Dipl.-Betriebswirt Christoph Wildensee, CISM

Funktionsübernahme in Personalunion – Rollenkollision in SAP®

Inhalt

1 Die Problematik
2 Die Analyse

1. Die Problematik

1.1 Einleitung

Bei der Einführung von SAP® im Unternehmen werden Arbeitsplätze definiert, die sich üblicherweise an den Aufgaben der Mitarbeiter in den Fachbereichen orientieren. Sie beinhalten alle notwendigen Transaktionen und Berechtigungsobjekteingrenzungen für die Aufgabenwahrnehmung.

Hinzu kommen Add-On-Rollen, um spezifische Anforderungen abzudecken, die dadurch entstehen, dass einzelne Personen neben der Funktionsausübung des Standard-Arbeitsplatzes noch weitere Aufgaben wahrnehmen. Dies können bestimmte Key-User- oder koordinierende Aufgaben sein, aber auch als kritisch im Unternehmen definierte Funktionen, die aus der Standard-Rolle herausgenommen wurden und nur ausgesuchten Personen zugebilligt werden, die als Funktionsträger ein besonderes Maß der Verantwortung tragen. Entsprechend sollten die Rollen nach dem Grundsatz „So wenig Berechtigungen wie möglich, so umfangreiche Berechtigungen wie nötig!“ ausgestaltet sein.

Die Vorgehensweise der Berechtigungsdefinition selbst kann jedoch mit innerbetrieblichen Ressourcenzuweisungen kollidieren. Es ist häufig zu erkennen, dass die SAP-Administration, speziell die der Berechtigungsadministration, stark unterbesetzt ist und sich um alle Systeme kümmern muss. Dies schließt nicht nur eine verteilte SAP-Landschaft ein, sondern auch Trennungen nach Produktion, Test/Integration, Qualitätssicherung und Entwicklung, die gleichermaßen Anforderungen an die Administration stellen.

Es ist nachvollziehbar, dass die Berechtigungsadministration versucht, zur Entlastung im Tagesgeschäft Vereinfachungen in der Berechtigungsdefinition vorzunehmen. Dies sind üblicherweise:

- Eine neue Funktionszuweisung zu einer Rolle wird über den Profilgenerator als Kleinstprofil hinzugefügt. Es wird nicht überprüft, ob an anderer Stelle / in anderen Rollen ein solches Profil bereits existiert, das dann der anzupassenden Rolle ebenfalls zugewiesen werden kann. Man findet solche Kleinstprofile mehrfach vor, so dass die zu verwaltenden Objekte der Organisation aufgebläht werden. Kleinstprofile haben zumeist eine oder nur wenige Transaktion(en) und eine oder wenige Berechtigungsobjektausprägung(en).
- Sofern beispielsweise neue Buchungskreise hinzukommen und Rollen hierfür erweitert werden, werden keine abgestimmten Kontrollen / Quer-Checks durchgeführt, sondern die Rollen vollständig um den oder die neuen Buchungskreis(e) oder andere organisatorische Eingrenzungen erweitert.
- Teilweise werden Arbeitsplätze aus Vereinfachungsgründen in der Form gebildet, dass beispielsweise eine Sachbearbeiterrolle (SB) gebündelt definiert wird. Mehrere Sachbearbeiter sollen also eine identische Aufgabe übernehmen, aber beispielsweise jeder für eine andere Gesellschaft. Es wird aber lediglich eine Rolle gebildet mit einer Buchungskreiseingrenzung für alle hier bearbeiteten Gesellschafts-Buchungskreise. Dies führt dazu, dass alle Personen, die die Rolle erhalten, in allen Buchungskreisen vollumfängliche SB-Rechte erhalten. So wird die Menge der zu verwaltenden Rollen reduziert auf Kosten der Sicherheit und Ordnungsmäßigkeit. Nachgelagerte Kontrollen durch z. B. Vorgesetzte sollen korrigierend wirken, was dann selten tatsächlich im Detail erfolgt.
- Eine Vielzahl von Berechtigungen könnte in den zugehörigen Berechtigungsobjekten eine Eingrenzung erhalten, aber auch dies wird häufig unterlassen. Die stärksten Eingrenzungen erfolgen auf der organisatorischen Ebene über Mandant, Buchungskreis u. Ä., bereits wesentlich seltener über Berechtigungsgruppen, die meisten Berechtigungsobjekte werden aber mit einer Generalberechtigung ausgeprägt (‚*'). Dies reduziert zwar wiederum – eine Generaleingrenzung führt zunächst zu keiner regelmäßigen administrativen Anpassungsnotwendigkeit über Change-Requests – die Anzahl der zu verwaltenden Objekte und entlastet somit die Berechtigungsadministration, dies birgt aber auch das Risiko, dass kumulierende Berechtigungen entstehen. Beispiele für häufig auftretende Generalberechtigungen in SB-Rollen im Bereich FI sind die Berechtigungsobjekte F_BKPF_BLA, F_BKPF_BUP, F_BKPF_GSB, F_BKPF_VW, F_BNKA_MAN, F_REGU_KOA. Eingrenzungen erfolgen dann lediglich in den Objekten F_BKPF_BUK, F_BNKA_BUK, F_REGU_BUK und F_SKA1_BUK.

Charakteristisch ist also eine insgesamt relativ niedrige Anzahl an Rollendefinitionen (zur vereinfachten Rollenzuweisung in den Fachbereichen) bei einer hohen Anzahl von Einzelprofilen und Generalberechtigungen in einer größeren Anzahl von Berechtigungsobjekten in den SB-Rollen – überwiegend dienen Transaktionen als Funktionseingrenzung. Die Darstellung erhebt natürlich keinen Anspruch auf Vollständigkeit, zeigt aber zumindest die Grundprobleme der SAP-Administration, die häufig anzutreffen sind.

