Compliance Baustein

Der Weg zum rollenbasierten Berechtigungsmodell

Wie senken Vorstände und Geschäftsführer ihr Haftungsrisiko beträchtlich? Erst wer transparente Prozesse hat und weiß wer was zu welcher Zeit darf, ist auf der sicheren Seite. Rollenbasiertes Berechtigungsmanagement ist ein zentraler Sicherheitsfaktor.

Um „Compliant" zu sein, bedarf es organisatorischer und darauf angepasster IT-Maßnahmen.
Rollen ergeben sich aus einer gründlichen Prüfung der Geschäftsprozesse und -erfordernisse und können daher sehr präzise auf die jeweiligen Nutzer bzw. Nutzergruppen zugeschnitten werden.
Durch ein Rollenkonzept und ein zentrales revisionssicheres Berechtigungsverwaltungssystem können der Verwaltungsaufwand und unproduktive Zeiten signifikant gesenkt werden. Das Einsparungspotenzial ist umso höher, je heterogener die IT-Anwendungslandschaft ist.

Meta-Modell Projektablaufplan.

Projektphasen

Es hat sich ein vierstufiges Vorgehen bewährt: Zunächst erfolgt eine detaillierte Ist-Aufnahme (Phase 1), in deren Rahmen die Besonderheiten hinsichtlich der organisatorischen Voraussetzungen und der eingesetzten IT-Systeme erfasst werden. Danach (Phase 2) wird auf Basis dieser Informationen das Soll-Konzept für die künftige Vergabe und Verwaltung von Berechtigungen erstellt.
Darauf aufbauend wird geklärt, in welchen Schritten die Realisierungsphase (Phase 3) durchgeführt werden soll. Bereits während der Implementierung kann mit den Überlegungen begonnen werden, welche Auditing-Maßnahmen (Phase 4) eingesetzt werden, um die dauerhafte Einhaltung und Verbesserung des Konzepts zu gewährleisten. Es kann auch notwendig werden, operative Arbeitsprozesse an die in den Berechtigungsprofilen festgelegten Rechte anzupassen.

(1) Basisinformationen erfassen

Basis für die Implementierung eines unternehmensweiten rollenbasierten Berechtigungsmodells ist eine detaillierte Ist-Aufnahme. Hierbei wird geklärt, welche Sicherheitsrichtlinien im Unternehmen vorliegen, wie die aktuellen Administrationsprozesse aussehen, welche Anwendungssysteme berücksichtigt werden sollen und wie in diesen bisher Berechtigungen vergeben werden. Außerdem ist es in dieser Phase entscheidend, Transparenz für sämtliche Besonderheiten zu schaffen.

(2) Soll Konzept „Administration"

Ein unternehmensweites Soll-Konzept ist entscheidend für die erfolgreiche Umsetzung eines einheitlichen rollenbasierten Berechtigungsmodells in möglichst vielen Systemen. Darin werden – basierend auf den Sicherheitsrichtlinien des Unternehmens – die Administrationsrichtlinien festgelegt.

Es werden unter anderem Fragen wie „Erfolgt künftig eine zentrale oder dezentrale Administration?" (Prozesse und Beteiligte) und „Soll die Rechtevergabe stellen- oder tätigkeitsorientiert erfolgen?" und „Berücksichtigen wir systemspezifische Besonderheiten oder kann eine Standardisierung erfolgen?" geklärt. Je mehr Details geklärt werden, desto weniger Überraschungen ergeben sich in Nachfolgeprojekten, wenn weitere Anwendungssysteme eingebunden werden sollen. Aus dem Sollkonzept ergeben sich Kriterien für ein möglicherweise benötigtes zentrales, rollenbasiertes und revisionssicheres Berechtigungsmanagementsystem.

