

Das Rollenkonzept in SAP R/3 – Gestaltungsmöglichkeiten aus Sicht der IV-Revision

Von Dipl.-Betriebswirt Christoph Wildensee, Hannover¹

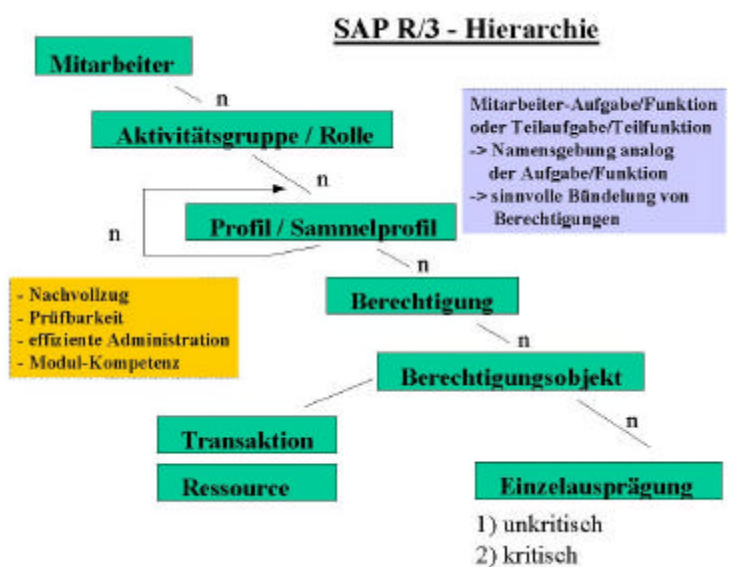
Einführung

Das Berechtigungskonzept dient als grundlegende Sicherheitsfunktion des SAP R/3-Systems. Elemente dieses Konzeptes sind die Aktivitätsgruppe ([Template- {ab 4.6}]Rolle), das Profil/Sammelprofil, das Berechtigungsobjekt und seine Steuerungsfelder, die Transaktion und letztendlich das Zusammenspiel dieser Komponenten zu einer Berechtigungsstruktur. Die Festlegung von Rahmenbedingungen, die innerhalb des Berechtigungskonzeptes einzuhalten sind, ist eine der wichtigsten Definitionen, bevor die Systemanpassung durchgeführt und das System produktiv gesetzt wird. Im Customizing und der dazugehörigen Dokumentation entscheidet sich der Erfolg oder Misserfolg des zugrundeliegenden Berechtigungskonzeptes. Die Kriterien zur Bemessung sind überschaubar:

Das Berechtigungskonzept muss aus Sicht der Revision

- verständlich, zuverlässig und prüfbar
 - ordnungsgemäß gemäß der rechtlichen Rahmen
 - somit nachvollziehbar (sowohl aus Sicht der Administration als auch der Revision und des Fachbereiches)
 - administrierbar (d.h. Vorhaltung von möglichst wenig Verwaltungsobjekten) und
 - praktikabel im Sinne von nutz-/handelbar (insbesondere aus Sicht des Fachbereiches)
- sein.

Dieses führt nicht nur dazu, dass es ordnende Elemente geben muss, die als Berechtigungssammler nachvollziehbar/prüfbar und über ein sinnvolles Beantragungswesen zuweisungsfähig sind, sondern auch, dass Funktionen sinnvoll abgegrenzt und in Form von „Berechtigungsbausteinen“ vorgehalten werden. Innerhalb des SAP-Systems kann eindeutig definiert werden, wer welche Funktion ausüben soll (Transaktion und Berechtigungsobjekt), was der Einzelne mit Daten durchführen kann (Aktivitätensteuerung Anzeigen, Ändern, Löschen etc.) und innerhalb welcher organisatorischen Grenzen er dies tun darf (Buchungskreis, Einkaufsorganisation etc.).



Entsprechend sind aufgaben-/funktionsorientiert Gruppierungen von Berechtigungen möglich, die zum einen ein Minimum an Verwaltungsobjekten bedeuten, zum anderen aber besonders auch die Administration und die Beantragungsseite in größeren Unternehmen entlasten.