F_BKPF_BLA	Buchhaltungsbeleg: Berechtigung für Belegarten
F_BKPF_BUP	Buchhaltungsbeleg: Berechtigung für Buchungsperioden
F_BKPF_GSB	Buchhaltungsbeleg: Berechtigung für Geschäftsbereiche
F_BKPF_VW	Buchhaltungsbeleg: Vorschlagswerte Belegart / BSchl ändern / anzeigen
F_BKPF_KOA	Buchhaltungsbeleg: Berechtigung für Kontoarten
F_BKPF_BUK	Buchhaltungsbeleg: Berechtigung für Buchungskreise
F_BNKA_MAN	Banken: Generelle Pflegeberechtigung
F_BNKA_BUK	Banken: Berechtigung für Buchungskreise
F_SKA1_BUK	Sachkonto: Berechtigung für Buchungskreise
F_SKA1_KTP	Sachkonto: Berechtigung für Kontenpläne
F_SKA1_AEN	Sachkonto: Änderungsberechtigung für bestimmte Felder
F_LFA1_BUK	Kreditor: Berechtigung für Buchungskreise
F_LFA1_GEN	Kreditor: Zentrale Daten
F_LFA1_APP	Kreditor: Anwendungsberechtigung
F_LFA1_GRP	Kreditor: Kontengruppenberechtigung
F_LFA1_AEN	Kreditor: Änderungsberechtigung für bestimmte Felder
F_REGU_BUK	Automatische Zahlung: Aktionsberechtigung für Buchungskreise
F_REGU_KOA	Automatische Zahlung: Aktionsberechtigung für Kontoarten usw.

Tab. 1: Maßgebliche FI-Berechtigungsobjekte

1.2 Grundlagen

Der Zugang zu SAP-Funktionalitäten erfolgt geregelt über die Zuweisung von Transaktionscodes, die den Zugang an sich bedeuten, und die Zuweisung von Berechtigungsobjekten, die je nach Ausprägung ihrer Steuerungsfelder die Information selbst determinieren und die Art des Zugriffs auf diese Information. Transaktionen sind ABAP-Programme. Ein Programm kann hier mehrere Transaktionen abarbeiten, d. h., der Aufruf von Transaktionen kann dazu führen, dass ein und dasselbe Programm abläuft, es steuert lediglich den unterschiedlichen Zugriff auf die Information und den Manipulationsgrad (z. B. über unterschiedliche Dynpros, Ein- und Ausblenden von Informationsblöcken). Eines der interessantesten Beispiele für ein solches Vorgehen ist das Einstiegsprogramm SAPMF05A. Es steuert nicht nur die Belegbuchungstransaktion FB01, sondern insgesamt über 100 Transaktionen – die meisten davon sind manipulierender Art (Erfassen, Buchen, Stornieren, Auflösen etc.).

TCODE	Dynpronr	Text	TCODE	Dynpronr	Text
F-01	100	Musterbeleg erfassen	F-35	101	Forfaitierung buchen
F-02	100	Sachkontenbuchung erfassen	F-36	122	Wechselzahlung
F-03	131	Ausgleichen Sachkonto	F-37	113	Anzahlungsanforderung Debitor
F-04	122	Verrechnung auflösen	F-38	109	Statistische Buchung erfassen
F-05	100	Fremdwährungsbewertung buchen	F-39	115	Debitorenanzahlung auflösen
F-06	103	Zahlungseingang buchen	F-40	122	Wechselzahlung
F-07	103	Zahlungsausgang buchen	F-41	100	Kreditoren Gutschr. erfassen
F-19	116	Statistische Buchung zurücknehmen	F-42	100	Umbuchung erfassen
F-20	102	Wechselobligo zurücknehmen	F-43	100	Kreditoren Rechnung erfassen
F-21	100	Umbuchung erfassen	F-44	131	Ausgleichen Kreditor
F-22	100	Debitoren Rechnung erfassen	F-47	112	Anzahlungsanforderung
F-25	116	Umkehrwechsel auflösen	F-48	110	Kreditorenanzahlung buchen
F-26	123	Schnellerfassung Zahlungseingang	F-49	108	Debitorischer Merkposten
F-27	100	Debitoren Gutschrift erfassen	F-51	122	Umbuchen und Ausgleichen
F-29	111	Debitorenanzahlung buchen	F-52	103	Zahlungseingang buchen
F-30	122	Umbuchen und Ausgleichen	F-53	103	Zahlungsausgang buchen
F-31	103	Zahlungsausgang buchen	F-54	114	Kreditorenanzahlung auflösen
F-32	131	Ausgleichen Debitor	F-55	109	Statistische Buchung erfassen
F-33	101	Wechselverwendung buchen	F-56	116	Statistische Buchung zurücknehmen
F-34	101	Inkasso buchen	F-57	108	Kreditorischer Merkposten
F-90	100	Anlagenzugang d. Kauf m. Kreditor	FB50	1099	Sachkontenbuchung Einbildtransaktion
F-91	122	Anlagenzugang a. Verrechnungskonto	FB60	1099	Erfassung eingehender Rechnungen
F-92	100	Anlagenabgang d. Verkauf m. Debitor	FB65	1099	Erfassung eingehender Gutschriften
FB01	100	Beleg buchen	FB70	1099	Erfassung ausgehender Rechnungen
FB05	122	Buchen mit Ausgleichen	FB75	1099	Erfassung ausgehender Gutschriften
FBR2	104	Beleg buchen	FBA1	113	Anzahlungsanforderung Debitor
FB08	105	Beleg stornieren	FBA2	111	Debitorenanzahlung buchen
FB10	126	Re/Gu Schnellerfassung	FBA3	115	Debitorenanzahlung auflösen
FB11	107	Gemerkten Beleg buchen	FBA6	112	Anzahlungsanforderung Kreditor
FB1D	131	Ausgleichen Debitor	FBA7	110	Kreditorenanzahlung buchen
und weitere					

Abb.1: Beispieltransaktionen Programm SAPMF05A (Tabelle TSTC)

Soll eine der dargestellten Transaktionen (hier aus dem Bereich FI) beim Aufruf entsprechende Ergebnisse offerieren, werden für die korrekte Abarbeitung zunächst der Transaktionscode und die Ausprägung der benötigten Berechtigungsobjekte im Benutzerstammsatz abgefragt. Ausgangspunkt ist die Tabelle USOBT (Relation Transaktion => Berechtigungsobjekt). In dieser kann abgelesen werden, welche Berechtigungsobjekte in welcher Ausprägung benötigt werden, um die Funktion auszuüben.