(3) Soll-Konzept detaillieren und implementieren

Wie in den ersten Projektphasen hängt auch der Erfolg der Implementierung von der Einbeziehung der Beteiligten ab: Die Administratoren und Anwendungsverantwortlichen kennen die Besonderheiten der einzelnen Systeme.
Die Betriebsorganisation sowie die Fachabteilungen überblicken die Arbeitsabläufe und die dazu notwendigen Anwendungen und Kompetenzen. Die Security-Abteilung muss die Einhaltung der Sicherheitsrichtlinien und des Soll-Konzepts überwachen. Die Implementierung erfolgt in vier Schritten:

1. Rollenmodellierung: Design der fachlichen Berechtigungsprofile,
2. Rechtekonzeption: Abstimmung der Berechtigungsprofile,
3. Qualitätssicherung der Berechtigungsprofile,
4. Umsetzung der Berechtigungsprofile in den einzelnen Systemen und Anpassung der Antrags- und Administrationsprozesse.

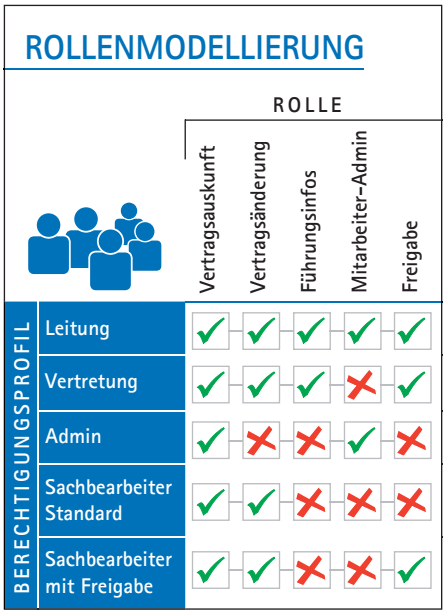
➔

Mit Ausnahme von Schritt 1 können die weiteren Schritte systemweise und unabhängig voneinander durchgeführt werden. Die Rollenmodellierung kann sowohl abteilungsintern als auch abteilungsübergreifend erfolgen.
Ein mögliches Ergebnis kann z. B. folgendermaßen aussehen: Das Berechtigungsprofil „Sachbearbeiter mit Freigabe" erhält die Rolle Vertragsauskunft, Vertragsänderung und Freigabe von Zahlungen bis zur im System hinterlegten Höhe.

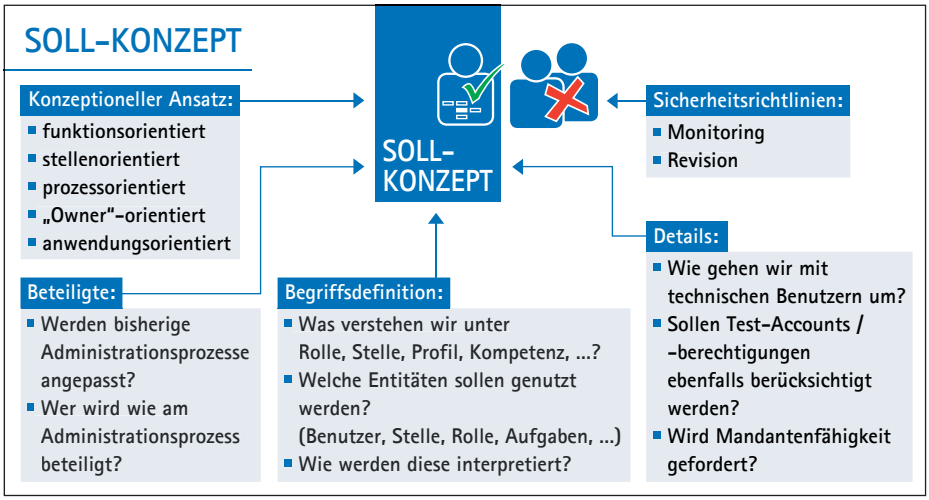
(4) Auditing-Maßnahmen

Nach Modellierung und Implementierung müssen regelmäßige Auditing-Maßnahmen eingeführt werden. Dies im Sinne des Investitionsschutzes und der kontinuierlichen Minimierung des Haftungsrisikos. Die Erfahrung zeigt, dass es bei der rollenbasierten Berechtigungsmodellierung nicht ausreicht, ein allgemeines Konzept zu erstellen und umzusetzen. Der Erfolg eines rollenbasierten Berechtigungsmodells hängt entscheidend davon ab, wie es im Vorfeld gelingt, die verschiedenen Einflussfaktoren in einem Soll-Konzept zu berücksichtigen und somit einen allgemein gültigen Standard für das Unternehmen zu setzen, die Besonderheiten der individuellen Systeme abzubilden und die Administrationsprozesse zu überprüfen.