¹ C. Wildensee ist bei der Stadtwerke Hannover AG als IV-Revisor tätig.

Prüfungsstrukturen

Der IV-Revisor muss sich, wenn er sich im SAP-Umfeld bewegt, mit den Ordnungsbegriffen des SAP-Systems vertraut machen. Einige dieser Begriffe werden im folgenden kurz dargestellt.

Aktivitätsgruppe

Das Konzept von SAP R/3 sieht vor, dass Aktivitätsgruppen als Rollendefinitionen dienen und somit als „Berechtigungssammler“ untergeordneter Tätigkeiten oder sonstiger Ordnungskriterien innerhalb des Berechtigungskonzeptes strukturieren (ab Release 4.6 auch [Template-]Rollen genannt). Die Definition von Aktivitätsgruppen kann unterschiedlich erfolgen. Als eine der sinnvollsten Möglichkeiten hat sich die Einrichtung der Aktivitätsgruppen als betriebswirtschaftliche Funktion, Stelle oder Arbeitsplatz herausgestellt, die wiederum ihre Teilfunktionen oder -aufgaben innerhalb der Profile und Sammelprofile abbildet. SAP lässt für die Bezeichnung einer Aktivitätsgruppe bis zu 30 Zeichen zu (siehe über Tabelle DD03L).

Die wichtigsten Prüftabellen für Aktivitätsgruppen sind die folgenden:

Tabelle	Beschreibung
AGR_DEFINE	Aktivitätsgruppe (AktGr.) mit Bezeichnung
AGR_PROF	AktGr. mit zugehörigem Hauptprofil
AGR_1016	AktGr. mit zugehörigen Profilen (auch Teilprofile)
AGR_1250	AktGr. mit zugehörigen Profilen und Berechtigungsobjekten
AGR_1251	wie zuvor, jedoch mit Steuerungsfeldeingrenzung
AGR_USERS	Zuordnung der AktGr. zu den SAP-Nutzern
AGR_SELECT	AktGr. mit zugeordneten Transaktionscode/Menü etc.

Tab. 1: Tabellen zur Prüfung im Bereich Aktivitätsgruppen

Profil / Sammelprofil

Profile und Sammelprofile bieten die weitere Möglichkeit der Untergliederung, Berechtigungen innerhalb des SAP-Systems auf bestimmte Ressourcen zu strukturieren. Profile können dabei als Abbild und Sammler logisch zusammengehöriger, einzelner Berechtigungen im SAP-System im Sinne von Arbeitsschritten verstanden werden. Sammelprofile bündeln diese wiederum zu Tätigkeiten. Hier schließt sich der Kreis, denn diese Arbeitsschritt- u/o Tätigkeitsbeschreibungen werden in der Aktivitätsgruppe zu Funktionen/Stellen zusammengefasst. - In vielen Unternehmen werden insbesondere die Sammelprofile nicht genutzt, Profile gelten dort als alleinige Zusammenführung von Ressourcenzuweisungen und Zugriffsdefinitionen. Dies kann zum einen daran liegen, dass die Verwaltung und Einrichtung Schwächen aufweist, zum anderen aber auch, dass die von SAP mitgelieferten Sammelprofile und Rollendefinitionen alter SAP R/3-Releasestände sicherheitstechnische Schwächen aufwiesen (häufige Stern-Berechtigungen). Sie waren zum Teil so eklatant, dass sie nur unter intensiver Nachbearbeitung überhaupt nutzbar waren. So haben viele Unternehmen die vorgefertigten SAP-Bestandteile verworfen und darüber hinaus das Ordnungskriterium Sammelprofil ungenutzt gelassen. - Profile beinhalten die Berechtigungsobjekte (insgesamt gibt es mehr als 800) mit entsprechenden Ausprägungen der Steuerungsfelder, über die die Zugriffe auf die SAP-Ressourcen gesteuert werden, somit also z.B. Aktionen auf Belege (Buchen, Anzeigen, Ändern), Transaktionen und Gruppenzugriffe (Benutzergruppen, Tabellen etc.). Grundsätzlich ist das Profil und seine Unterordnung das Hauptkriterium für den Revisor, da hier die Verbindung zum Berechtigungsobjekt und zur konkreten Ausprägung des Zugriffs geschaffen wird. SAP lässt für die Bezeichnung eines Profiles nur bis zu zehn Zeichen zu.

