Analyse der Einkaufsbestellberechtigungen in SAP ERP

Dipl.-Betriebswirt Christoph Wildensee, DBA, CISM, CRISC, ist IV-Revisor bei der Stadtwerke Hannover AG.

Einleitung

Häufig wird unterstellt, dass bei der Analyse von Werteflüssen die höchste Priorität in den monetären Abflüssen aus dem Unternehmen und in der korrekten Allokation zu Kostenstellen und Aufträgen liegt. Die Interne Revision analysiert entsprechend mit besonderem Augenmerk und Prioritätsvorgabe durch die Geschäftsführung z.B. neben stichprobenartigen, geclusterten Betrachtungen der getätigten Finanzmittelabgänge, der korrekten Verbuchung und der IKS-Definitionen im Finanz- und Rechnungswesen auch das Berechtigungskonzept und die -vergabe neuralgischer Berechtigungen besonders im (ehemals FI und CO) „Financial Accounting“ und „Management Accounting“. [1] Schon die IKS-Definitionen der Fachbereiche fokussieren nicht selten auf die weitgehend isolierte Betrachtung dieser Funktionen und lösen nicht immer den prozessualen Integrationsgedanken. Über Jahre gesehen ist der „Procure-to-Pay Business Process“ mit Teilen des ehemaligen MM – in der Procure-Auslöserfunktion oft stiefmütterlich behandelt – nicht unwesentlich, kann doch hier der Beginn der Werteflüsse und der im finalen Schritt abfließenden Finanzmittel ausgemacht werden. Fehler an der Stelle in der Vergabe von Anlage- und Änderungsberechtigungen können gravierende Folgen nach sich ziehen. Ausreißer, d.h. Eigenmächtigkeiten im Bestellprozess durch auslösende Fachbereiche, werden ggf. spät oder auch nie entdeckt. [2]

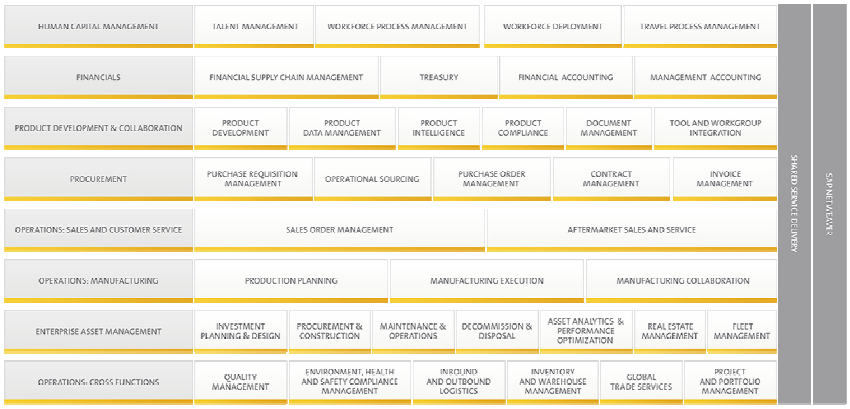

Abb. 1: Grundaufbau von SAP ERP. [3]

„Geschäftsprozesse werden modulübergreifend im SAP ERP-System abgebildet. Werteflüsse finden daher nicht in einem Modul statt, sondern ziehen sich, je nach Geschäftsprozess, über n Module.“ [4] Die Zusammengehörigkeit in der Betrachtung von Beschaffung, Materialfluss und Bezahlung ist offensichtlich, die modulunabhängige Betrachtung nachvollziehbar. [5] „Integrierte Werteflüsse bezeichnet die Wertschöpfung, die durch eine möglichst automatisierte Verknüpfung verschiedener Unternehmensbereiche erfolgt. In den Werteflüssen müssen unterschiedliche Quellen miteinander verbunden sein. […] Unter Materialfluss versteht man physische Warenbewegungen jeglicher Art, die Beschaffung oder die Gewinnung von Materialien sowie die Lagerhaltung, Verarbeitung und Auslieferung von Erzeugnissen.“ [6] „Mit der Bestellung wird mit einem Lieferanten eine Vereinbarung getroffen, die in der Bestellung beschriebenen Waren oder Dienstleistungen zu den angegebenen Konditionen bereitzustellen.“ [7]

---

[1] Vgl. auch Munzel, S. 28ff.
[2] Vgl. Herold, S. 11.
[3] Atena.
[4] Herold, S. 11.
[5] Vgl. Herold, S. 11.
[6] Herold, S. 10.
[7] Brückner, S. 40.

Grundsätzlich kann die Beschaffung im Unternehmen bzw. im Konzern unterschiedlich organisiert werden. Häufig ist ein zentraler Einkauf anzutreffen, wobei Unternehmensbereiche aber für bestimmte Materialien im operativen Betrieb keine besondere Einbindung des Einkaufs für den Bezug dieser benötigen, weil durch die Definition von Abrufen beim Lieferanten als Einkaufsbelegart Fachbereiche im gewissen Rahmen eigenständig agieren können (sollen).

