

Berechtigungen besser im Griff

Rollenkonzept professionell auf- und umgesetzt

Im Zeitalter von Governance und Compliance sind Management und Revision von Berechtigungen besonders wichtig. Bei gleichzeitig deutlich gesteigener Heterogenität und Komplexität der IT-Umgebungen lohnt sich häufig die Umsetzung durch ein Rollenkonzept. Richtiges Rollenmanagement erfordert dabei allerdings eine breite Aufstellung mit mehr als nur IT-Know-how.

Von Norbert Drecker, Köln

Mit der Zahl der IT-Anwendungen sowie einer organisationsübergreifenden und vernetzten Bereitstellung von Informationen wächst in Unternehmen die Gefahr, dass den Verantwortlichen das Berechtigungsmanagement entgleitet – vor allem, wenn es noch über die Vergabe individueller Rechte geregelt ist. Diese Entwicklung bewirkt nicht nur eine unzureichende Berechtigungskontrolle und damit eine mögliche Gefährdung sensibler Anwendungen und Daten, sondern zieht auch den Nachweis der Erfüllung interner Richtlinien und externer Vorschriften in Mitleidenschaft. Ein professionelles Rollenkonzept hilft hier, ein ebenso professionelles

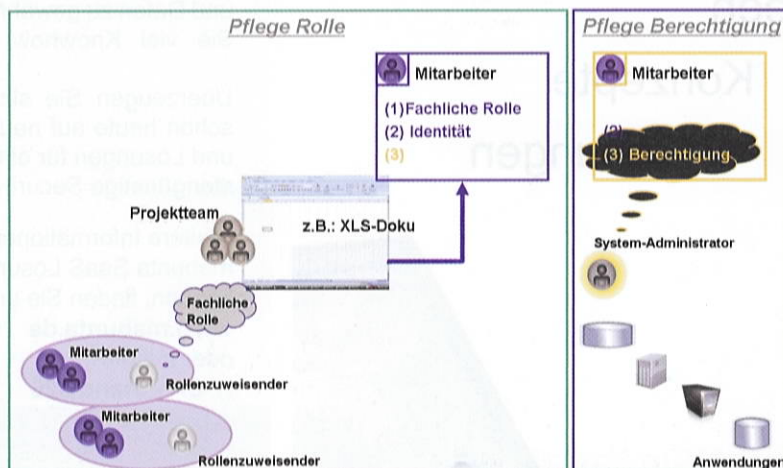
Berechtigungsmanagement umzusetzen.

Wer nach der Analyse eines unbefriedigenden Ist-Zustands zur Schlussfolgerung gelangt, den Kampf für die Einführung oder Verbesserung eines Rollenkonzepts aufzunehmen, ist meist ein betriebsnaher IT-Verantwortlicher – denn er muss ein intimer Kenner des täglichen Berechtigungsmanagements sein. Unterstützung für sein Projekt findet er ebenfalls am ehesten bei Gleichgesinnten (ITlern), sofern diese bereit sind, sich neben dem Tagesgeschäft für Verbesserungen in Richtung eines professionellen Berechtigungsmanagements einzusetzen.

Doch für ein dauerhaft erfolgversprechendes Rollenkonzept reicht der Antrieb allein aus der IT-Abteilung heraus nicht aus: Zusätzlich muss auch die organisatorische Sicht mit ihren fachlichen Anforderungen vertreten sein. Nur unter dieser Voraussetzung ist eine tragfähige Ausgestaltung eines Rollenkonzepts möglich, das fortan dem Berechtigungsmanagement zugrunde liegen soll.

Das heißt: Sowohl die Fachabteilungen als auch die Revision und das Management müssen für das Vorhaben gewonnen werden! Das gelingt oft am besten durch die Darstellung des mit dem Vorhaben verknüpften risikominimierenden sowie governance- und compliance-relevanten Nutzens. Die Systematik dahinter: Unternehmen legen in Governance ihre Geschäftsinhalte fest und definieren den Rahmen der Unternehmensethik sowie die dazu gehörigen Regeln. Daraus leiten sich die Vorgaben für das Risk-Management im Sinne der Organisation ab, das wiederum die Compliance speist: Denn letztlich fordert diese Instanz Nachweise ein, wie weit die festgelegten Governance- und Risk-Management-Vorgaben auch nachweislich eingehalten wurden.