Die wichtigsten Prüftabellen für Profile sind die folgenden:

Tabelle	Beschreibung
UST12	Objekte und Ausprägungen je Profil
UST04	Profile pro SAP-Nutzer
UST10S	Profile mit Objekt und Berechtigung
UST10C	Sammelprofil mit zugehörigen Profilen
USR11	Texte zu den Profilen

Tab. 2: Tabellen zur Prüfung im Bereich Profile

Profilgenerator

Der Profilgenerator (PFCG) ist als Erleichterung bei der Definition von Berechtigungsstrukturen für die Administration gedacht. Ziel ist die Bereitstellung eines Tools zur Generierung von Berechtigungen und der gleichzeitigen zentralen Ablage der definierten Strukturen nebst Nutzer-Zuweisung. Der Profilgenerator arbeitet in der Form, dass sich der Administrator entweder direkt die notwendigen Berechtigungsobjekte mit entsprechender Ausprägung der Steuerungsfelder oder durch Menübäume die notwendigen SAP-Funktionen auswählt, woraufhin der Profilgenerator die benötigten Berechtigungsobjekte, Transaktionscodes etc. automatisch übernimmt. Die Ablage erfolgt in einem Profil, welches genau einer Aktivitätsgruppe zugeordnet ist. Sofern z.B. buchungskreisabhängige Komponenten bereitgestellt werden müssen, ist die Generierung mehrerer Profile unter einer Aktivitätsgruppe jedoch ohne weiteres möglich. Sofern der Administrator keine Änderungen vornimmt, schlägt der Profilgenerator einen Standard-Profilnamen vor und vergibt ihn automatisch mit fortlaufender Nummerierung.

Typische Ist-Situation

Häufig findet man in Unternehmen – insbesondere durch die schwache personelle Ressourcenversorgung im administrativen Umfeld und die große Anzahl von Systemen (Test/Integration, Qualitätssicherung, Produktion für Classic und HR getrennt, ggf. IS-Module getrennt, jeweils mit eigenen Basis-Komponenten etc.) – eine mehr „kreative“ (d.h. unstrukturierte, undokumentierte, vorgabenlose und verfahrensablauftechnisch unzureichende) Berechtigungsverwaltung vor, die oft gipfelt in einer Vielzahl von Verwaltungsobjekten, d.h.

- mehrere tausend Aktivitätsgruppen
- mehrere tausend Profile
- geringfügige Anzahl von genutzten Sammelprofilen
- mehrere zehntausend Zuweisungen von Profilen zur Gesamt-SAP-Nutzer-Zahl.

Ein typisches Beispiel für die Abbildung in einem Unternehmen zeigt die folgende Darstellung:

Betrachtungsgegenstand	Anzahl z.B.
SAP-Nutzer	(pro) 1.000
Aktivitätsgruppen	ca. 2.000 - 2.500
Profile	ca. 2.500 - 3.000
Profilzuweisungen zu SAP-Nutzern	ca. 120.000
kaum Nutzung von Sammelprofilen als Strukturgeber	
Profile/AktGr werden über Profilgenerator erstellt	
kaum Pflege der Texte zu Profilen und Aktivitätsgruppen	
Differenz AktGr. zu Profilen über Direktzuweisung	
somit durchschnittliche Anzahl von Profilen pro SAP-Nutzer	etwa 120

Tab. 3: Zahlenbeispiel - Typisches Ist in einem Unternehmen

Eine derartige Ist-Situation führt zu erheblichen Fehlerquellen in den Verfahrensabläufen der SAP-Berechtigungsvergabe. **Welche Gründe führen aber zu einer solchen Ausgestaltung ?**

Häufige konzeptionelle Schwächen

Kleinstprofile

Profile sollten wie oben erwähnt als Arbeitsschritt- oder Tätigkeitsabbildung der Mitarbeiter in SAP gesehen werden. Hier sind die notwendigen Berechtigungsobjekt- und Transaktionscodeeingrenzungen vollständig enthalten.