„Aus der Sicht der Materialwirtschaft und des Einkaufs ist die Einkaufsorganisation für die gesamte Abwicklung von Einkaufsfunktionen zuständig. Da die Einkaufsorganisation eine zentrale Rolle im Bereich des Einkaufs wahrnimmt, ist es erforderlich, sich einen Überblick darüber zu verschaffen, welche Form des Einkaufs im Unternehmen systemseitig zum Einsatz kommt. Dabei kann eine Einkaufsorganisation:

- mehreren Buchungskreisen zugeordnet sein = konzernbezogener Einkauf
- einem buchungskreis zugeordnet sein = firmenbezogener Einkauf
- ohne Zuordnung zu einem Buchungskreis bestehen
- mit einer oder mit mehreren anderen Einkaufsorganisationen verknüpft werden (=Referenzeinkaufsorganisation)
- Einkaufsorganisationen müssen einem oder mehreren Werken zugeordnet werden (=werksbezogener Einkauf); Berechtigungen für die Bearbeitung der Einkaufsvorgänge können je Einkaufsorganisation vergeben werden.

Die Einkaufsorganisationen werden in der Tabelle T024E gespeichert.“ [8]

Eine Bestellanforderung (über Transaktion ME54) definiert im Rahmen der zielgerichteten Materialbereitstellung den im System dokumentierten, konkreten Bedarf des anfordernden Fachbereiches. [9] „Darauf aufbauend wird innerhalb der Bestellabwicklung eine Bestellung generiert (Erstellung, Freigabe über Transaktion ME21, ME28 / Ablage in Tabellen EKKO, EKPO / Anzeige über Transaktion ME23N).“ [10] Der Einkauf kann Anforderungen aus div. Fachbereichen in einer Bestellung bündeln.

Nachfolgend wird ein Weg aufgezeigt, wie im Bereich der Beschaffungsberechtigungen zur Bestellanlage Konflikte in der Berechtigungsherstellung erkannt und reduziert werden können. Dieses Vorgehen kann zur Verifizierung automatisiert generierter Ergebnisse berechtigungsauswertender Drittanbieter-Tools (mit SoD-Konfliktanalyse) ebenfalls genutzt werden.

Grundlagen

Folgende Grundannahmen werden getroffen:

Das Unternehmen weist einen zentralen Einkauf auf, der grundsätzlich alle Bestellungen im System auslösen soll. Es erfolgt keine besondere Kompetenzverteilung innerhalb der Gruppe der Einkäufer. Es gibt allerdings unter Einkaufsbelegtyp (in Domäne EBSTYP [Typ des Einkaufsbelegs]) **„Bestellung“ Einkaufsbelegarten** (Tabelle T161), die einer besonderen Beachtung unterliegen. Bestellungen, die einen besonderen Wert für das Unternehmen darstellen und deren Konditionen, Lieferantenumsätze usw. grundsätzlich reglementiert bekannt sein sollen, werden als „GB“ angelegt. Es gibt nur eine geringe Anzahl an Berechtigten im Einkauf, die einen anlegenden Zugriff erhalten. Auch der Sichtzugriff ist in der Berechtigtenzahl begrenzt, neben den zuvor erwähnten Einkäufern auf Beschäftigte des Finanz- und Rechnungswesens und auch der Internen Revision. Weiter wird eine Einkaufsbelegart für Abrufe der operativen Fachbereiche bereitgestellt, die diese selbständig beim Lieferanten auslösen können. Die Vorgänge laufen unter der Belegart „AB“ (Abruf per Fax) und sie können durch die Fachbereiche eigenständig angestoßen werden (Aktivität 01). Jeder Fachbereich hat wenige Berechtigte als SAP-KeyUser, die diese Funktion ausüben können. Weiterhin gibt es ein Portal zur Beschaffung von Katalogware (Büromaterial, Druckerpapier, Zubehör etc.), die unter der Belegart

[8] Herold, S. 13.
[9] Vgl. Brückner, S. 39.
[10] Herold, S. 20.

„EC“ bestellt wird. Neben dem Stammhaus gibt es verschiedene Tochterunternehmen, die sowohl auf der Ebene der Buchungskreise als auch der Einkaufsgruppe (Tabelle T024), der Einkaufsorganisation (Tabelle T024E) und der Werke (Tabelle T001W / T024W) berechtigungsseitig unterschieden werden.

T161			**T024E**		**T024W**	
BSTYP	**BSART**	**BATXT**	**EKORG**	**EKOTX**	**WERKS**	**EKORG**
F (Bestellung)	AB	Abruf per Fax	1000	Stammhaus	100-199, 1000	1000
F (Bestellung)	EC	EC Purchase Order	3000	Tochter1	300-399, 3000	3000
F (Bestellung)	RB	Rahmenbestellung	5000	Tochter2	500-599, 5000	5000
F (Bestellung)	GB	Besondere Materialien	7000	Tochter3	700-799, 7000	7000
F (Bestellung)	NB	Normalbestellung	9000	Tochter4	900-999, 9000	9000
F (Bestellung)	[…]					
F (Bestellung)	UB	Umlagerungsbestellung				

Tab. 1: Beispielwerte der Steuerungstabellen für die nachfolgende Analyse (Auszug).