Abbildung 1: Konzeption der Rollen und Unterstützung von Fachseite in „Etappe 1“



Rollenkonzept als Wegeplan

Leider fehlt in etlichen Unternehmen eine übergreifende „Landkarte“, welche die Wege verzeichnet, wie Informationen für diese Abläufe zeitnah und gezielt die richtigen Ansprechpartner erreichen sollen und können. Die Folgen sind – neben einem unnötig hohen Aufwand – unvollständige und fehlgeleitete Informationen. In der Konsequenz lassen sich Go-

vernance-, Risikomanagement- und Compliance-Anforderungen nur unzureichend erfüllen. Überdies steigt im undurchsichtigen Wegewirrwarr das Risiko, dass „Wegelagerer“ wichtige Informationen abgreifen.

Ein für alle Berechtigte transparentes Rollenkonzept räumt mit diesen Nachteilen gründlich auf, indem es die Verfahren für das Berechtigungsmanagement vereinheitlicht und alle Berechtigungen so beschreibt, dass sie – auch außerhalb der IT-Abteilung – nachvollziehbar sind. Auf diese Weise wird das Berechtigungsmodell für die Fachseite, die Revision und das Management mit ihren jeweiligen Verantwortungsbereichen verständlich – einschließlich der Wechselwirkungen zwischen den einzelnen Instanzen.

Das Prinzip des Rollenmanagements weist jedem Mitarbeiter im Unternehmen, gegebenenfalls

auch bei Geschäftspartnern, eine Rolle mit seinen persönlichen Rechten für einzelne Anwendungen zu. Unverzichtbarer Anker ist die Aufnahme eindeutiger Identitäten, die in der Regel einer natürlichen Person entsprechen.

Etappe 1: Planung

Rollen haben neben der organisatorischen aber auch eine fachliche Aufhängung: Deshalb müssen für die Entwicklung eines hieb- und stichfesten Rollenkonzepts zunächst die Organisation und die Abläufe sowie die daran beteiligten Anwendungen, Fachverantwortlichen (inklusive ihrer Verantwortungsbe-reiche) und Mitarbeiter sowie deren Tätigkeitsfelder untersucht werden. Dazu müssen alle Beteiligten in Beziehung zu den Organisationsstrukturen sowie Geschäftsprozessen (bzw. Applikationen) gesetzt werden, an denen sie mitwirken.

Viele dieser Informationen lassen sich aus bestehenden Geschäftsdatenbanken entnehmen, um sie anschließend beispielsweise in Form eines Spreadsheets oder (besser) über Rollen-Tools darzustellen. Den wesentlicheren Input liefern jedoch die Verantwortlichen der Fachseite: Erst eine eingehende Vorab-Recherche ermöglicht es, die individuellen Rollen für die erforderlichen Rechte (zunächst grob) herauszubilden – getreu der Devise so viel Berechtigungen wie notwendig, aber nicht mehr als nötig.

Teil dieser Analyse sollten auch die internen Richtlinien und externen Vorschriften sein, die von den Fachverantwortlichen beziehungsweise Mitarbeitern bei der Arbeit mit den Anwendungen zu befolgen sind. Nur unter dieser Voraussetzung wird sich später mittels Auditing- und Reporting-Tools genau gegenüberstellen lassen, was der

Einzelne darf und wo und wann die vergebenen Berechtigungen davon abweichen.

Etappe 2: Prüfung

Im zweiten Schritt geht es darum, das entwickelte Rollenkonzept auf Richtigkeit zu prüfen, es zu ergänzen und weiter anzupassen. Hierzu eignet sich nichts besser, als die technischen Informationen zu den bereits existierenden Berechtigungen in IT-Anwendungen zu Rate zu ziehen. Die relevanten Berechtigungsdaten sollten dazu aus den Anwendungen extrahiert und in einem universellen Format (z. B. als CSV-Datei) gespeichert werden. Diese Informationen sind zwingend von den Systemverantwortlichen mit einer Beschreibung der Felder und Attribute zu versehen, damit eine Verständnisbrücke für die Fachseite geschlagen und Fehldeutungen ausgeschlossen werden können.

