



# Von der Rolle

## Rechtevergabe

**Größere Unternehmen verlieren allmählich den Überblick über die Rechtevergabe ihrer Mitarbeiter gegenüber den Applikationen. Das hat Folgen bis in die Revision hinein. Die Zugriffe können nachträglich nicht mehr lückenlos nachvollzogen werden. Rollen helfen, Ordnung in die Zugriffe und Revisionen zu bringen.**

**D**azu müssen solche Rollen, die die Eigenschaften und Rechte einzelner Mitarbeiter im Unternehmen repräsentieren, planvoll auf den Weg gebracht werden. Gefragt ist ein in sich schlüssiges Rollenkonzept. Es setzt die Mitarbeiter an den Geschäftsprozessen mit den Applikationen in Beziehung zur Organisation mit den einzelnen Fachbereichen und Aufgaben. Nur mit einem ganzheitlichen Blick können für jeden Mitarbeiter stimmige Rollen einschließlich der Rechte und Attribute abgeleitet werden. Attribute ermöglichen unter anderem, die persönlichen Berechtigungen bis auf Funktionsbereiche einzelner Applikationen herunter zu brechen. Das setzt voraus, dass das Tätigkeitsfeld jedes Mitarbeiters, inklusive der bestehenden internen und externen Regeln, genau nachvollzogen und festgehalten wird. Zu professionell entwickelten Rollen gehört, dass die Identität jedes Mitarbeiters verlässlich abgesichert wird. So dürfen in größeren Unternehmen Namensgleichheiten nicht zu Verwechslungen führen. Rollenkonzepte werden dann in aller Regel im Topdown-Ansatz anhand von Organisationszugehörigkeit und Aufgabenmerkmalen durch Erhebungen erstellt und dokumentiert. Verlässliche Rollen und Identitäten sind die Grundvoraussetzung dafür, dass:

- ◆ vergebene Berechtigungen systematisch einer Prüfung unterzogen werden können,
- ◆ später eine solide Basis für die Berechtigungsverwaltung, zum Beispiel für User-Provisioning, herausgebildet werden kann.

Noch ist es nicht soweit. Mit einem dritten Schritt sollten mögliche Rechte-, Regel- und Funktionskollisionen abgefangen werden. Die Top-down-Vorgehensweise kann zu Fehlzuordnungen und damit zu doppelten oder falschen Mitarbeiteraktionen führen. Deshalb sollten Bottom-up Unterscheidungen wie in PLZ-Gebiete oder in Fach-/Zuständigkeitsbereiche zur Gegenprüfung hinzugezogen werden. Weiterführende,

hilfreiche Informationen dafür finden die Verantwortlichen in den Geschäftsdatenbanken. So können sie das Rollenkonzept, beispielsweise über Spreadsheets, sukzessiv verfeinern.

Diese Verfahrensweise zieht kaum Aufwände nach sich. Denn für die Applikationsattribute fällt, anders als beim klassischen User-Provisioning-Prozess, keine Integration der Applikationen über Konnektoren respektive Agenten an. Statt dessen werden die Attribute über das jeweils einfachste verfügbare Verfahren der Applikationen extrahiert. Anschließend werden sie nach Bedeutung geordnet, als CSV-Datei hinterlegt und dem Rollenkonzept gegenübergestellt. Das Ergebnis dieser Verfeinerung – kollisionsfreie Rollen – sollte den Berechtigungsvergebern in den Fachabteilungen zur Zwischenprüfung vorgelegt werden. Bevor die Bevollmächtigten im Unternehmen das Rollenkonzept mit allen Einzelrollen einer finalen Prüfung unterziehen, um es schließlich abzusegen.

Vorteile bringt das entwickelte Rollenkonzept auch für Revisionen. Jede Rolle mit ihren Rechten und Attributen ist eindeutig dem Mitarbeiter zuordbar. Somit wird transparent, was er darf und was nicht. Handlungen darüber hinaus treten den Revisoren über die Rollen plastisch vor Augen. Ebenso kann über Administrationsrollen jederzeit geprüft werden, ob von den Systemverwaltern über ihre Befugnisse hinaus Eingriffe auf Applikationen ausgingen. Die Ergebnisse jeder Revision einschließlich aller eingesetzten Rollen sollten lückenlos dokumentiert werden. Das ist notwendig, um sowohl die Einhaltung als auch die Verstöße gegenüber internen und externen Regeln nachweislich zu belegen. Diese dokumentierte Brainware wird außerdem dafür gebraucht, um das Rollenkonzept in einem Zeitrhythmus gegenüber dem Ist-Zustand – Organisation, Identitäten, Geschäftsprozesse, Applikationen – zu prüfen und die Rollen entsprechend anzupassen. Auch die Rollen der Administratoren sollten in die regelmäßigen Prüfungen einbezogen werden, von ihnen mit ihren erweiterten Befugnissen können ebenfalls Pflichtverletzungen, beabsichtigt oder unbeabsichtigt, ausgehen.

Revisionen können über Papier abgewickelt werden. Oder es wird ein Rollen-Managementsystem eingesetzt. Es vereinfacht, dokumentiert revisionsfähig und beschleunigt die Rollenprüfung. Jedem Bevollmächtigten wird automatisch ihr Teil der Rollen am Bildschirm eingeblendet, den sie zu verantworten haben. Eines sollten die Verantwortlichen bei der Rollenkonzeption beherzigen: keep it simple. Es sollten nie mehr Rollen im Unternehmen eingeführt, die Rollen nicht mehr in Rechte und Attribute differenziert werden, als unbedingt notwendig ist.

**Norbert Drecker ist Geschäftsführer von Twinsec**  
E-Mail: [Norbert.Drecker@Twinsec.de](mailto:Norbert.Drecker@Twinsec.de)