Berechtigungssteuerung

„Jede Transaktion wird durch einen Transaktionscode repräsentiert und erfordert im Allgemeinen zusätzliche Spezifikation der zu berechtigenden Funktionalität. Dies geschieht in Form von Berechtigungsobjekten mit entsprechend ausgeprägten Feldwerten, die in Berechtigungsprofilen gesammelt werden. Das Berechtigungskonzept des SAP-Systems basiert auf diesen Berechtigungsprofilen, die dem jeweiligen SAP-Benutzer im Benutzerstammsatz […] in Form von Rollen zugewiesen werden.“ [11] Ein Transaktionsaufruf, hinter dem ein codiertes Programm zur Abarbeitung der betriebswirtschaftlichen Funktion innerhalb des SAP ERP steht, fordert also einen bestimmten Umfang an Berechtigungsobjektfeldausprägungen an, damit die angeforderte Funktion gewährt wird. Die Tabelle TSTC enthält dabei die Zuweisung Transaktionscode zu Programm und die Tabelle TSTCT die Beschreibung der Transaktion in den verschiedenen Sprachen des Systems. In den Tabellen USOBT und USOBT_C sind die Berechtigungsvorschläge zu den Transaktionen gepflegt. Diese werden im Profilgenerator (Transaktion PFCG) bei der Erstellung einer neuen Rolle und nach dem Zuweisen einer Transaktion ausgelesen. Die benötigten Berechtigungsobjekte werden dann automatisch hinzugefügt. Die anschließende Ausprägung der vorgegebenen Berechtigungsobjekte steuert dann die eigentlichen Zugriffsrechte einer Rolle. Ist innerhalb des Benutzerstammsatzes die angeforderte Soll-Ausprägung vorhanden, wird die Funktionsnutzung gewährt, ansonsten unter Hinweisgebung durch das System abgelehnt. Die Bestellauslösung z.B. wird durch die Transaktionscodes ME21 oder ME21N angesteuert.

Bestellungen anlegen		
S_TCODE	Transaktion	ME21 (Bestellung hinzufügen), ME21N (Bestellung anlegen) oder Substitution über z.B. SA38 unter Angabe des aufrufenden Programms, z.B. Programmname RM_MEPO_GUI
M_BEST_BSA	Aktivität	01 (Anlegen), 09 (Preisanzeige)
	Einkaufsbelegart	gem. Tabelle T161 (Einkaufsbelegarten)
M_BEST_EKG	Aktivität	01 (Anlegen), 09 (Preisanzeige)
	Einkäufergruppe	gem. Tabelle T024 (Einkaufsgruppen)
M_BEST_EKO	Aktivität	01 (Anlegen), 09 (Preisanzeige)
	Einkaufsorganisation	gem. Tabelle T024E (Einkaufsorganisationen)
M_BEST_WRK	Aktivität	01 (Anlegen)
	Werk	gem. Tabelle T001W / T024W (Werke / zulässige Einkaufsorganisationen zum Werk)

Tab. 2: Berechtigungsobjektausprägungsanforderungen aus Tabelle USOBT zu ‘Bestellungen anlegen‘.[12]

Neben den auslösenden Transaktionscodes ist es auch möglich, eine Substitution eines solchen durch eine Transaktion hervorzurufen, die das Anstarten eines Programms ermöglicht, so z.B. über SA38 (ABAP-Reporting), OODR (Reportvariante für Zeitauswertung) und andere. Sofern bei Vorliegen der Objektausprägungen ein Benutzerstammsatz eine solche Transaktion aufweist, kann er ebenfalls die jeweilige Funktion nutzen. Eine Bestellfreigabe, die über Transaktion ME28 (oder dem Programm RM06EF00) und dem Berechtigungsobjekt M_EINK_FRG (Tabellen T16FC und T16FG) finalisiert wird, ist damit zwar nicht verbunden, häufig wird aber eine Freigabestrategie gefahren, die bewirkt, dass Bestellvorgänge verschiedener Einkaufsbelegarten ohne weitere Freigabe durchlaufen und die

[11] Brückner, S. 33.
[12] Vgl. Brückner, S. 40.

Lieferung anstoßen. Die Bestätigung der Warenlieferung / Wareneingangsmeldung (Transaktion MIGO [Warenbewegung] mit den zugehörigen Berechtigungsobjekten M_MRES* und M_MSEG* [Reservierungen und Wareneingang / Warenbewegungen / Materialbelege]) im System bildet dann die Grundlage der ausgehenden Zahlung. Insoweit ist die Definition einer Bestellung eine maßgebliche und kritische, d.h. zu reglementierende Berechtigung. Der Fokus einer kritischen Auseinandersetzung sollte dabei auf namensbezogenen Stammsätzen (– weniger auf System- und Schnittstellenusern –) liegen. Dies betrifft insbesondere auch administrative und modulbezogene (Betreuer-)Accounts mit weitreichenden Berechtigungen, wenn sie namensbezogen vergeben werden. [13] Wenn solche Stammsätze innerhalb der Module auslösende Berechtigungen im Produktionssystem aufweisen, ist dies als kritisch zu sehen.