Name	Typ Prüfkennzeichen	Objekt	Feldname	Wert	Wert
F-31	TR	F_BKPF_BUK	ACTVT	01	
F-31	TR	F_BKPF_BUK	BUKRS	$BUKRS	
F-31	TR	F_BKPF_GSB	ACTVT		
F-31	TR	F_BKPF_GSB	GSBER	$GSBER	
F-31	TR	F_BKPF_KOA	ACTVT	01	
F-31	TR	F_BKPF_KOA	KOART	$KOART	
F-31	TR	F_SKA1_BUK	ACTVT		
F-31	TR	F_SKA1_BUK	BUKRS	$BUKRS	

Abb. 2: Tabelle USOBT für Transaktion F-31 (Zahlungsausgang buchen)

Wenn nun einige der Berechtigungsobjekte im Benutzerstammsatz aus dem oben genannten Grund der Administrationsvereinfachung üblicherweise mit Generalausprägung vorliegen und beispielsweise lediglich zwei der benötigten Berechtigungsobjekte im Detail ausgeprägt werden, entsteht hier sehr schnell die Gefahr einer übergeordneten Berechtigung.

Insbesondere der Einblick in den Ablauf der jeweiligen Berechtigungsobjektsteuerung (und ggf. sogar bereits die PAI- und PBO-Prozesse [Process after Input / Process before Output]) ist / sind von Belang. Häufig werden nach Aufruf der Transaktion die Rahmendaten nahezu vollständig strukturiert bereitgestellt und lediglich der letzte Schritt der Funktion (z. B. Anlegen oder Buchen) wird bei Fehlen der Berechtigungsobjektausprägung nicht vollzogen. Es ist für die Prüfung von Bedeutung, in welcher Struktur die Abarbeitung erfolgt, d. h. zu welchem Zeitpunkt Überprüfungen stattfinden. Die Berechtigungsobjektsteuerung erfolgt teilweise nicht unbedingt (vollständig) zu Beginn der Verarbeitung, sondern nicht selten erst sehr spät oder zumindest abgestuft innerhalb der Transaktionsverarbeitung.

1.3 Konsequenz dieses Ansatzes bei der Vergabe von zwei oder mehreren Rollen

Nehmen wir an, dass ein Benutzerstammsatz zwei Rollen aus dem Modul FI erhält. Rolle 1 beinhaltet eine nahezu vollumfängliche Berechtigung für eine spezielle Beteiligung, Buchungskreis 1500. Gebündelt sind hier alle Berechtigungsobjekte des FI-Bereiches mit Generalausprägung (‚*') in den Steuerungsfeldern mit lediglich einer Einschränkung der Berechtigungsobjekte, in denen der Buchungskreis als Steuerungsfeld vorkommt.
Im Detail z. B. wie folgt:

Rolle 1:

F_BKPF_BUK	ACTVT	Aktivität	*
	BUKRS	Buchungskreis	1500
F_BKPF_BUP	BRGRU	Berechtigungsgruppe	*
F_BKPF_BLA	ACTVT	Aktivität	*
	BRGRU	Berechtigungsgruppe	*
F_BKPF_GSB	ACTVT	Aktivität	*
	GSBER	Geschäftsbereich	*
F_BKPF_KOA	ACTVT	Aktivität	*
	KOART	Kontoart	*
F_BKPF_VW	ACTVT	Aktivität	*
F_BL_BANK	ACTVT	Aktivität	*
	BUKRS	Buchungskreis	1500
	HBKID	Kurzschlüssel Hausbank	*
	HKTID	Kurzschlüssel Kontenverbindung	*
	ZLSCH	Zahlweg	*
F_BNKA_BUK	ACTVT	Aktivität	*
	BUKRS	Buchungskreis	1500
F_BNKA_MAN	ACTVT	Aktivität	*
F_SKA1_BUK	ACTVT	Aktivität	*
	BUKRS	Buchungskreis	1500
S_TCODE	TCD	Transaktionscode	F*

... und weitere Berechtigungsobjekteingrenzungen.

Selbst wenn in der Praxis doch eher selten eine Transaktionsberechtigung F* vorkommt, soll dies an dieser Stelle lediglich darlegen, dass Sachbearbeiterrollen existieren können, die – ggf. auch über dezidierte Nennung der zugelassenen Transaktionscodes – nahezu vollumfängliche oder zumindest weit gefasste Berechtigungen in einem Modul, hier FI, bieten.

Rolle 2 soll wiederum für das Stammhaus, Buchungskreis 1000, lediglich wenige ändernde und überwiegend anzeigende Berechtigungen beinhalten. Selbst wenn aber nur wenige ändernde Berechtigungen aus dem FI-Bereich vergeben wurden, kann es analog Abbildung 2 vorkommen, dass die hier als wesentlich zu erkennenden Berechtigungsobjekte mit Buchungskreiseingrenzung ebenfalls mit Generalberechtigung oder zumindest mit expliziter Stammhauskennung und mindestens einem hohen Manipulationsgrad (01 oder 02) auftreten.