Es ist jedoch oftmals feststellbar, dass Profile jeweils als „Kleinstprofil“ definiert werden, d.h. sie beinhalten lediglich wenige Berechtigungsobjekte mit einer bestimmten Ausprägung (z.B. Modul CO: Bestimmte Ausprägung in K_VRGNG [erlaubte Vorgänge in der Kostenrechnung, Ist-Buchung, Verrechnung] zusammen mit einer Transaktionscodezuweisung in S_TCODE). Dieses modulübergreifende **Zerstückeln von zusammengehörigen Berechtigungsobjekten** zu den vorgenannten Kleinstprofilen führt dazu, dass oftmals **redundante Profile** definiert werden. Die häufige Erklärung lautet, dass der zuständige Moduladministrator für eine im Fachbereichsinteresse liegende schnelle Lösung zu sorgen hat. Also wird das benötigte Delta ermittelt, ein Profil hieraus generiert und dem Mitarbeiter zugewiesen. Dass ggf. ein solches Profil oder eines mit einer minimalen Variation bereits existiert, konnte er dann in der Zeit nicht erkennen. Somit erfolgt fast ausschließlich eine Orientierung der Profildefinition an den SAP-Objekten und nicht an Aufgabenabbildungen.

Diese Kleinstprofile führen dazu, **dass Mitarbeiter Berechtigungen über eine Vielzahl von Profilen und damit über eine redundante Berechtigungsobjektzuweisung erhalten**, die beispielsweise den Entzug einer Berechtigung (z.B. bei Wechsel des Mitarbeiters in einen anderen Fachbereich) massiv erschweren, da erst ermittelt werden muss, welche Profile die Berechtigung zur Verfügung stellen. Zu beachten ist, dass die umfangreichste Berechtigungsobjekteingrenzung in den zugewiesenen Profilen des Mitarbeiters die Berechtigung definiert, gleichgültig, aus welchen Profilen sie stammt. So erhält ein Mitarbeiter eine Berechtigungsobjektzuweisung in Variationen über zwischen zwei und mehr als zehn Zuweisungen. Als Beispiel wird der folgende Block dargestellt (tatsächlich vorgefundenes Ist in einem Unternehmen).

Beispiel einer extremen Minimierung einer Profildefinition – buchungskreisabhängige Trennung:

F_BKPF_BUK	Buchhaltungsbelege	Berechtigung auf Buchungskreise
ACTVT	03	Anzeigen
BUKRS	0100	

Diese Ausgestaltung ist in **neun** Profilen definiert. Sie werden mit anderen Profilen in Kombination vergeben, die dann die entsprechend anderen F_BKPF-Berechtigungsobjekte beinhalten. Die Beschreibung dieser neun Profile sieht wie folgt aus:

FI Beleg Anzeigen Buchungskreis 0100
FI Dauerbeleg Anzeigen Buchungskreis 0100
FI Debitoren Konto Posten anzeigen Buchungskreis 0100
FI Debitoren Konto Salden anzeigen Buchungskreis 0100
FI Konto Posten anzeigen Buchungskreis 0100
FI Konto Salden anzeigen Buchungskreis 0100
FI Musterbeleg Anzeigen Buchungskreis 0100
FI Vorerfasste Belege Anzeigen Buchungskreis 0100
MM Rechnungsprüfung anzeigen Buchungskreis 0100

In etwa der selben Anzahl bestehen Profile, die beim Berechtigungsobjekt F_BKPF_BUK die Ausgestaltung ACTVT 03 (Anzeige) und BUKRS * (alle Buchungskreise) bzw. wiederum in etwa der selben Anzahl Profile mit der Ausgestaltung ACTVT 01,02,03,06,08,77 (Hinzufügen, Ändern, Anzeigen, Löschen, Änderungsbelege anzeigen, Vorerfassen) und BUKRS 0100 aufweisen.

