Die Zahl der Anwendungen sowie die organisationsübergreifende und vernetzte Bereitstellung von Informationen in den Organisationen wachsen. Damit steigt auch die Gefahr, dass den Verantwortlichen die Berechtigungen, geregelt über die Vergabe individueller Rechte, außer Kontrolle geraten. Diese Entwicklung schlägt sich nicht nur in einer unzureichenden Berechtigungskontrolle und damit in der Gefährdung sensibler Anwendungen und Daten nieder. Auch der Nachweis der Erfüllung eigener interner Richtlinien und externer Vorschriften leidet darunter. Ein professionelles Rollenkonzept, basierend auf einer handhabbaren Technologie, ist die richtige Antwort.

Erfolgreiche Einführung eines Rollenkonzepts

Norbert Drecker, TWINSEC GmbH

Das Thema „Rollenkonzepte“ wird oft als abgehoben, abstrakt und praxisfern eingeordnet. Daher zunächst zwei Praxisbeispiele, die anhand der Anforderungen die nachfolgenden Beschreibungen zu den Ansätzen und Technologien nachvollziehbar machen:

- Von Seiten der Aufsichtsbehörden ist einem Finanzinstitut vorgegeben, die Nachweise darüber zu liefern, welche Mitarbeiter der Organisation Zugriff auf die Anwendungen haben und ob der Missbrauch von Berechtigungen ausgeschlossen ist. In der Organisation des Finanzinstituts war dazu ein Verfahren zu etablieren, um für die kritischen Anwendungen eine Zertifizierung und den Check zur „Seperation of Duty“ (SoD) für Tausende von Mitarbeitern von Hunderten von Vorgesetzten durchzuführen.
- Ein Versicherer verwendete in der Vergangenheit in diversen Anwendungen bereits Rollenansätze zur Berechtigungsvergabe. Im Unternehmen ist nun ein einheitliches und durchgängiges Rollenkonzept gefordert, das die sich ändernden Geschäftsanforderungen abbilden kann und zur Rechtevergabe als Vorgabe dient. In der Organisation des Versicherers war dazu eine Umgebung zur Verwaltung eines Rollenkonzepts einzuführen, die in Verbindung mit einem IDM-System die Berechtigungen mit den Anwendungen zunehmend automatisiert abgleicht.

Das Rollenkonzept ist das Fundament des Erfolgs

Die Rollen, die die Eigenschaften und Rechte einzelner Mitarbeiter im Unternehmen repräsentieren, sind systematisch zu erheben und zu gestalten, um das Fundament zur Lösung der Anforderungen zu bilden. Gefragt ist ein in sich schlüssiges Rollenkonzept. Es setzt die Mitarbeiter in den Geschäftsprozessen mit den Anwendungen in Beziehung zur Organisation mit den einzelnen Fachbereichen und Aufgaben. Denn es ist eine ganzheitliche Sicht notwendig, um für jeden Mitarbeiter stimmige Rollen und, davon abgeleitet, die Berechtigungen in Anwendungen vergeben zu können. Das setzt voraus, dass die Aufgaben jedes Mitarbeiters und die zugehörigen Regeln beschrieben und nachvollziehbar sind. Nur unter dieser Voraussetzung sind persönliche Rollen auf die Anwendungen, auf die der Mitarbeiter Zugriff haben soll, funktional ausrichtbar.

Die Fachseite gehört mit ins Boot

Eine systematische Rollenverwaltung unterliegt der Regel, dass jeder Mitarbeiter im Unternehmen, gegebenenfalls auch Geschäftspartner, eine Rolle zur Ableitung seiner persönlichen Rechte für einzelne Anwendungen erhält. Unverzichtbarer Anker ist zunächst die Aufnahme der eindeutigen Identitäten, die in der Regel eine natürliche Person spiegelt.

Rollen haben neben der organisatorischen vor allem eine fachliche Aufhängung. Deshalb werden für die Entwicklung eines hieb- und stichfesten Rollenkonzepts zunächst die Organisation und die Abläufe sowie die daran beteiligten Anwendungen, Fachverantwortlichen inklusive ihrer Verantwortungsbereiche und Mitarbeiter einschließlich ihrer Tätigkeitsfelder untersucht. Dazu müssen die Verantwortlichen und Mitarbeiter in Beziehung zu den Organisationsstrukturen und den Geschäftsprozessen/Anwendungen gesetzt werden, an denen sie mitwirken.

Viele dieser Informationen können aus den bestehenden Geschäfts-Datenbanken oder aus vorhandenen Tabellen gezogen werden. Den wesentlichen Input liefern jedoch die Verantwortlichen der Fachseite. Dazu sind umfassende Recherchen durchzuführen, die oft in Form von Interviews zu führen sind, um die Vielfalt der Tätigkeitsfelder in Form von Rollen zu fassen. Dabei gilt: so viele Rollen wie notwendig, aber nicht mehr als nötig. Teil dieser Analyse sind auch die internen und externen Richtlinien, die in der Organisation – in Form von Policies und rechtlichen Vorschriften – bei der Arbeit mit den Anwendungen befolgt werden müssen. Dies ist die Voraussetzung dafür, dass dann auch in Audit-Verfahren nachvollziehbar wer-

den kann, was der Einzelne darf, und dass Abweichungen aufgedeckt werden können.