Die Fachabteilungen prüfen dann zunächst die einzelnen Rollen durch den Abgleich der im Unternehmen angewandten technischen Anwendungsberechtigungen mit dem Rollenkonzept aus der ersten Etappe. Dabei werden nicht selten bestehende Missverständnisse zwischen gewollten fachlichen Anforderungen und technischen Umsetzungen aufgedeckt. Erst wenn die fachlichen Rollen mit der Umsetzung der technischen Berechtigungen – ohne unnötiges Beiwerk – übereinstimmen, können die Fachrollen finalisiert werden.

Die zweite Prüfung innerhalb dieser Etappe zielt auf die Personen ab, die aktuell den einzelnen Fachrollen zugeordnet sind: Solche personenbezogenen Prüfungen sind notwendig, um überflüssige, aber auch vergessene Berechtigungen aufzudecken. Das Ergebnis ist ein bereinigter Bestand an Benutzerberechtigungen, die anschließend der Fachseite zur Zertifizierung vorgelegt werden können. Innerhalb dieser Projektphase sollte sich das Team idealerweise eines Tools bedienen, dass sowohl beim Abgleich unterstützt als auch die festgelegten Informationen automatisch dokumentiert.

Vorteile

Verlässliche Identitäten, Rollen und Regelzuordnungen sind letztlich die Grundvoraussetzung dafür, dass mit Blick auf die technische Realisierung

- _____ vergebene Berechtigungen systematisch einer Prüfung unterzogen werden können,
- _____ eine solide Berechtigungsverwaltung herausgebildet werden kann (z. B. für User-Provisioning) sowie
- _____ Regeln aufgrund von internen Richtlinien oder externen Vorschriften nun per Auditing und

Reporting immer eindeutig einem Verantwortlichen zugewiesen und genau bemessen werden können.

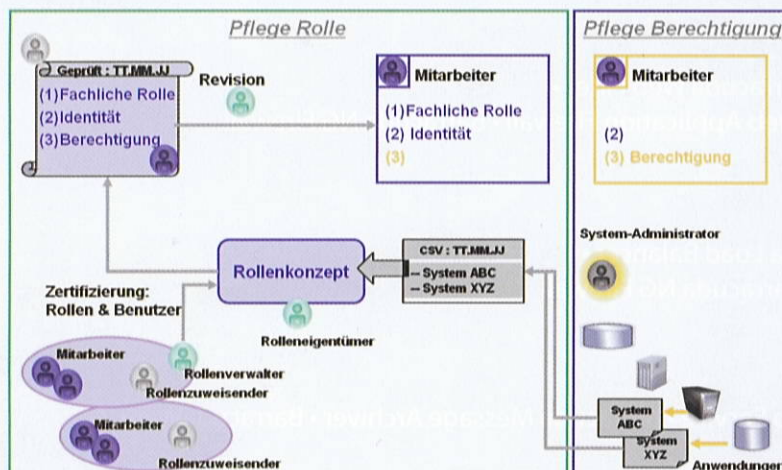
Sobald das Rollenkonzept nach den zwei initialen Etappen verlässlich steht und von den Bevollmächtigten im Rahmen einer Schlussprüfung abgesegnet wurde, sollte die begleitende Dokumentation exakt ausweisen, welcher persönlichen Rolle welche Anwendungsrechte sowie Attribute für Funktionen und Inhalte innerhalb der Applikationen verbindlich zugeordnet wurden. Diese Transparenz über alle Rollen erleichtert später nicht nur den Systemadministratoren die Überwachung und Steuerung der Zugriffskontrolle. Bei künftigen internen Veränderungen können so auch alle notwendigen Rollen-, Rechte- und Regelanpassungen schnell und gezielt lokalisiert und durchgeführt werden. Darüber hinaus profitiert das Unternehmen bei Revisionen – wer darf aktuell was? – von einer solchen lückenlosen und verbindlichen Dokumentation.