Kombinationsprofil

Sofern solche wie zuvor dargestellten Profile in einer hohen Anzahl und in einer solchen Minimalausprägung in allen Modulen vorhanden sind, dienen sie als **Kombinationsprofile**. Sie definieren also allein nicht zwangsläufig eine kritische Ausprägung, können jedoch im Zusammenspiel mit anderen Profilen kritische Ausprägungen beinhalten. Insofern ist eine Prüfung von kritischen Ausprägungen hier ausgesprochen schwierig, da ja erst das Zusammenspiel mehrerer Berechtigungsobjekte mit einer jeweils bestimmten Ausprägung, ggf. zusätzlich mit einem Transaktionscode, kritische Ausprägungen darstellen.

Profilname	Berechtigungsobjekt	Aktivität	KoKrs	Vorgang CO
T-67011111	K_VRGNG	02	0100	RKL, RKLÜ
keine weiteren Berechtigungsobjekte				CO-Leistungsverrechnung
oder		Aktivität	WERKS	
T-67022222	M_MRES_WWA	01,02,06	*	Reservierung .anl./änd./löschen
keine weiteren Berechtigungsobjekte				alle Org.-ebenen Werk

Tab. 4: Beispiele für Profile mit nur einem Berechtigungsobjekt, oftmals redundant vorhanden

Für den Revisor ist immer wichtig zu erfahren, aus welchen Quellen kritische Berechtigungen stammen. Die Abfrage im AIS (SECR) „Zeige alle Profile, die eine bestimmte Berechtigungsobjekt-kombination [mehrerer Objekte] beinhalten“ führt zu einem fehlerhaftem Ergebnis, da nur die Profile gezeigt werden, die die gesamte Ausgestaltung aufweisen. Er kann somit nur nach den Mitarbeitern dieser Kombination suchen und muss sich mühsam an die beteiligten Profile „herantasten“.

Bei einer solchen Vergabe ist die Kombinationsmöglichkeit dieser Profile derart hoch, dass das Identifizieren der Schwachstellen und somit das Eindämmen von kritischen Berechtigungen mit einem unverhältnismäßig hohen Aufwand verbunden ist. Das hier dargestellte Aufblähen der Profillandschaft (ein nahezu identisches Bild wird auch bei den Aktivitätsgruppen geliefert, da alle hier aufgeführten Profile über den Profilgenerator aufgebaut wurden und entsprechende Aktivitätsgruppenzuweisungen aufweisen) führt im Laufe der Zeit zur vollständigen Intransparenz, da eine Prüfung zur Bereinigung nicht mehr möglich ist - **Redundanz ist normal und aufgrund der Komplexität kaum noch zu verhindern.**

Konsequenz des Ansatzes

Der vorgenannte Ansatz verleitet dazu, dass Berechtigungsdeltas schnell und unkompliziert eingespeist werden. So entsteht ein nahezu 1:1-Verhältnis zwischen Profilen und Aktivitätsgruppen bei einer unverhältnismäßig hohen Anzahl dieser Elemente. Der Struktureffekt geht verloren. An seine Stelle tritt jedoch ein anderer, der die Konsequenz der vorgenannten Punkte beschreibt: Mitarbeiter erhalten trotz nahezu identischer Aufgaben keine identischen Berechtigungszuweisungen. Im Laufe der Zeit ergibt sich eine „**Individualisierung der Berechtigungsvergabe**“. Diese führt letztlich zu mehr Aufwand bei der Beantragung für neue Mitarbeiter durch den Fachbereich, bei der Administration, und natürlich auch bei der Prüfung. Der Grundgedanke, Berechtigungsstandards zu bilden und Deltas nur in geringer Anzahl zuzulassen, ist so nicht durchzuhalten.