Im Detail z. B. wie folgt:

Rolle 2:

F_BKPF_BUK	ACTVT	Aktivität	* (Delta-Objekt mit ‚*' oder ggf. 01/02)
	BUKRS	Buchungskreis	1000
F_BKPF_BUP	BRGRU	Berechtigungsgruppe	*
F_BKPF_BLA	ACTVT	Aktivität	01
	BRGRU	Berechtigungsgruppe	*
F_BKPF_GSB	ACTVT	Aktivität	01
	GSBER	Geschäftsbereich	*
F_BKPF_KOA	ACTVT	Aktivität	01, 02, 03, 77
	KOART	Kontoart	K, M, S
F_BKPF_VW	ACTVT	Aktivität	03
F_BL_BANK	ACTVT	Aktivität	* (Delta-Objekt mit ‚*')
	BUKRS	Buchungskreis	1000
	HBKID	Kurzschlüssel Hausbank	*
	HKTID	Kurzschlüssel Kontenverbindung	*
	ZLSCH	Zahlweg	*
F_BNKA_BUK	ACTVT	Aktivität	* (Delta-Objekt mit ‚*')
	BUKRS	Buchungskreis	1000
F_BNKA_MAN	ACTVT	Aktivität	03
F_SKA1_BUK	ACTVT	Aktivität	01 (Delta-Objekt mit ‚*' oder ggf. 01/02)
	BUKRS	Buchungskreis	1000
S_TCODE	TCD	Transaktionscode	FB03 (Beleg anzeigen) AB01 (Anlagenbeweg. erfassen) AB08 (Anlagen-EP stornieren) AIBU (Umbuchen AiB) F-03 (Ausgleichen Sachkonto)

... und weitere Berechtigungsobjekteingrenzungen.

Entscheidend ist hier also, dass die Rolle 2 eine Bündelung von wenigen Funktionen ist, aber trotzdem für den Buchungskreis 1000 die Berechtigungsobjekte mit Buchungskreiseingrenzung und Generalberechtigung in der Aktivität oder zumindest mit dezidierter Eingrenzung manipulierender Art vorhanden sind.

Werden beide Rollen gleichzeitig einem Benutzerstamm zugewiesen, führt dieser Stammsatz neben seiner Hauptaufgabe also in Personalunion eine zusätzliche Rolle aus, entsteht eine kumulierende Berechtigung in der Form, dass nun auch für den Buchungskreis 1000 (Stammhaus) alle FI-Berechtigungen der Rolle 1 zur Verfügung stehen (Transaktionen und ggf. fehlende Berechtigungsobjekte mit passender Eingrenzung). Dies bedeutet, dass SAP® nach Eingabe des Transaktionscodes, den es aus Rolle 1 (Beteiligung) bezieht, die Berechtigungsobjekte beider Rollen paart und somit für die Bearbeitung des Stammhauses die passenden Berechtigungsobjekteingrenzungen aus beiden Rollen erhält. Beispielsweise ist dem Stammsatz nun das Buchen einer Kreditorenrechnung über Transaktion FB60 auch im Buchungskreis 1000 möglich.

SAP trifft keine Unterscheidung, ob/dass sich eine Berechtigung (Transaktion oder Berechtigungsobjekteingrenzung) nur auf eine Rolle beziehen und nicht der zweiten Rolle zur Verfügung stehen soll. Die Berechtigung kommt zustande, sofern die Zusammensetzung der benötigten Berechtigungsobjekteingrenzungen incl. Transaktionscode aus dem gesamten Berechtigungsstammsatz vollständig ist – die höchste Kombinationsausprägung determiniert den Manipulationsgrad der jeweiligen organisatorischen Ebene (hier Buchungskreis Stammhaus).

Die Analyse der Rollenzuweisungen, d.h. die Verteilung der Rollen innerhalb der Fachbereiche (z.B. Verteilung der Rollen auf die Benutzerstammsätze; Tabelle AGR_USERS nach Bereinigung der Zuweisungen über abgelaufenes Enddatum), die Identifizierung kritischer Rollenkombinationen, weiterhin die Identifizierung der verantwortlichen Profile und hieraus abgeleitet die Festlegung, unter welchen Bedingungen diese Profile anderen Rollen ebenfalls zur Verfügung stehen dürfen bzw. welche Rollen auf keinen Fall miteinander gepaart werden können, weil sie Kombinationsverursacher darstellen, sind die wesentlichen Punkte.

1.4 Fazit

Die Definition von Rollen und die Abgrenzung der Fachbereichsaufgaben ist ein wesentlicher Schritt im Einsatzkonzept von SAP. Es kommt nicht unbedingt häufig vor, dass Rollen gepaart vergeben werden, üblicherweise gibt es lediglich Add-On-Rollen für spezielle Fachaufgaben, die eine gesonderte Funktionszuweisung notwendig machen. Erfolgt jedoch eine Paarung von vollständigen Fachbereichsrollen auf einem Benutzerstamm, kann dies zu erheblichen Funktionserweiterungen dieser Person führen – Erweiterungen, die weder gewollt noch per se erkannt werden.

Problematisch sind grundsätzlich zunächst alle Rollen, die eine Unterscheidung in der Abarbeitung nach Buchungskreisen vornehmen und einen großen Bearbeitungsumfang bieten. Wenn diese mit Rollen eines anderen Buchungskreises gepaart werden, wobei lediglich die buchungskreisgesteuerten Berechtigungsobjekte einen hohen Manipulationsgrad aufweisen müssen (also wenige manipulative Transaktionen bereitgestellt werden), ergibt sich fast automatisch eine kumulative Berechtigungserweiterung. Anders herum ist dies natürlich ebenso. Diesem grundsätzlichen Fehler des SAP kann nur begegnet werden, indem

- Rollen unterschiedlicher Buchungskreise getrennt voneinander vergeben werden, eine Paarung also ausgeschlossen ist (ggf. auch über den Aufbau von mehreren Benutzerkennungen für eine Person)
- der Transaktionsumfang eingeschränkt wird für z.B. Beteiligungen_SB
- es eine Trennung für die unterschiedlichen Buchungskreise in Sicht und Sachbearbeitung gibt
- die Sachbearbeitung von Beteiligungen nicht übergreifend gefasst und dann nur auf wenige Schultern verteilt und mit weiteren Funktionen des Stammhauses gepaart wird (z.B. eine Rollenbündelung Beteiligungen_SB mit vollumfänglichen FI-Berechtigungen für mehrere kleine Beteiligungen, Verteilung auf wenige Sachbearbeiter/-innen, die sich gegenseitig vertreten; wenige dieser Gruppe erhalten zusätzlich die Rolle Hauptbuch_SB oder Kreditoren_SB für das Stammhaus. Dies ist eine klassische Konstellation für kumulierende Berechtigungen).