Nachfolgend wird ein mögliches Prüfungsvorgehen zur Analyse der Anlageberechtigungen von Bestellbelegen für das Stammhaus (ohne explizite Unternehmensbeteiligungen) beschrieben.

Berechtigungsanalyse

Zunächst ist von Interesse, welche Rollen auslösende Elemente beinhalten. Kombinationsrisiken entstehen insbesondere dann, wenn – zuzüglich zum Berechtigungsobjekt S_TCODE – mehrere Berechtigungsobjekte die Funktionsbereitstellung determinieren, da es durchaus üblich ist, dass sich solche zusammensetzenden Berechtigungen nicht aus einer einzigen Rolle speisen, sondern sich die abgleichende Ausprägung des Berechtigungsstammsatzes zum angeforderten Berechtigungs-Soll aus mehreren Rollen bildet. Das System selektiert zum anfordernden Benutzerstammsatz zu den Berechtigungsobjekten die Höchstausprägung, die dieser aus den verschiedenen Rollen mit den jeweiligen Profilen als untergeordnete Strukturelemente aufweist, „gleichgültig, aus welchen Profilen sie stammt.“ [14] So ist es möglich, dass Rollen einzeln betrachtet unproblematisch sind, jedoch in Kombination eine kritische Wirkung entfalten. „Sie definieren also allein nicht zwangsläufig eine kritische Ausprägung, können jedoch im Zusammenspiel mit anderen Profilen kritische Ausprägungen beinhalten.“ [15] Es ist davon auszugehen, dass die Einkäuferrolle in sich alle notwendigen Objekte in Höchstausprägung vereint. Ob jedoch noch andere Rollen existieren, die auslösend wirken, und wie diese Wirkungen in Kombination mit anderen Rollen eintreten, muss geprüft werden. Sofern dies manuell geprüft werden soll, stehen bekannte SAP-Reports zur Verfügung. Reports wie beispielsweise RSUSR002 (Benutzer nach komplexen Selektionskriterien), RSUSR020 (Profile nach komplexen Selektionskriterien) und RSUSR070 (Rollen nach komplexen Selektionskriterien) – auslösend z.B. über Transaktion SUIM (Benutzerinformationssystem) – können eingangs nicht mit mehr als drei (bzw. mit zusätzlicher expliziter Transaktionscodenennung) Berechtigungsobjekten arbeiten, d.h. es können nicht alle hier angeforderten Berechtigungsobjekte als Selektionskriterium eingegeben werden, um die Berechtigungen auflösend (und somit die basierenden Rollen und hiermit versorgten Berechtigten) darzustellen. Insoweit können Teilmengen gebildet und über die korrespondierenden Tabellen der Berechtigungssteuerung verifiziert werden.

Es ist sinnvoll, alle Rollen zu ermitteln, die die entsprechenden Berechtigungsobjekte bereitstellen. Die Transaktion muss dabei zunächst nicht als Selektionskriterium angegeben werden, denn zum einen kann diese substituiert werden, zum anderen ist es auch möglich, dass zu einem späteren Zeitpunkt der auslösende Transaktionscode versehentlich einer Rolle zugewiesen wird. Es bleibt folglich wichtig, die Rollen zu identifizieren, die die Ausprägungen der Objekte beinhalten, auch wenn den Personen (ggf. noch) nicht die Transaktion zur Verfügung steht. Ferner kann dies in einem abschließenden Schritt nachgeholt werden. Nachfolgend kann über den Report RSUSR070 und einer Aufbereitung die Herkunft der Berechtigungen mit entsprechender Ausprägung dargestellt werden.

[13] Vgl. Palandrani, S. 26.
[14] Wildensee, S. 13.
[15] Wildensee, S. 13.

Felderausprägungen zur Informationsverarbeitung "Bestellung anlegen" in EKORG 1000 (Stammhaus)

