Rollenkollisionen in SAP – Die Analyse

Dipl.-Betriebswirt Christoph Wildensee, CISM

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.

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 die Reports RSUSR002 (Benutzer nach komplexen Selektionskriterien) und RSUSR020 (Profile nach komplexen Selektionskriterien) ein möglicher zentraler Anlaufpunkte bei der Berechtigungsanalyse, wenngleich dies eine veraltete Methode ist, die nicht mehr verwendet werden sollte. Weitaus sinnvoller ist das Vorgehen über den Report RSUSR070 (Rollen […]), der in der Rollenanalyse ebenfalls Berechtigungsobjektausprägungsabfragen erlaubt. Einzelrollen, die eine 1:1-Verbindung zu den Profilen aufweisen, werden gebündelt zu Sammelrollen, die den jeweiligen Arbeitsplätzen entsprechen.
Es ist weit verbreitet, 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. Neben Sammelrollen- sind auch direkte Einzelrollenzuweisungen zu Benutzerstämmen 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 weit reichende 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 weit reichend berechtigte Verursacher zu ermitteln. Ziel muss es sein, die Ausgangsprofile zu identifizieren, die ihre Berechtigungen im Stammsatz weitergeben zu einer Höchstausprägung. Die Identifizierung der auslösenden Profile, die den Einzelrollen entsprechen, 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 Sammelrollen (Arbeitsplätze) 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 RSUSR070 geschaut werden, welche Rechte (Objektrechte und Transaktionsumfang) hier im Detail implementiert sind. Bei Einsichtnahme in den Berechtigungsstammsatz können hier die verursachenden Berechtigungen abgeleitet werden. Die Suche nach relevanten Transaktionen und ausgeprägten Berechtigungsobjekten analog Tabelle USOBT kann hier zu markanten Treffern 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 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 RSUSR070 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.

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 weitestgehend 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.

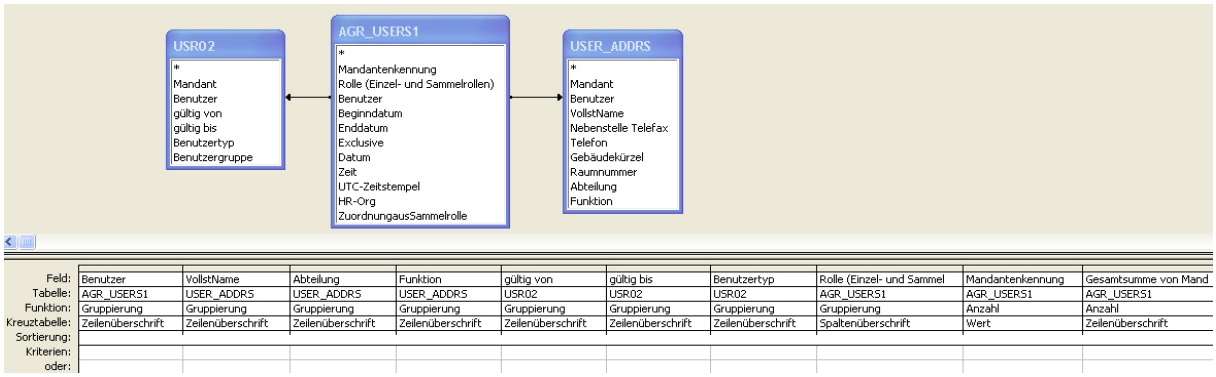
Die Untersuchungskriterien innerhalb der Berechtigungsanalyse sind also nochmals in Kürze dargestellt folgende:

- Rollen mit einem stark ausgeprägten 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 Verursacherrollen bildet somit den Ausgangspunkt für die Identifizierung kritischer Arbeitsplätze. Werden diese erkannt und zudem auch die Rollen, die für die zu begrenzende Organisation als SB-Arbeitsplätze nicht mit den Verursacherrollen 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, welches 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. Zuweisungs- und Kollisionsanalyse unterzogen werden.

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.