Die Problemstellung ist für andere organisatorische Trennungen und auch für andere Module ebenfalls latent vorhanden, zieht jedoch gerade im FI-Bereich hinsichtlich der Ordnungsmäßigkeit (Kreditorensachbearbeitung, Sachkonten- und Rechnungsbearbeitung, Freigaben und Zahlungsströme etc.) weitreichende Kreise. Insofern kann eine Analyse der eigenen SAP-Umgebung – auch im Hinblick auf modulübergreifende Verursacher-Rollen (speziell z.B. auch in Kombination mit Berechtigungen aus dem Modul MM) – sehr wichtig sein und der Revisionsabteilung interessante Einblicke in die Rollen und die Aufgabenwahrnehmungen der Fachbereiche ermöglichen.

2. Die Analyse

2.1 Einleitung

Werden zwei oder mehrere Rollen in einem Stammsatz gepaart, ist es möglich, dass sich die Berechtigungen gegenseitig beeinflussen – es entstehen ggf. höherwertige, d.h. kumulierende Berechtigungen, die nicht gewollt und überblickt werden. SAP trifft keine Unterscheidung, dass sich eine Berechtigung nur auf eine Rolle beziehen, aber der anderen Rolle nicht zur Verfügung stehen soll. Sofern die Zusammensetzung der für den Transaktionsaufruf benötigten Berechtigungsobjekteingrenzungen aus dem gesamten Berechtigungsstammsatz vollständig gegeben ist, wird der Zugang gewährt. Die höchste Kombinationsausprägung determiniert den Aufruf der und den Manipulationsgrad auf die Information.

Für die Prüfung ist es unerlässlich, die Verursacher solcher Rollenkollisionen zu identifizieren. Grundsätzlich ergibt sich zum einen die Frage, welche Rollen und darin enthalten welche Profile ggf. kritische Kombinationen auf Berechtigungsobjektebene bereitstellen. Zum anderen muss sich am Ende hieraus ergeben, welche

Rollen auf keinen Fall mit anderen Rollen zu kombinieren sind, um weitestgehend gegenseitig höherwertig beeinflussende Berechtigungen auszuschließen.

2.2 Grundlagen und Vorgehen

Die Berechtigungsverwaltung in SAP ist ausgesprochen komplex und schwer zugänglich. Die unterste Ebene der Berechtigungszuweisung ist die Bündelung von Berechtigungsobjektausprägungen zu Berechtigungen. Diese Berechtigungen fügen sich zu Profilen zusammen. Die Ebene der Profile ist beispielsweise über den Report RSUSR002 (Benutzer nach komplexen Selektionskriterien) eine der zentralen Anlaufpunkte bei der Berechtigungsanalyse. Mehrere Profile werden ggf. zu Sammelprofilen zusammengefügt. In den Rollen finden sich die Profile/Sammelprofile wieder. Die mit Profilzuweisungen definierten Rollen stellen üblicherweise die Arbeitsplätze dar. Es ist weitverbreitet, dass eine Trennung zwischen Menü- und Modulrollen eingezogen wird, d.h. zwischen den Transaktionscodezuweisungen als eigenständigen Rollenkomplex und den Bündelungen der Berechtigungsobjektausprägungen als ebenfalls jeweils separate Sammlung. Die Rollen werden wiederum den Benutzern/Stammsätzen zugewiesen, so dass die Gesamtberechtigung zusammengesetzt wird. Aber auch direkte Profilzuweisungen zu Benutzerstämmen sind generell möglich.

Tabellenname	Bedeutung	Relevante Inhalte
AGR_1016	Name des Profils der Aktivitätsgruppe	Rolle, Profil
AGR_1016B	Name des Profils der Aktivitätsgruppe	Rolle, Profil, Text
AGR_1250	Berechtigungsdaten zur Aktivitätsgruppe	Rolle, Objekt, Berechtigung
AGR_1251	Berechtigungsdaten zur Aktivitätsgruppe	Rolle, Objekt, Berechtigung, Feldname, Wert (Von), Wert (Bis)
AGR_1252	Org.ebenen zu den Berechtigungen	Rolle, Org.ebene, Wert (Von), Wert (Bis)
AGR_AGRS	Rollen in Sammelrollen	Sammelrolle, Rolle
AGR_AGRS2	Definition (der jeweiligen) Rolle	(Sammel-)Rolle, Rolle
AGR_DEFINE	Definition Rollen	Rolle (Einzel- und Sammelrollen), Rolle (enthaltene Rollen aus Rolle)
AGR_PROF	Profilname zur Rolle	Rolle, Profil (Sammel- und Einzelprofil)
AGR_USERS	Zuweisung Rollen zu Benutzern	Rolle (Einzel- und Sammelrollen), Benutzer, Beginn- und Enddatum der Rollenzuweisung
TSTC	SAP-Transaktionscodes	Transaktion, Programm, Text/Bedeutung
USER_ADDR(S)	Benutzer nach Adressdaten	Benutzer, Name, Org.ebene, Funktion
USOBT	Relation Transaktion → Berechtigungsobjekt	Transaktion, Typ, Objekt, Feldname, Wert (Von), Wert (Bis)
USOBT_C	Relation Transaktion → Ber.objekt (Kunde)	Transaktion, Typ, Objekt, Feldname, Wert (Von), Wert (Bis)
USR02	Anmeldedaten der Benutzer	Anmeldedaten, Stammsatzgültigkeit
UST04	Benutzerstämme	Benutzer, Profil
UST12	Benutzerstamm – Berechtigungen	Objekt, Berechtigung, Feldname, Wert (Von), Wert (Bis)
UST10C	Benutzerstamm – Sammelprofile	(Sammel-)Profil, (Einzel-)Profil
UST10S	Benutzerstamm – Einzelprofile	(Einzel-)Profil, Objekt, Berechtigung