Zwei Möglichkeiten der Ausgestaltung

Erkennbar ist, dass die Ausgestaltung der Berechtigungskonzeption mit einer überwiegenden Orientierung an den SAP-Objekten (mitarbeiterabhängige Delta-Ermittlung und -Zuweisung) nicht zwangsläufig sinnvoll ist, d.h. eine betriebswirtschaftliche Funktionsorientierung ist hierdurch vor dem Hintergrund der Beurteilungskriterien nicht abbildbar.

Die nachfolgenden beiden Gestaltungsmöglichkeiten bieten Chancen zur Bereinigung der vorgenannten Schwächen. Es sind die beiden meistgenutzten Ansätze zur Implementierung eines Berechtigungskonzeptes.

Aufgaben-/Funktionsbezogene Gruppierung

Die aufgaben-/funktionsbezogene Gruppierung stellt die aus den Arbeitsplatzbeschreibungen abgeleiteten Aufgaben in den Vordergrund und lagert diese als SAP-Abbild identifizierten Beschreibungen in Profile aus. Auf Aktivitätsgruppenebene werden diese Aufgaben zusammengefasst und als Stellen- oder Funktionsbeschreibungen abgelegt. Der Vorteil hierbei ist, dass Profile als Abbild von Aufgaben diese vollständig definieren und fachbereichsübergreifend genutzt werden können. Sammelprofile können als Sammler/Bündelungen von Aufgabenabbildungen flankierend wirken.

Beispiel:

Der Einkäufer als zentrale Beschaffungsinstantz muss in seinem Arbeitsumfeld eine Vielzahl an Aufgaben/Tätigkeiten ausführen, so z.B. die folgenden:

- | | |
|------------------------------------|--|
| - Anfragen anlegen/ändern | alleinige Funktion des Einkäufers |
| - Anfragen anzeigen | verwendbar auch in anderen Fachbereichen |
| - Bestellungen anlegen/ändern | alleinige Funktion des Einkäufers |
| - Bestellungen anzeigen | verwendbar auch in anderen Fachbereichen |
| - Rahmenverträge anlegen/ändern | alleinige Funktion des Einkäufers |
| - Rahmenverträge anzeigen | verwendbar auch in anderen Fachbereichen |
| - Buchhaltungsbelege anzeigen etc. | verwendbar auch in anderen Fachbereichen |

Diese Tätigkeiten sind eindeutig zu identifizieren und auch eine Abbildung der SAP-Funktionalität ist möglich. Notwendig ist die Definition der Aufgabenabdeckung auf Profilebene, die sowohl die Eingrenzung der Berechtigungsobjekte als auch der Transaktionen bedeutet.

Beispiel Bestellung anzeigen:

Profildefinition:

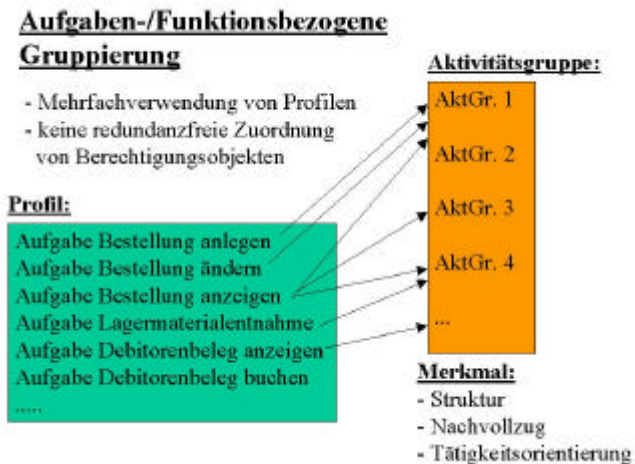
<u>Berechtigungsobjekt</u>	<u>Steuerungsfelder</u>	<u>Eingrenzung</u>
M_BEST_BSA	ACTVT / BSART	03 / *
M_BEST_EKO	ACTVT / EKORG	03 / *
M_BEST_EKG	ACTVT / EKGRP	03 / *
M_BEST_WRK	ACTVT / WERKS	03 / *
S_TCODE	TCD	ME23 u.a.

Hier sind alle zusammengehörigen Berechtigungsobjekte auch gemeinsam definiert. Ein solches Profil kann auch in anderen Bereichen als Einzelaufgabeabbildung genutzt werden, so dass redundante Profile nicht entstehen sollten.