	M_BEST_BSA mit ACTVT = 01 und BSART =	M_BEST_EKG mit ACTVT = 01 und EKGRP = *	M_BEST_EKO mit ACTVT = 01 und EKORG = */1000	M_BEST_WRK mit ACTVT = 01 und WERKS = 100-199, 1000
1. C:DVKMAT_A DV-Koordination Mat.wirtschaft+Einkauf	01,02,03,04,08,09 AAA-GAZ, GCA-ZZZ	01,02,03,04,08,09 *	01,02,03,04,08,09 *	01,02,03,04,08,09 *
2. M:BESTO0_F Einkauf (Grundrolle)	01,02,03,04,08,09 AAA-GAZ, GCA-ZZZ	01,02,03,04,08,09 *	* *	* *
3. M:BESTO3_F Techn. Fachbereiche (TFB)	01,02,08,09 AAA-GAZ, GCA-ZZZ	01,02,08,09 *		
4. M:BE0000_A Einkauf (Grundrolle)	01,02,03,04,06,08,09,76 AAA-GAZ, GCA-ZZZ	01,02,03,04,06,08,09,76 *	01,02,03,04,06,08,09,76 *	01,02,03,04,06,08,09,76 *
5. M:DVKOAL_A DV-Koordination Mat.wirtschaft+Einkauf	01,02,03,04,06,08,09,76 AAA-GAZ, GCA-ZZZ	01,02,03,04,06,08,09,76 *	01,02,03,04,06,08,09,76 *	01,02,03,04,06,08,09,76 *
6. M:BEGBST_A Einkauf (Ausgesuchte Benutzer)	01,02,03,04,06,08,09,75,76 GB			
7. M:E_NOT____ Notfalluser	* *	* *	* *	* *
8. M:RA0000_A Nicht Einkauf (für EKO Töchter)			01,02,03,04,08 *	
9. M:Bexxxx_A (xxxx nicht 0000)	01,02,03,04,06,08,09,75,76 AB	01,02,03,04,06,08,09,75,76 <EKGRP-Eingrenzung>	01,02,03,04,06,08,09,75,76 1000	01,03,04,06,09,76 100-199, 1000 300-399, 3000 500-599, 5000 700-799, 7000 900-999, 9000

Abb. 2: Auslösende Rollen mit entsprechenden Objektausprägungen (Auszug).

Eine Überprüfung ist möglich über die Tabelle AGR_1251 (Berechtigungsdaten zur Aktivitätsgruppe). Unter Angabe von M_BEST_BSA im Feld OBJECT, ACTVT unter FIELD, 01 unter LOW (in einem weiteren Schritt alle Ausprägungen anzeigen lassen und die Generalberechtigung '*' identifizieren) und DELETED = leer offeriert die Tabelle alle Rollen, die entsprechende Inhalte aufweisen. Die weiteren Objekte sind ebenfalls in der Form abzufragen. Die jeweilige Ausprägung der Steuerungsfelder für alle Berechtigungsobjekte, die in den Rollen vorhanden sind (Feld AGR_NAME als zu füllendes Suchfeld), kann ebenfalls über diese Tabelle oder über den Report ausgegeben und dann aufbereitet werden. Die Benennungen der Rollen werden über die Tabelle AGR_DEFINE dargeboten (Felder AGR_NAME und TEXT). Zusätzlich können auch die auslösenden Profile über die Tabelle UST12 (Benutzerstamm: Berechtigungen) mit den Feldern OBJCT (jeweilig relevantes Berechtigungsobjekt), AKTPS (A), FIELD (z.B. ACTVT) und VON (z.B. 01 [und '*'-Eingrenzung analog zuvor]) entnommen werden.

Eine entsprechende Darlegung kritischer Rollen-Benutzer-Zuweisungen kann erstellt werden über eine Kreuztabellenanalyse der zuvor ermittelten Rollen über die per TO_DAT (Bis-Datum der Gültigkeit) eingegrenzte Tabelle AGR_USERS (Zuordnung Rollen zu Benutzern) und der organisatorischen Zuordnung per View USER_ADDR (Benutzer nach Adressdaten; Felder BNAME, NAME_FIRST, NAME_LAST [oder NAME_TEXTC], KOSTL, DEPARTMENT). Ableitbar ist darüber eine Liste der kritischen Benutzerstämme, die entsprechende Rollen(kombinationen) aufweisen.

					M_BEST_BSA	M_BEST_EKG	M_BEST_EKO	M_BEST_WRK
					mit ACTVT = 01/02/03/08/09	mit ACTVT = 01/02/03/08/09	mit ACTVT = 01/02/03/08/09	mit ACTVT = 01/02/03/08/09
Benutzer	Gültig von	Gültig bis	Benutzertyp	problematisch	und BSART <> AB	und EKGRP = *	und EKORG = */1000	und WERKS = 100-199, 1000
HA40xx	01.01.2007	31.12.9999	A Dialog	1	M:BESTO3_F	M:BESTO3_F	M:BE1380_A	M:BE1380_A
HF2Dxx	01.01.2007	31.12.9999	A Dialog	1	M:BESTO3_F	M:BESTO3_F	M:BE1380_A	M:BE1380_A
HG2Lxx	29.12.2006	31.12.9999	A Dialog	1	M:BESTO3_F	M:BESTO3_F	M:BE1390_A	M:BE1390_A
HK22xx	22.06.2004	31.12.9999	A Dialog	1	M:BESTO3_F	M:BESTO3_F	M:BE1380_A	M:BE1380_A
HN00xx	01.01.2007	31.12.9999	A Dialog	1	M:BESTO3_F	M:BESTO3_F	M:BE1380_A	M:BE1380_A
HN00xx	01.01.2007	31.12.9999	A Dialog	1	M:BESTO3_F	M:BESTO3_F	M:BE1380_A	M:BE1380_A
HN10xx	01.01.2007	31.12.9999	A Dialog	1	M:BESTO3_F	M:BESTO3_F	M:BE1380_A	M:BE1380_A
HN10xx	01.01.2007	31.12.9999	A Dialog	1	M:BESTO3_F	M:BESTO3_F	M:BE1380_A	M:BE1380_A
HN41xx	01.01.2007	31.12.9999	A Dialog	1	M:BESTO3_F	M:BESTO3_F	M:BE1380_A	M:BE1380_A
HN41xx	01.01.2007	31.12.9999	A Dialog	1	M:BESTO3_F	M:BESTO3_F	M:BE1380_A	M:BE1380_A
HN41xx	01.01.2007	31.12.9999	A Dialog	1	M:BESTO3_F	M:BESTO3_F	M:BE1380_A	M:BE1380_A
USR22xx	09.01.2007	31.12.9999	A Dialog	1	M:BESTO0_F+ M:BE0000_A (ehemals Einkäufer)	M:BESTO0_F+ M:BE0000_A	M:BESTO0_F+ M:BE0000_A+ M:RA0000_A	M:BESTO0_F+ M:BE0000_A
USR36xx	16.06.2010	31.12.9999	A Dialog	1	M:BESTO3_F	M:BESTO3_F	M:BE1380_A	M:BE1380_A
USR39xx	10.06.2009	31.12.9999	A Dialog	1	M:BESTO3_F	M:BESTO3_F	M:BE1380_A	M:BE1380_A
USR46xx	02.08.2011	31.12.9999	A Dialog	1	M:BESTO3_F	M:BESTO3_F	M:BE1380_A	M:BE1380_A
Überprüfung notwendig:				15				