Tab. 1: Ausschnitt aus den relevanten Tabellen der Berechtigungsprüfung

Ganz bewusst wurde bei der hier vorliegenden Betrachtung die Kombinationsmöglichkeit von Rollen/Arbeitsplätzen im Bereich der Buchungskreise gewählt (siehe Teil 1: – Funktionsübernahmen in Personalunion – Rollenkollisionen in SAP®). Wenn zunächst davon auszugehen ist, dass die Kombination von Rollen auf Sachbearbeiterebene (SB) **innerhalb einer Organisation** (BUKRS) bewusst erfolgt, um beispielsweise einem Key-User mit hohem Kenntnisstand ggf. eine herausgehobene Funktion ggü. den Kolleginnen und

Kollegen einzuräumen, bekommt die Kombination **über organisatorische Grenzen hinweg** eine andere Schärfe. Wie oben erwähnt ist es möglich, dass sich Berechtigungen dahingehend auswirken, dass sich eine weitreichende Befugnis in einer Organisation auch auf die andere Organisation in Form einer Kumulation auswirkt – der Sachbearbeiter überträgt aus der eigentlich gewollt stark ausgeprägten Organisation (Rolle 1) Berechtigungsinhalte auf die schwach ausgeprägte Organisation (Rolle 2).

Für die Prüfung ist es zunächst also wichtig, kritische, d.h. für eine Kombination von Berechtigungen weitreichend berechtigte Verursacher zu ermitteln. Ziel muss es sein, die Ausgangsprofile zu identifizieren, die ihre Berechtigungen im Stammsatz weitergeben zu einer Höchstausprägung, d.h. die Identifizierung der auslösenden Profile ist der Beginn. Entsprechend sind die Profildefinitionen herauszufinden, die in einer untergeordneten Organisation stark ausgeprägte Transaktions- und Objektberechtigungen und in den nicht buchungskreisgesteuerten Objekten ein Höchstmaß an Ausprägung aufweisen. Diese Verursacherprofile beinhalten also in den Objekten, die das Feld Buchungskreis nicht als Steuerungsfeld aufweisen, weitestgehende Generalberechtigungen oder zumindest hohe Manipulationsgrade.

Sofern bereits Hinweise vorliegen, welche (Sammel-) Rollen ggf. problematisch sein können, z.B. über die Rollenkennzeichnung FI:SB_GESELLSCHAFT_A (für Sachbearbeitung Gesellschaft Vollzugriff [all]; Einsicht in die Tabelle AGR_DEFINE) oder die Anzahl der in bestimmten Rollen enthaltenen, kritischen FI-Transaktionscodes, kann über die Rollenanalyse, d.h. beispielsweise dem Herausgreifen einer konkreten Benutzerkennung, die diese Rolle zugewiesen bekommen hat, über den Report RSUSR002 geschaut werden, welche Rechte (Objektrechte und Transaktionsumfang) hier im Detail implementiert sind. Bei Einsichtnahme in den Berechtigungsstammsatz können hier die verursachenden Berechtigungen und Profile abgeleitet werden. Die Suche nach relevanten Transaktionen und ausgeprägten Berechtigungsobjekten analog Tabelle USOBT kann hier zu markanten Profiltreffern führen. Werden diese in das Feld Rolle der AGR_AGRS eingetragen, erhält man alle Rollen, die mit dieser Berechtigung ausgestattet sind. Auch die Tabelle USOBT_C ist einzubeziehen, da diese den tatsächlichen, im System gültigen Zustand widerspiegelt (über Transaktion SU24 ggf. kundenspezifische Anpassungen).

Weiterhin sind nun die Sachbearbeiterrollen des Stammhauses herauszufiltern, die in Kombination mit den zuvor genannten Rollen/Profilen kritische Kombinationen ergeben können. Auch hier kann zunächst über die Tabelle AGR_DEFINE erkannt werden, welche SB-Rollen des Stammhauses existieren, die ggf. in Kombination problematisch sein können. Wird auch hier dann über den Report RSUSR002 und konkreten Benutzerkennungen explizit nach ausgeprägten FI-Berechtigungsobjekten, die mit Bezug zum Buchungskreis des Stammhauses und einem hohen Manipulationsgrad in der Aktivität ausgestattet sind (F_BKPF_BUK, F_SKA1_BUK usw.), gesucht, sind hier bereits konkrete Kombinationsausschlüsse zu erkennen. Einzuplanen ist zusätzlich noch die Überprüfung der Einzelprofile in Sammelprofilen (Tabellen UST10S und UST10C) und die der Einzelrollen in Sammelrollen (Tabellen AGR_AGRS und AGR_AGRS2).

Liegen jedoch keine Hinweise zu möglichen Verursacherrollen/-profilen vor, ist die Analyse schwieriger.

Zunächst ist das organisatorische Umfeld zu ermitteln. Die Tabelle T001 gibt Aufschluss über die vorhandenen Buchungskreise. Anschließend erfolgt die Rollenüberprüfung über die Tabellen UST12 und AGR_1251. In der UST12 können zu den FI-Objekten alle Einträge eingesehen und mit Vorgabewerten eingeschränkt werden. Als Ergebnis erhält man Hinweise zu kritischen Berechtigungen. Die Tabelle UST12 wird aus den Informationen der Tabelle AGR_1251 automatisch generiert. Dies führt dazu, dass die beiden Tabellen inhaltlich grundsätzlich identisch sind bzw. sein sollten.

Trotzdem ist dieses Unterfangen nicht ganz so einfach, wie es zunächst klingt. Die Tabellen UST12 und AGR_1251 enthalten bei größeren Unternehmen und SAP-Classic-Systemen möglicherweise um 250 000 bis ggf. sogar weit über 500 000 Datensätze. Analysen sind in diesem Umfeld kaum über einfache Datenbankabfragen und Filterungshilfsmittel wie in MS-Access durchzuführen. IDEA und ACL können (auch unter Nutzung von Hilfsfeldern u.Ä.) bei der Identifizierung relevanter Berechtigungen, Profile und Rollen helfen; trotzdem bleibt meist die Notwendigkeit, die Hinweise durch Einsicht in konkrete Benutzerstammsätze zu verifizieren.