Die IT-Verantwortlichen komplettieren die Bootsbesatzung

Oftmals ist aber „gut gedacht" nicht schon gleich „gut getan". Daher ist das entwickelte Rollenkonzept noch auf Richtigkeit zu prüfen und gegebenenfalls anzupassen. Hierzu werden die Anwendungsverantwortlichen zu Rate gezogen, die zu den bereits genutzten Anwendungen die relevanten Berechtigungsdaten identifizieren und herausziehen. Diese Informationen sind zwingend von den Anwendungsverantwortlichen mit einer Beschreibung der Felder und Attribute zu versehen, damit die Deutung auch der Fachseite ermöglicht wird.

Die Fachseite prüft zunächst die einzelnen Rollen durch den Abgleich der im Unternehmen angewandten technischen Anwendungsberechtigungen gegen das Rollenkonzept. Dabei kann es nicht überraschen, dass bei diesem Vorgehen oft lange gelebte Missverständnisse zwischen gewollter fachlicher Anforderung und der nach bestem Wissen interpretierten technischen Umsetzung aufgedeckt werden. Am Ende der Prüfung und nach eventuell durchzuführender Nachjustage kann dann die Rolle allgemein als zertifiziert gelten.

Des Weiteren ist noch zu prüfen, wem die Rollen wirklich aktuell zugeordnet sind. Dies dient dazu, überflüssige und vergessene Anwendungsberechtigungen aufzuspüren und einen bereinigten Stand herzustellen, auf den man nun zukünftig bauen kann.

Ein Projekt-Team, bestehend aus Fachseite und IT, muss sich in diesen Prozessen eines Tools bedienen können, das die Abgleiche technisch unterstützt und auch die Dokumentation der Informationen und Festlegungen abbilden kann. In den skizzierten Praxisbeispielen nutzten der Finanzdienstleister und der Versicherer in der initialen Projektphase Oracle Identity Analytics (OIA), um die Identitäten über einen Import zentral zu übernehmen, und die Fachverantwortlichen führten dann die Rollen ein. Zur Prüfung der Schlüssigkeit und der Richtigkeit des Rollenkonzepts konnten ebenfalls Importschnittstellen von OIA verwendet werden, um die real genutzten Berechtigungsinformationen zum Abgleich bereitzustellen und eine Beschreibung dazuzugeben. Als Ergebnis standen die zertifizierten Rollen für eine Zuweisung zu den Benutzern in der Organisation zur Verfügung.

Einmal über diese Prozesse validiert und dokumentiert, konnte das Rollenkonzept in die betriebliche Nutzung überführt werden. Im Falle des Finanzdienstleisters wurde die Rezertifizierung unter OIA als Prozess aufgesetzt, über den die Vorgesetzten dann die Zugehörigkeit der Mitarbeiter zur Organisation und ihre Nutzungsrechte zu Rollen überprüften, bestätigten oder zur Nachbearbeitung bereitstellten. Unter Nutzung von OIA konnte zudem automatisch der Fortschritt der Rezertifizierung verfolgt und vor allem dokumentiert werden. Am Ende wurden dann die Reports von OIA genutzt, um die Ergebnisse einer Revision zu präsentieren oder Überprüfungen zu veranlassen.

Gleichermaßen wurden diese Eigenschaften in der Umgebung des Versicherers eingesetzt. Dieser machte sich darüber hinaus zunutze, dass Schnittstellen zwischen OIA zu Oracle Waveset (OW) und Oracle Identity Manager (OIM) implementiert sind. Darüber wurden die unter OIA verwalteten Rollen mit dem Identity Management synchronisiert und dienten als Basis für das Antragsverfahren und der Provisionierung von Berechtigungen für ausgewählte Anwendungen.

Fazit

Eine verlässliche Verwaltung von Anwendungsberechtigungen kann in mittleren und größeren Organisationen oder in Organisationen mit hohen Anforderungen zur Rechte-Trennung und deren Nachweis nur auf Basis eines Rollenkonzepts dargestellt werden. Das bedingt, dass Identitäten, fachliche Rollen und Anwendungsberechtigungen systematisch in festen Beziehungen zu definieren sind.

Externe Beratung zur Methodik und zur Technologie kann die Bewältigung dieser Aufgabe wirkungsvoll unterstützen. Die unverzichtbaren Leistungsträger sind aber die Mitarbeiter der Organisation selbst, die mit ihrem Wissen um die fachlichen Anforderungen und die Anwendungen das Rollenkonzept aus der Taufe heben müssen.

Fach- und IT-Seite haben ein gemeinsames Verständnis zu Rollen und Berechtigungen zu erarbeiten, prüfen zunächst den Ist-Stand und dokumentieren diesen erstmals in einer gemeinsam verständlichen Form. Ab dann profitieren Management, Revision, Fachseite und IT-Verantwortliche gleichermaßen, wenn es zu Veränderungen innerhalb der Organisation, Identitäten, Geschäftsprozesse, Anwendungen oder Sicherheits-Richtlinien / -Vorschriften kommt. Zudem macht es das Rollenkonzept erst handhabbar, regelmäßig wiederkehrende Prüfungen in Form von Re-Zertifizierungen durchführen zu können und den Nachweis erbringen zu können, die Rechteverwaltung im Griff zu haben.

Rollenkonzepte bedingen die Zusammenführung vieler verschiedenartiger Informationen und deren Bereitstellung für vielfältige Prozesse und Auswertungen. Daher ist eine Technologie zu unterlegen, die Daten zu Rollenkonzepten aufnimmt, darstellt, anpassbar macht, Analysen und Reports unterstützt und Revisionsansprüchen genügt. Ansonsten sorgt eine lebende Organisation in kürzester Zeit dafür, dass auch das beste Rollenkonzept die Zukunftsperspektiven einer Eintagsfliege hat.

Norbert Drecker
TWINSEC GmbH
norbert.drecker@twinsec.de