Abb. 3: Übersicht der Benutzerstammsätze mit Rollenkombinationen (Auszug).

Es kommt vor, dass Beschäftigte unternehmensintern wechseln und (versehentlich) ihre bisherige(n) Rolle(n) beibehalten und um die neue Rolle ergänzt werden, wenn der Entzug der alten Rolle nicht sauber erfolgt. Wenn die ehemalige(n) Rolle(n) aber die des Einkäufers ist (sind), ist (sind) die Einkäuferrolle(n) und evtl. weitere Rollen, die nicht mehr der tatsächlichen Aufgabenwahrnehmung entsprechen, umgehend zu entziehen. Dies trifft insbesondere auch dann zu, wenn die Rollenvergabe über ein externes Identity- & Access Management Tool wie z.B. QuestOne gesteuert wird, denn dann verlassen sich sowohl der IT-Treuhänder als auch die berechtigungsverantwortlichen Fachbereiche (hier Materialwirtschaft und Einkauf) auf die hinterlegten – per Remote im Produktionssystem anstoßenden – Automatismen der Berechtigungssteuerung, die auch die gesetzlichen Dokumentations- und Nachweispflichten im Bereich der Berechtigungskonzeption als externes Tool gewährleisten müssen (vgl. hierzu z.B. 5.5.1 und 6.2.4 GoBS i.V.m. FAIT1.3.1(23) und FAIT1.4.2(84)), aber fehlerhaft implementiert sein können. Entsprechend sollten auch die definierten und relevanten Workflow-Prozess- und -Freigabeprozesse im IAM-Tool separat analysiert werden.

Nach entsprechender Überprüfung der organisatorischen Zuweisung kann im Ergebnis festgestellt werden, dass sowohl die Einkäuferrollen (M:BESTO0_F, M:BE0000_A und M:BEGBST_A) als auch die Rollen der DV-Koordination des Bereiches Materialwirtschaft und Einkauf (C:DVKMAT_A und M:DVKOAL_A) weitreichend als anlegende Verursacherrollen definiert sind. Es gibt aber auch eine Kombinationsrolle, die außerhalb des Einkaufs eine weitreichende Berechtigung in der Steuerung der Einkaufsbelegarten bereitstellt.

Berechtigungen im technischen Bereich (TFB) werden kombiniert vergeben über die Rollen M:BESTO3_F mit einer hohen Ausprägung im Bereich Einkaufsbelegart, M:RA0000_A mit ausschließlicher und hoher Ausprägung im Bereich der Einkaufsorganisation und der Gruppe M:BExxxx_A mit jeweils starker Eingrenzung im Bereich Einkaufsbelegart, Einkaufsgruppe und Einkaufsorganisation und unterschiedlicher Ausprägung im Bereich der Lagerorte / Werke. So sind unterschiedliche Zugriffe zur Bestellung für Töchter realisiert. Die Höchstausprägung im technischen Bereich, also außerhalb des Einkaufs, wird vergeben über die Kombination M:BESTO3_F (Grundrolle TFB) mit M:RA0000_A (Delta-Kombinationsrolle – auch, aber nicht ausschließlich für den Einkauf, sondern vornehmlich für die organisationsübergreifende TFB-KeyUser-Funktion, die für mehrere Organisationsbereiche der TFB zentral bestellen soll / muss; Vollzugriff auf alle Tochterunternehmen ausschließlich im Bereich EKORG) und M:BExxxx_A (mit starker organisatorischer Begrenzung).