Die Untersuchungskriterien innerhalb der Berechtigungsanalyse sind also nochmals in Kürze dargestellt folgende:

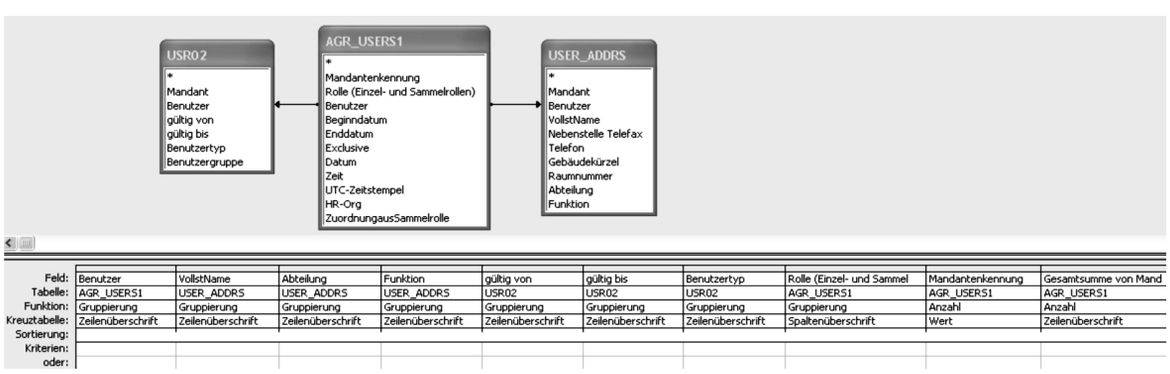
- Rollen mit einem weitreichenden FI-Transaktionsumfang in einer Sachbearbeiterrolle einer untergeordneten Gesellschaft, hier nahezu alle FI-Berechtigungsobjekte ohne Buchungskreissteuerung mit Generalausprägung, Berechtigungsobjekte mit Buchungskreissteuerung mit Eingrenzung des Buchungskreises der untergeordneten Gesellschaft → abgeleitete Verursacherprofile

- Rollen mit einem geringeren Umfang an FI-Transaktionen des Stammhauses, trotzdem durch wenige ändernde Transaktionszuweisungen auch Berechtigungsobjekte mit Buchungskreissteuerung mit einem Höchstmaß an Manipulationsgraden (Aktivität möglichst mit Generalausprägung oder zumindest mit 01, 02, 05, 06, 07, 76, 77 [Hinzufügen, Ändern, Sperren, Löschen, Erfassen usw.]), Objekte ohne Buchungskreissteuerung sind hier nicht wesentlich von Bedeutung
- Eine Kombination bedeutet, dass die Transaktionen und die Masse der Berechtigungsobjekte aus der Rolle der untergeordneten Gesellschaft geliefert werden und die Objekte mit Buchungskreissteuerung aus der Stammhausrolle, um nun auch die umfängliche Berechtigung der untergeordneten Gesellschaft auf das Stammhaus zu übertragen. Die Berechtigungsobjektausprägungen mit Buchungskreissteuerung aus der Stammhausrolle definieren dabei den tatsächlichen Manipulationsumfang.
- (Dies gilt auch bei einer Umkehrung der Buchungskreissteuerung innerhalb der Rollen.)

Das Aufspüren der Verursacherprofile bildet somit den Ausgangspunkt für die Identifizierung der Rollen und daraus folgend der Sammelrollen. Werden diese erkannt und zudem auch die Rollen und Sammelrollen, die für die zu begrenzende Organisation als SB-Arbeitsplätze nicht mit den Verursacherrollen/-sammelrollen kombiniert werden dürfen, ist zuletzt die Verteilung der Rollen auf die Benutzerstämme und die Ableitung des Handlungsrahmens (Überprüfung, ggf. Entziehen der Rollen) durchzuführen.

Dies ist möglich über die Tabelle AGR_USERS. Zunächst sind alle Einträge zu eliminieren, die ein Enddatum (befristete Rollenzuweisung) aufweisen, das nicht in unsere Betrachtung passt. Das Feld Enddatum sollte also möglichst einen weit in die Zukunft gerichteten Eintrag enthalten. Sollte hier beispielsweise zu einem Stammsatz ein Datum vorkommen, das in Kürze eintritt, ist an dieser Stelle zu entscheiden, wie mit einem solchen Eintrag umzugehen ist. Die Prüfung stellt üblicherweise einen Status quo fest, entsprechend ist auch ein solcher Inhalt relevant. Trotzdem kann zu diesen Stammsätzen ggf. am Ende eine Feststellung zum automatisierten Auslaufen der Berechtigung getroffen werden.

Die Tabelle kann über eine Kreuztabellenabfrage analysiert werden. Die Rollen werden in die Horizontale und die Benutzerkennungen in die Vertikale gesetzt. Es ist möglich, dass die Anzahl der Rollen zu groß ist für eine solche Analyse. Hier kann es sinnvoll sein, eine Bereinigung um bereits als unkritisch erkannte Rollen, z. B. aus anderen Modulen, vorzunehmen und nur die Rollen stehen zu lassen, die aus dem kritischen Bereich stammen, um die Anzahl der zu verarbeitenden Rollen in der Horizontalen möglichst gering zu halten. Das Ergebnis dieser Abfrage wird um die Inhalte der Tabelle USER_ADDR ergänzt; den Ergebnisinhalten der Verteilung werden also die Inhalte der USER_ADDR (bzw. USER_ADDRS; Name, KSt, Organisationszugehörigkeit, Funktion) und der Stammsatzgültigkeit aus Tabelle USR02 angehängt, um abgelaufene Benutzerstämme zu entfernen und für die verbleibenden Stammsätze eine funktionale Zuordnung herzuleiten. So können aufgrund der organisatorischen Ebene und Funktion Treffer bereits im Ansatz geklärt werden.