Vorteile	Nachteile
Eindeutige Aufgabenbeschreibungen und Abbild in SAP möglich	<u>Redundante</u> Berechtigungsobjektzuweisungen über mehrere Profile
Bausteinsystem ermöglicht Verwendung der Profile fachbereichsübergreifend; sehr strukturiert gut umsetzbar in Unternehmen kleiner und mittlerer Größe	Notwendig ist die vollständige Identifikation und Analyse der Aufgaben bei den Mitarbeitern und Abbildung in SAP => kaum leistbar ab einer bestimmten Mitarbeiter- und Aufgabenanzahl (Funktionstrennungsprinzip)
Identifikation der Profile schnell möglich, Sammelprofile können optimierend wirken	Analyse der beteiligten Berechtigungsobjekte pro Transaktion, adaptiert auf die Aufgabenbeschreibungen => langwieriger Prozess
Zuweisung und Entzug von Funktionalität schnell und unkompliziert	Keine Reduzierung der Profilanzahl, ergibt zwar Struktur und ggf. Übersicht, ist jedoch zunehmend kaum administrier- und prüfbar

Tab. 5: Vor- und Nachteile der aufgaben-/funktionsbezogenen Gruppierung

Darstellung des Berechtigungskonzeptansatzes:



Ein entscheidender Nachteil ist hiermit verbunden, der hier nochmals herausgestellt werden muss. Der Ansatz der aufgaben-/funktionsbezogenen Gruppierung ist nur dort denkbar, wo die Anzahl genau abgegrenzter Aufgaben überschaubar und feststellbar ist, woraus sich wiederum klare Berechtigungseingrenzungen ableiten lassen, d.h. wo die Abbildung der Aufgaben/Tätigkeiten in SAP-Funktionen/Berechtigungsobjekte und den entsprechenden Steuerungsfeldereingrenzungen nebst Transaktionscodes unkompliziert erfolgen kann. Vor allem aber muss diese Abgrenzung von jemandem durchgeführt werden.

Die Aufgabe der genauen Tätigkeitsanalyse der Stellen liegt zwar grundsätzlich im Interesse aller Fachbereiche, wird jedoch im Vorfeld der Berechtigungskonzeption kaum ausreichend durchgeführt. Eine genaue Aufgabenbeschreibung der Fachbereichsmitarbeiter und hieran gespiegelt die Abbildung der Aufgaben in SAP-Funktionalität ist ein schwieriger und langwieriger Prozess. Diesem entziehen sich die Fachbereiche mangels Kapazität und Fachkompetenz sehr häufig. Eine Standardisierung erfolgt somit meist über den Berater oder den IT-Dienstleister selbst - beide mit zu wenig Sachkompetenz in den Prozessen ausgestattet, um die Konsequenzen einer Definition für die Mitarbeiter in den Fachbereichen abzuschätzen – „quick&dirty“-Lösungen wird wieder Vorschub geleistet, **die Anzahl der Profile wird nicht geringer**. Der theoretische Ansatz ist m.E. positiv zu sehen, Erfahrungen haben jedoch gezeigt, dass er langfristig nicht durchzuhalten ist – zumindest nicht in größeren Unternehmen. Die Beurteilungskriterien werden bei hohem Gefahrenpotential nur bedingt erfüllt.

Stellenbezogene Gruppierung auf Profilebene

Eine Alternative bietet die stellenbezogene Gruppierung auf Profilebene. Dieser Ansatz stellt das Profil – wie dies in vielen Unternehmen der Fall ist – in den Vordergrund als höchstes Ordnungskriterium. Die Aktivitätsgruppe wird nur als Beschreibungselement genutzt. Das Entscheidende an diesem Ansatz ist, **auf Profilebene eine komplette Stelle** mit allen Aufgaben/Tätigkeiten/Funktionen **abzubilden** und so für eine Standardisierung zu sorgen. Definiert wird ein zentrales Stellenprofil, welches unterstützt wird durch wenige Zusatzprofile, die lediglich customizing-abhängige Zusätze beinhalten. So werden beispielsweise zusätzliche buchungskreis- und kostenrechnungskreisabhängige Komponenten über Zusatzprofile bereitgestellt.