Ziel muss es sein, abschließend zu überprüfen, ob die Rollen den Beschäftigten zugewiesen sind, die organisatorisch als Aufgabenträger durch die Fachbereiche benannt wurden. Ist es dann das Ziel, die Fachbereiche darauf zu beschränken, ausdrücklich nur eine oder zumindest wenige Einkaufsbelegarten (AB steht synonym für eine starke Eingrenzung der Einkaufsbelegarten, ggf. zuzüglich weiterer, außerhalb des Einkaufs notwendiger Einkaufsbelegarten [Portal-„EC“ nur dann in den Rollen der Fachbereichsstammsätze, wenn die Portal-‘SAP ERP‘-Schnittstelle nicht über einen privilegierten Schnittstellenuser bedient wird. Vgl. zur RFC-Berechtigungsreduktion von RFC-Schnittstellenusern, die meist sehr weitreichende Rechte aufweisen, auch SAP-Note 1682316 mit Xiting RoleBuilder]) eigenverantwortlich auszuführen, muss die Rolle M:BESTO3_F dahingehend angepasst werden, auf die gewünschten Belegarten zu beschränken. Wird die Rolle aber auch von anderen Fachbereichen verwendet, die den erweiterten Zugriff benötigen, muss sie den TFB-Beschäftigten ggf. entzogen werden, um dann ausgesuchte Rollen der Rollengruppe M:BExxxx_A um die dort fehlenden Einkaufsbelegarten zu ergänzen für die TFB-Beschäftigten, die die Rolle zuvor verloren haben. Der Entzug einer Rolle bedeutet aber wiederum, dass zunächst geschaut werden muss, ob noch weitere, nicht im Fokus liegende Objekte in der zu entziehenden Rolle vorhanden sind, die dann in der Arbeitsplatzdefinition verloren gehen. Wenn diese Objekte und deren Ausprägung nicht anderweitig aus weiteren Rollen bei den Beschäftigten vorliegen, sind diese Objekte ggf. zu substituieren.

Der Prüfer sollte sich immer fragen, ob etwaige Anpassungen alle Interessen der mit dieser Rolle versorgten Fachbereiche widerspiegeln oder ggf. darauf aufbauend kompensierende Anpassungen in weiteren, bereichs- oder funktionsspezifischen Rollen notwendig sind. Auch dies kann wiederum zu Wirkungen in anderen Fachbereichen führen, so dass die Anpassung einen iterativen Prozess bedeutet, bis alle Rollen den Fachbereichsnotwendigkeiten entsprechen.

Der Pfad, den eine Berechtigung unter Beachtung der auslösenden Rollen nimmt, sollte je organisatorischer Gruppierung zur Verifizierung dargestellt werden. Hierüber kann der Bedarf zur Anpassung unkompliziert identifiziert werden. Sofern die auslösende Rolle mehr als einen Organisationsbereich berechtigt, ist die Darstellung analog anzupassen und der Anpassungsbedarf konfliktfrei zu definieren.

Im Übrigen können auch die Änderungsberechtigungen auf Bestellungen mit den oben erwähnten Berechtigungsobjekten und analogem Vorgehen geprüft werden (ACTVT = 02). Ebenso kann das Vorgehen auch bei der Prüfung von Rahmenverträgen (Objekte M_RAHM*) gewählt werden.

Auslöser				Objektausprägungen			
M:BEx000_M			Rollenname	M_BEST_BSA	M_BEST_EKG	M_BEST_EKO	M_BEST_WRK
UserID	Name	OE					
HG2Exx	Klaus Düwelei	3xx	M:BE13x0_A	01,02,03,04,06,08,09,75,76	01,02,03,04,06,08,09,75,76	01,02,03,04,06,08,09,75,76	**01,02,03,04,06,08,09,75,76**
HF33xx	Detlef Meyer	3xx		AB	3x	1000	**100-199, 1000**
HF12xx	Wolfgang Kahle	3xx					
HF31xx	Manuela Franke	3xx	M:BE13x0_M	02,03,04,06,08,09,76	02,03,04,06,08,09,76	**02,03,04,06,08,09,76**	**02,03,04,06,08,09,76**
HT02xx	Thomas Graf	3xx		AB	3x	**1000, 7000**	**100-199, 1000, 700-799**
			M:BEx000_M	**02,04,06,08,09,76**	**02,03,04,06,08,09,76**	**02,03,04,06,08,09,76**	**02,03,04,06,08,09,76**
	M_BEST_WRK			**AAA-GAZ, GCA-ZZZ**	*	**7000**	**700-799**
	je nach Ziel WERKS						
			M:BEx3x0_A	01,02,03,04,06,08,09,75,76	01,02,03,04,06,08,09,75,76	01,02,03,04,06,08,09,75,76	**01,02,03,04,06,08,09,75,76**
				AB	3x	7000	**700-799**

Abb. 4: Besondere Verifizierung des Berechtigungspfades bei Änderungsaktivität (ACTVT=02) mit Transaktionen ME22 / ME22N.

Zuletzt können die erkannten namensbezogenen Berechtigten dahingehend überprüft werden, ob sie die auslösenden Transaktionen oder eine analoge Transaktionscodesubstitution im Benutzerstammsatz aufweisen.

