S@PPORT

Entscheidungsgrundlagen für Auswahl, Installation und Betrieb von SAP*-Lösungen

AUSGABE 1-2_2011 | 7,50 EURO

ISSN 2190-118X

SAP-PROJEKTE: EINFÜHRUNG, MIGRATION UND RELEASEWECHSEL

KONSTANTE VERÄNDERUNG

Projekte im SAP-Umfeld gehören zu der Königsdisziplin in der IT-Welt. Zu der Komplexität der Projekte kommt eine Vielzahl unterschiedlicher Add-on-Lösungen und auch bei der Auswahl der Dienstleister gilt es sorgfältig abzuwägen.

SEITE 15

STELLENANZEIGEN AUF SEITE 55

Lückenlose und nachhaltige Prozesse für Benutzerrechte

Wer eine durchgängige Benutzerverwaltung (Identity-Management) einführt, will sicherlich eines erreichen: einen lückenlosen und nachhaltigen Beantragungs- und Genehmigungsprozess für Benutzerrechte. Die Notwendigkeit, den Fachbereich dabei verantwortlich einzubeziehen und entscheiden zu lassen, ist heute in den wenigsten Fällen schon gelebte Praxis. Wie komme ich diesem Compliance-Ziel näher?

Abb. 1: Grundsätze und Einflüsse beim Berechtigungsdesign der Benutzerverwaltung

*Von Rolf-Udo Gilbert**

Grundlage für den Einbezug des Fachbereichs in verantwortlicher Rolle ist ein transparentes, funktionsorientiertes und durchgängig strukturiertes SAP-Berechtigungskonzept mit klar definierten Arbeitsplatzfunktionen. Das Berechtigungsdesign beeinflusst viele Themenbereiche – wesentlich auch die Benutzerverwaltung.

Wie kann ich einerseits die Verantwortungsübernahme des Fachbereichs und andererseits auch eine Arbeitserleichterung für die IT-Basis erreichen? Sieben Aspekte lassen sich als Anforderung für das Berechtigungsdesign ableiten:

- Richtige Einführungsreihenfolge der IT-Komponenten
- Transparenz durch durchgängige Namensvergabe der Rollen
- Rechteauswahl für die Beantragung
- Data-Owner-Prinzip für alle Rechte
- Hierarchie der Rollen
- Mitarbeit des Fachbereichs
- Risikoanalyse und Compliance

Wie bereits im S@PPORT-Supplement „SAP & Sicherheit" (10-2010) auf Seite 8 ff. beschrieben, darf man das Pferd nicht von hinten aufzäumen. Wenn die Berechtigungseinstellungen über Jahre gewachsen und die in Abb. 1 genannten fünf Grundsätze (im gelben Pfeil der Abbildung) nicht mehr erfüllbar sind, ist ein Redesign der Rollen vor Einführung eines IdM unabdingbar. Die Testphase für die Rollen kann bereits auch als Test für die Beantragung und Genehmigung der Test-User-Rechte dienen; damit verringert sich die Einführungszeit des IdM.

** Rolf-Udo Gilbert ist Geschäftsführer der consonoIT und Mitglied im BMON-Verbund. Er beschäftigt sich seit vielen Jahren mit Anwendungssicherheit in SAP-Systemen und unterstützt bei Auswahl und Einführung von Sicherheitslösungen. Er ist Mitautor des neuen „Best-Practice-Leitfaden zur Einführung der SAP BusinessObjects GRC-Lösungen" der DSAG. Dieser Leitfaden ist zu finden unter: http://www.dsag.de/fileadmin/media/Leitfaeden/100602_Leitfaden_SAP_BO_ACBP_screen.pdf*

Namensvergabe – ein zentraler Punkt

Die Namensvergabe der SAP-Rollen ist ein zentraler Punkt für Transparenz und Verständnis. Der Kurzname einer SAP-Rolle reicht stellenmäßig nicht aus, die betriebliche Funktion (wie z. B. „Debitorenstammdaten", „Mahnwesen"), den Funktionstyp wie „Bearbeiten" oder „Anzeigen" und die organisatorischen Einheiten transparent widerzuspiegeln; dies erreicht man nur über den Langnamen mit seinen maximal 81 Zeichen und auch nur dann, wenn dieser einheitlich aufgebaut ist. Der Fachbereich muss aus dem Rollenangebot zur Beantragung eines zusätzlichen Rechtes für einen Mitarbeiter die richtige Rolle auswählen können. Auch für einen „Nicht-ITler" heißt dies: eindeutige und aussagefähige Rollen werden benötigt. Diese „Trivialität" benötigt jedoch einen Automatismus, um die Durchgängigkeit der Namensvergabe auch bei Rollenänderung in den Griff zu bekommen.

Darüber hinaus dürfen auch nur die Arbeitsplatzfunktionen zur Auswahl angezeigt werden, die der User für sich oder einen Mitarbeiter beantragen kann. Aus einer Menge von 50 und mehr auszuwählen, wird keine Akzeptanz finden und erschwert es auch dem Vorgesetzten, den Antrag zu genehmigen. Über den Rollennamen muss ein Filter gelegt werden können, um die Untermenge pro Fachbereich klar ableiten zu können.