Administration und Technik

Die Systemadministratoren tragen beim Rollenmanagement eine besondere Verantwortung: Sie interpretieren für die Fachseite die Rollen mit ihrer spezifischen Expertise und prägen damit die System- und Anwendungseigenschaften für alle Benutzer. Zudem müssen sie nach den festgelegten Regeln die Benutzerberechtigungen pflegen, sofern diese Aufgabe nicht von einem User-Provisioning-System erledigt wird.

Darüber hinaus haben Systemadministratoren jedoch auch Berechtigungen, die weit über die klassischen Benutzerrechte hinaus gehen und die sich dementsprechend nur schwer in kontrollierbare Prozesse einbinden lassen. Eine Prüfung, ob sie ihre erweiterten Rechte immer im Sinne des Unternehmens anwenden, ist nur über eine ausführ-

Abbildung 2: Validierung und Zertifizierung der Rollen in „Etappe 2“



liche Systemprotokollierung und gegebenenfalls Sicherheitsalarmierung möglich.

Die detaillierten Ergebnisse des Rollenkonzepts können – wie bereits angesprochen – entweder zur technischen Realisierung des Rollenmanagements innerhalb eines Identity- und Access-Management-(IAM)-Systems herangezogen werden. Oder sie können als Grundlage für die technische Umsetzung des Rollenmanagements direkt innerhalb der Anwendungen dienen. Selbst der Aufwand einer direkten technischen Kopplung zwischen Rollenmanagement und User-Provisioning hält sich in Grenzen, da diese Verbindung oftmals innerhalb einer umfassenden Produkt-Suite einzelner Anbieter vorbereitet und zusammengeführt werden kann.

Mittlerweile bietet der Markt Software-Tools, die alle Etappen des Rollenkonzepts wirkungsvoll unterstützen. Der Vorteil ist allem voran eine drastische Reduktion der Entwicklungszeit. Allerdings haben solche Werkzeuge auch ihren Preis – und der sollte zur möglichen Projektverkürzung und Aufwandreduzierung ins Verhältnis gesetzt werden. Die Software-Tools vereinfachen

darüber hinaus meist auch den Betrieb des Rollenmanagements und eine Re-Zertifizierung des Rollenkonzepts – notwendige Anpassungen können dadurch schneller und so gegebenenfalls kostensparend durchgeführt werden.

Revisionen auf Basis des Rollenkonzepts und -modells können durchaus ganz klassisch auf Papier abgewickelt werden. Alternativ kann jedoch auch ein Rollenmanagementsystem zum Einsatz kommen: Es vereinfacht und beschleunigt die Rollen- und Regelprüfung, indem es elektronisch eine revisionsfähige Dokumentation liefert. Im Rahmen des Rollenmanagements können so jedem Bevollmächtigten automatisch diejenigen Rollen und Regeln am Bildschirm vorgelegt werden, die er zu verantworten hat.

So oder so sollte für die Rollen „keep it simple“ gelten, um weder bei der Administration noch bei Revisionen jemals den Überblick zu verlieren.

Fazit

Auch nach der technischen Realisierung des Rollenmanagements profitieren Unternehmen

von einem hieb- und stichfesten Rollenkonzept, das detailliert dokumentiert wurde. Dem Management, der Revision, der Fachseite und den IT-Verantwortlichen steht damit eine verständliche und einheitliche Entscheidungsgrundlage zur Verfügung.

Zudem lässt sich immer wieder (z. B. regelmäßig im Halbjahresrhythmus) auf einfache Weise prüfen, ob das Rollenmanagement aktuellen Anforderungen weiter standhält. Eine Re-Zertifizierung der entwickelten Rollen mit den Rechten, Attributen und Regeln ist immer dann sinnvoll, wenn es zwischenzeitlich zu Veränderungen innerhalb der Organisation, bei Identitäten, Geschäftsprozessen, Applikationen, Sicherheitsstrategien oder auch Richtlinien und Vorschriften gekommen ist. Schon bei Veränderungen in einem einzelnen dieser Bereiche sollten die Verantwortlichen zur eigenen Sicherheit eine Re-Zertifizierung des Rollenkonzepts ansetzen. ■

Norbert Drecker ist Geschäftsführer der Twinsec GmbH.