Frank Böhm, FSP GmbH



Beispiel:
Berechtigungsprofil: „Sachbearbeiter mit Freigabe" erhält die Rollen Vertragsauskunft, Vertragsänderung, und Freigabe von Zahlungen bis zur im System hinterlegten Höhe.



Einflussfaktoren Soll-Konzept

Praxisbeispiel zu rollenbasierter Rechtekonzeption

Zentrales, rollenbasiertes und revisionssicheres Berechtigungsmanagement

Ein großes Finanzdienstleistungsunternehmen hatte unterschiedliche historisch gewachsene Anwendungssysteme auf verschiedenen Plattformen im Einsatz. Der Administrationsprozess sah vor, dass die Beantragung von EDV-Berechtigungen zwar über eine zentrale Organisationseinheit, die eigentliche Administration jedoch dezentral bei den einzelnen Systemadministratoren erfolgte.
Aufgrund von Abhängigkeiten zwischen einzelnen Systemen kam es immer wieder zu Verzögerungen bei der Bereitstellung von EDV-Berechtigungen. Außerdem war die systemübergreifende Transparenz hinsichtlich sämtlicher Berechtigungen eines Benutzers nur mit sehr großem Aufwand zu erreichen. Ziel war es, eine zentrale und einheitliche Datenbasis für sämtliche EDV-Berechtigungen zu schaffen, in der neben den aktuellen auch die historisierten Rechte auf Knopfdruck abrufbar sind. Außerdem sollte für den Antrag von Standardberechtigungen nur noch eine Freigabe des Antrags durch den Administrator erfolgen. Die Zuweisung der Berechtigungen in den einzelnen Systemen sollte ein speziell hierfür eingeführtes Berechtigungsmanagement-System automatisieren.
Zukünftig sollte es einen zweigeteilten Administrationsprozess geben:
Zunächst sollten Berechtigungsprofile grundlegend gestaltet werden (Anlegen, Ändern, Löschen). Danach sollte die automatisierte Vergabe der Standardberechtigungen an einzelne Benutzer (die Profilzuweisung) erfolgen. Aus diesen Vorgaben ergaben sich dann die unternehmensspezifischen Anforderungen an das Soll-Konzept zur künftigen Berechtigungsmodellierung und -administration.
Administrationsprozess und Rollenkonzept. Durch die Zweiteilung des Administrationsprozesses werden zusätzliche Anforderungen an die Administratoren gestellt: Ihre Aufgabe ist es nun, die Neuanlage und Änderungen von Profilen mit den Fachabteilungen und Anwendungsverantwortlichen abzustimmen und im Berechtigungsmodell zu hinterlegen. Wie sieht dieses Berechtigungsmodell aus? Um die Antragsstellung für die Fachabteilung möglichst einfach zu gestalten, orientieren sich die Berechtigungsprofile an den fachlichen Stellen (wie Abteilungsleiter, Administrator oder Sachbearbeiter). Jeder Mitarbeiter erhält also eine Stelle, die mit den notwendigen Rechten ausgestattet ist.
Die Modellierung dieser Stellen wird entscheidend durch die vorhandenen Entitäten der zentralen Berechtigungssoftware geprägt. In unserem Beispiel stehen Entitäten wie Aufgaben, Rollen und Rollengruppen zur Verfügung.
Diese ermöglichen – in Abhängigkeit der einzelnen Anwendungssysteme – die abteilungsinterne Strukturierung der Rechte. Zur Vereinfachung des Profildesigns werden Rollen definiert, die sich an Arbeitsvorgängen orientieren und somit jeweils von allen Mitarbeitern, einem Teil oder einigen wenigen erfüllt werden.