Eigentümer einer Rolle ist immer der jeweilige Fachbereich – nicht die IT (außer Basisfunktionalität). Beantragt ein User fachübergreifend ein Recht, muss der Workflow den Data-Owner erkennen können und abfragen, ob er diesem Antrag zustimmt. Wenn jeder Rollenname z. B. mit einem Modulkürzel beginnt und pro Modul oder Bereich (ORG-Einheit) ein Verantwortlicher definiert ist, funktioniert diese Steuerung. Die IT kann unmöglich

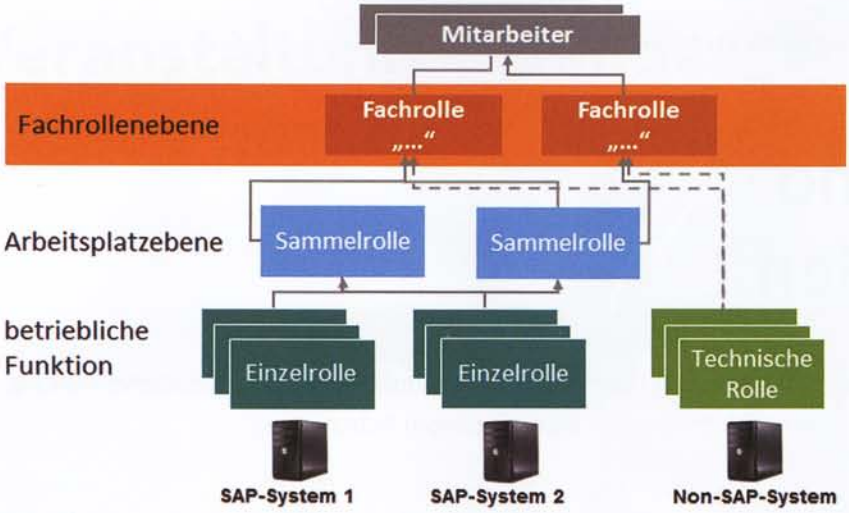

Abb. 2: Aufbau von Fachrollen

entscheiden, wer welche Rechte bekommen soll – außer ihren eigenen.

Neue Ebene der Rechtehierarchie

Mit dem IdM wird eine neue Ebene in der Rechtehierarchie eingeführt: die Fachrolle oder Businessrolle. Wir kennen vom „SAP ERP" Einzel- und Sammelrollen; die Fachrolle innerhalb des IdM kann weitere Rechte gruppieren und ergänzt diese mit Privilegien bzw. technischen Rollen (Non-SAP-Rechte). Wenn hier nicht im Vorfeld entschieden wird, wie eine Fachrolle aufgebaut werden soll, entsteht Wildwuchs und eine völlige Intransparenz. Fachrollen können z. B. eine Stelle beschreiben (in Verbindung mit HR-ORG) oder projektspezifischen Aufgabenbereichen entsprechen und auch untereinander in eine Hierarchie gesetzt werden. Eine mögliche Empfehlung sieht wie in Abb. 2 gezeigt aus. Eine von mehreren Möglichkeiten aggregiert im SAP-System Einzelrollen zu Sammelrollen und nur diese werden dem IdM bekannt gemacht (Synchronisierung). Die Sammelrolle (betriebswirtschaftliche Funktion) wird im IdM mit Zugriffsrechten zu LDAP-Verzeichnissen oder Exchange-Accounts bzw. Fremdsystemen ergänzt. Nur diese Fachrollen werden dem User dann zugewiesen.

Die Rollen (Funktionen sowie die Arbeitsplätze) werden mit dem Ansprechpartner des Fachbereichs besprochen und abgestimmt. Hierzu gibt es Vorgehensweisen, Tools und vorgefertigte Bausteine, um es für den Fachbereichsmitarbeiter verständlich zu machen – mit Transaktionen und Berechtigungsobjekten ist dieser zumeist überfordert. Die Umsetzung ist IT-Aufgabe. Die Werkzeuge können zusätzlich das Projekt beschleunigen, den Arbeitsaufwand drastisch reduzieren und eine hohe Qualität sicherstellen. Wird der Fachbereich jedoch nicht mit eingebunden, wird er niemals das Data-Owner-Prinzip leben und auch keine Änderungsvorschläge unterbreiten.

Sicherheit als oberstes Prinzip

Für viele ein neues Thema kommt durch die Vorschriften des seit 2009 gültigen BilMoG – Bilanzrechtsmodernisierungsgesetz (dort: SOD, Funktionstrennung); Funktionstrennung besagt, dass keine kritischen Rechtekombinationen bei einem Mitarbeiter zusammentreffen sollen. Wenn nun bereits Einzelrollen solche kritischen Funktionspaare beinhalten, wie soll dann auf Arbeitsplatz- und User-Ebene Funktionstrennung möglich sein? Daher gilt die eiserne Regel, Einzelrollen so zu bauen, dass diese „sicher" sind; bei Arbeitsplätzen (Sammelrollen) lässt sich das nicht immer durchhalten, da Key-User oder Vertreterregelungen oftmals eine Rechtehäufung bedingen. Dann müssen diese Risiken durch kompensierende Kontrollen reduziert werden. Wer eine automatisierte Risikoanalyse zeitnah durchführen kann, erkennt das Risiko und handelt dementsprechend.

Sicherlich gilt es beim Design von Rechtesystemen weitere wichtige Aspekte zu beachten; die hier dargestellten schaffen Akzeptanz im Fachbereich und ermöglichen, Verantwortung von der IT in den Fachbereich zu verlagern. Dies ist ein kontinuierlicher Weg, auf dem die IT die Verantwortlichen des Fachbereichs mitnehmen muss – eventuell auch unter Mithilfe der internen Revision. Das Ergebnis einer dann erfolgreichen IdM-Einführung in Verbindung mit sicheren und transparenten Rollen wird belohnt durch Aufwandsreduzierung, einfachere Administration und Nachvollziehbarkeit. *(ap)* @