Es sei der Hinweis erlaubt, dass auch in anderen „Modulen“ Funktionsaufrufe durch mehrere Berechtigungsobjekte und Steuerungsfeldausprägungen determiniert werden. Auch dort können sich die steuernden Objekte in mehreren Rollen wiederfinden und auf der Ebene der Benutzerstammsätze zusammensetzen, so dass das Problem der berechtigenden Rollenkombinationen grundsätzlich in allen modularen Bereichen des ERP auftritt.

Fazit

Fachbereiche außerhalb des Einkaufs müssen ebenfalls Bestellvorgänge auslösen können, dies ist nach gängiger Auffassung im Rahmen der Eigenverantwortung der operativen Fachabteilungen durchaus Standard. Es ist jedoch wichtig, dass die Berechtigungen eindeutig und konfliktfrei definiert sind. Dies ist möglich über Eingrenzungen in den Steuerungsfeldern Einkaufsbelegart, Einkaufsgruppe, Einkaufsorganisation und Werke / Lagerorte. Die Verteilung der an der Zugriffsberechtigung beteiligten Berechtigungsobjekte mit gewährenden Feldausprägungen auf verschiedene Rollen – dies ist eine Problematik, die in einer Vielzahl von Funktionsgewährungen in SAP vorkommt, da nicht selten mehrere Berechtigungsobjekte an der Zugriffsgewährung beteiligt sind – macht regelmäßige manuelle oder toolunterstützte Analysen sowohl durch die Revision als auch durch den Einkauf notwendig. Zur Verfügung stehen z.B. Tools wie CheckAud for SAP Systems oder auch SAP GRC Access Control zur Vermeidung von Berechtigungskonflikten. Darüber hinaus ist es möglich, die Einkaufsprozesse automatisiert zu monitoren, z.B. per Remedyne Fraud Prevention. Aber auch die Analyse in der Vergangenheit getätigter Beschaffungsvorgänge und die auslösenden Benutzer (z.B. auch bei Bestellanlagen über Tabelle EKKO mit den Feldern BSTYP, BSART, LOEKZ, AEDAT, ERNAM, EKORG und EKGRP) sollten im Fokus stehen. Dies kann dazu führen zu erkennen, ob zum einen Vorgänge außerhalb des Einkaufs angestoßen wurden, die dem Einkauf vorbehalten sein sollen, und – auch wenn dies zunächst datenschutzrechtlich problematisch erscheint – zum anderen, welche Personen bzw. abgeleitet welche Rollen hierfür verantwortlich sind.

Literatur

Atena	http://www.atena.pl/pliki/cms/190/schemat_sap_atena.png .
Brückner, Helga	SAP MM-Berechtigungen in der Praxis, in: PRev Revisionspraxis 1/2011, S. 33-42.
Herold, Marcus (Hrsg.)	Werteflüsse im SAP-System, Prüfmanual für die Praxis, 1. Auflage 2013, Boorberg-Verlag.
Munzel, Renata/Martin	SAP-Finanzwesen – Customizing 1. Auflage 2012, Galileo Press.
Palandrani, Alexandra	Grundsätze zur Überwachung privilegierter Accounts, in: PRev Revisionspraxis 1/2013, S. 25-28.
SAP	Remedyne Fraud Prevention, https://www.sapappsdevelopmentpartnercenter.com/en/news/remedyne-fraud-prevention_75/ .
Rüter/Schröder/ Göldner/Niebuhr	IT-Governance in der Praxis. Erfolgreiche Positionierung der IT im Unternehmen. 2. Auflage 2010, Springer-Verlag.
Wildensee, Christoph	Das Rollenkonzept in SAP R/3 – Gestaltungsmöglichkeiten aus Sicht der IV-Revision, in: ReVision 3/2002, S. 10-17.

Autor:

Dipl.-Betriebswirt Christoph Wildensee, DBA, CISM, CRISC, ist seit 1993 als IV-Revisor bei der Stadtwerke Hannover AG (SWH) tätig. Zusätzlich war er von 2008 bis 2012 auch Datenschutzbeauftragter der SWH und der entsprechenden Netzgesellschaft.

Abstract:

Die Berechtigungsobjekte M_BEST* determinieren den anlegenden und manipulierenden Zugriff auf definierte Einkaufsbelegarten des Einkaufs über Transaktionen wie z.B. ME21. Die ausschließlich zentrale Abarbeitung von allen Beschaffungsvorgängen ist in der heutigen Zeit eher selten anzutreffen. Bestimmte Einkaufsaktivitäten und somit Belegarten sind häufig auch freigegeben für Zugriffe operativer Bereiche im Unternehmen außerhalb des Einkaufs. So erfolgt auch dort in den Rollen die Zuweisung beschaffungsrelevanter Transaktionscodes und steuernder Berechtigungsobjektausprägungen. Die Rollendefinition können problematisch wirken, ergeben sich die tatsächlichen Berechtigungen doch erst als Zusammenfassung der zugewiesenen Rollen auf der Ebene der Stammsätze. Der Artikel beschreibt ein Prüfungs- und Dokumentationsvorgehen zur Analyse dieser prozessual kritischen Berechtigung.