Feld:	Benutzer	VollstName	Abteilung	Funktion	gültig von	gültig bis	Benutzertyp	Rolle (Einzel- und Sammel	Mandantenkennung	Gesamtsumme von Mand
Tabelle:	AGR_USERS1	USER_ADDRS	USER_ADDRS	USER_ADDRS	USR02	USR02	USR02	AGR_USERS1	AGR_USERS1	AGR_USERS1
Funktion:	Gruppierung	Gruppierung	Gruppierung	Gruppierung	Gruppierung	Gruppierung	Gruppierung	Gruppierung	Anzahl	Anzahl
Kreuztabelle:	Zeilenüberschrift	Zeilenüberschrift	Zeilenüberschrift	Zeilenüberschrift	Zeilenüberschrift	Zeilenüberschrift	Zeilenüberschrift	Spaltenüberschrift	Wert	Zeilenüberschrift
Sortierung:										
Kriterien:										
oder:										

Abb. 1: Kreuztabellenabfrage der AGR_USERS mit ergänzenden Informationen nach Tabellenkorrektur in MS-Access

Die Verteilung beinhaltet in der Horizontalen alle Rollenzuweisungen mit entsprechender Trefferzahl in der Vertikalen, wo die Benutzerstammkennungen aufgeführt sind.

Benutzerkennung	Benutzername	Organisationseinheit	Gesamtsumme Rollenzuweisung	FI:AZUBI	FI:SB_GESELLSCHAFT_A	FI:BETRIEBSPRUEFUNG	FI:CONTROLLING	FI:DEBITOREN_SB	FI:HAUPTBUCH_SB	FI:KREDITOREN_SB	FI:STEUER	FI:WIRTSCHAFTSPRUEFUNG	...	Beurteilung / Vorschlag
...														
USR0001	Name 1	OE 1x	5		1			1	1	1				Zuweisung überprüfen
USR0002	Name 2	OE 1x	5		1			1	1					Zuweisung entfernen
USR0003	Name 3	OE 1x	3		1					1				Zuweisung entfernen
USR0004	Name 4	OE 1x	4		1				1					Zuweisung überprüfen
USR0005	Name 5	OE 1x	5		1				1					Zuweisung überprüfen
USR0006	Name 6	OE 1x	3		1				1					Zuweisung überprüfen
USR0007	Name 7	OE 1x	6		1			1	1					Zuweisung überprüfen
USR0008	Name 8	OE 1x	3		1				1					Zuweisung überprüfen
USR0009	Name 9	OE 1x	3		1									Zuweisung überprüfen
USR0010	Name 10	OE 1x	3		1		1	1						Zuweisung entfernen
USR0011	Name 11	OE 1x	4		1				1	1				Zuweisung entfernen
USR0012	Name 12	OE 1x	2		1					1				Zuweisung überprüfen
(Hinweis: Überprüfung oder Entfernung je nach Aufgabenstellung des Arbeitsplatzes !)														
...														

Abb. 2: Beispielverteilung der markanten Rollen

Die Verursacherrollen und die auszuschließenden Sachbearbeiterrollen werden markiert; entsprechend lässt sich ablesen, welche Kombinationen zu korrigieren sind. Jede Stammsatzkennung, die sowohl eine Zuweisung in der Verursacherrolle als auch in einer oder mehreren kritischen Sachbearbeiterrolle(n) aufweist, muss betrachtet und einer näheren Funktions- bzw. Zuweisungsanalyse unterzogen werden.

2.3 Fazit

Auch wenn zunächst davon auszugehen ist, dass die Wirkung der ungewollten Berechtigungserweiterung im Rahmen der Rollenkombination bei Aufgabenwahrnehmungen in Personalunion eher selten zu finden ist, sollte die Gefahrenquelle gerade im Bereich FI nicht unterschätzt werden. Möglicherweise ohne Limitstruktur und flankierende IKS-Maßnahmen können hier ggf. Zahlungsströme oder andere nicht im Unternehmensinteresse liegende Aktionen ausgelöst werden. Diese Punkte werden weder aus den Reihen der Fachbereiche noch auf der Ebene der Berechtigungsadministration beachtet. Eine Analyse und Hinweisgebung aus der Revision ist entsprechend sinnvoll.

Ausgesuchte Literatur

Beyer/Fischer/Jäck u.a.: SAP Berechtigungswesen – Design und Realisierung von Berechtigungskonzepten für SAP R/3 und SAP Enterprise Portal, SAP Press/Galileo Press, Bonn, 2003.

Thomas Tiede, SAP R/3 Ordnungsmäßigkeit und Prüfung des SAP-Systems (OPSAP), 2. Auflage, Ottokar-Schreiber-Verlag, Hamburg, http://www.osv-hamburg.de.

Christoph Wildensee, Ausgesuchte Berechtigungsobjekte des SAP R/3-Systems als Prüfungsansatz für die IV-Revision – Eine Übersicht – Teil 1 bis 3 für Basis, FI & CO; Das SAP R/3 IS-U-Berechtigungskonzept – Versorgungswirtschaft; Externer Zugriff auf SAP R/3-Systeme über RFC etc., ReVision III/2001ff, Ottokar-Schreiber-Verlag, Hamburg, http://www.osv-hamburg.de; http://www.auditplan-xp.de/veroeff.html.

Alexander Stendal, Risiken im SAP-Berechtigungssystem erkennen und beseitigen, Zeitschrift Interne Revision (ZIR) 1/2009, S. 18–19.

Dipl.-Betriebswirt **Christoph Wildensee**, CISM, ist seit 1994 als IV-Revisor bei der Stadtwerke Hannover AG (enercity), einem großen kommunalen Energiedienstleister mit ca. 2 500 Beschäftigten und mehr als 2 Mrd. EUR Umsatz, tätig und verfügt somit über eine langjährige Erfahrung im Bereich der Revision. Er arbeitete 2001 und 2002 projektbezogen auch für die IBS-Gruppe aus Hamburg in der SAP-Beratung und ist Verfasser verschiedener Fachartikel – insbesondere zum Thema SAP®-Prüfung. Seit 2008 ist er in Personalunion auch Datenschutzbeauftragter der Stadtwerke Hannover AG und mehrerer Beteiligungen. Mehr zu ihm: http://www.auditplan-xp.de/leben.html.