änderungen der Modellierungsdaten (z.B. der Rechte einer Rolle) sind einer strengen Kontrolle (Vier-Augen-Prinzip) zu unterwerfen. Um die Revisionssicherheit zu sichern, sollte eine Rolle grundsätzlich nur so lange zu löschen sein, wie über sie noch keine Rechtezuordnung zu einem User erfolgt ist. Deshalb sollen Rollen, die einmal einem User zugeordnet waren nur auf –„nicht verfügbar“- gesetzt werden können. Es muss dann ebenfalls dafür gesorgt werden, dass die Berechtigungen einer –nicht verfügbaren- Rolle nicht mehr verändert werden dürfen.

3.3 Prüfziele der Internen Revision (IR)

Für die IR ist an den entsprechenden Stellen bereits auf mögliche Prüfziele hingewiesen worden. Diese Ziele lassen sich gruppieren nach dem Rollenmodell, der Userzuordnung zu den Rollen, dem definierten Zuordnungs- bzw. Beantragungsprozess und nach der Möglichkeit, Informationen in Richtung eines Frühwarnsystems zu erhalten.

Wichtig ist, dass ein Revisor beim Einsatz eines Rollenmodells nicht mehr vordergründig die Zuordnung von Systemberechtigungen zum User prüfen muss, sondern zu einem 2-stufigen Verfahren (Prüfung der Berechtigungen an den Rollen / Zuordnung der Rollen zu den Usern) übergehen muss: Ein Rollenmodell erfordert zwangsweise eine Standardisierung bzw. Gruppierung von Berechtigungen, was dazu führen kann, dass User auch Berechtigungen erhalten, die nicht unbedingt zur Erfüllung ihrer Aufgaben erforderlich sind. Deshalb ist durch die IR zu prüfen, ob die so genannten Berechtigungs-Spannweite der Fachrollen nicht zu groß gewählt ist. Letztlich ist es Aufgabe der Revision die Wirkungsweise des IKS innerhalb des IPM-Systems zu prüfen.