Beispiel „zentraler Einkaufssachbearbeiter“:

Profildefinition:

Im Profil finden sich modulübergreifend und redundanzfrei ca. 150 Berechtigungsobjekte nebst Steuerungsfeldereingrenzung wieder, die alle Zugriffsdefinitionen dieser Stelle abbilden. In Zusatz-

profilen werden z.B. buchungskreisabhängige Berechtigungsobjekte in die Gesamtberechtigung integriert.

...

F_BKPF_BED	ACTVT	03	BRGRU	*
F_BKPF_BEK	ACTVT	03	BRGRU	*
F_BKPF_BES	ACTVT	03	BRGRU	*
F_BKPF_BLA	ACTVT	03,08	BRGRU	*
F_BKPF_BUK	ACTVT	03,08	BUKRS	0100
F_BKPF_BUP	BRGRU	*		
F_BKPF_GSB	ACTVT	03	GSBER	*
F_BKPF_KOA	ACTVT	03	KOART	*
F_LFA1_AEN	VGRUP	*		
F_LFA1_APP	ACTVT	01,02,03,05,06,08	APPKZ	M
F_SKA1_BES	ACTVT	03	BRGRU	*
F_SKA1_BUK	ACTVT	03	BUKRS	0100
F_SKA1_KTP	ACTVT	03,08	KTOPL	*
M_BEST_BSA	ACTVT	01,02,03,04,06,08,09,76	BSART	AAA-GAZ, GCA-ZZZ
M_BEST_EKG	ACTVT	01,02,03,04,06,08,09,76	EKGRP	<Einkaufsgruppe>
M_BEST_EKO	ACTVT	01,02,03,04,06,08,09,76	EKORG	<Einkaufsorganisation>
M_BEST_WRK	ACTVT	01,02,03,04,06,08,09,76	WERKS	<Werkseingrenzung>
M_RAHM_BSA	ACTVT	01,02,03,04,06,08,09	BSART	*
M_RAHM_EKG	ACTVT	01,02,03,04,06,08,09	EKGRP	<Einkaufsgruppe>
M_RAHM_EKO	ACTVT	01,02,03,04,06,08,09	EKORG	<Einkaufsorganisation>
M_RAHM_WRK	ACTVT	01,02,03,04,06,08	WERKS	<Werkseingrenzung>

....

Tab. 5: Auszug aus dem zentralen Einkäuferprofil für BUKRS 0100

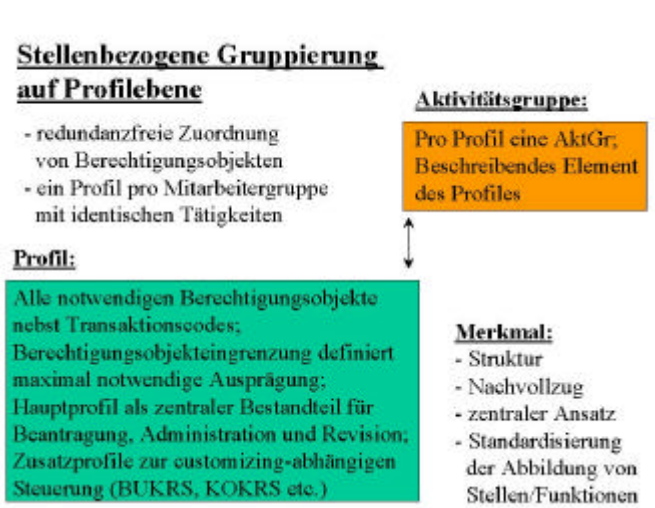
Bei diesem Ansatz überwiegen die Vorteile sowohl für den Fachbereich als auch für die Administration und die Revision.

Vorteile	Nachteile
Vollständig nutzbare Rollendefinitionen, Abgrenzung von anderen Rollen, lässt gewisses Maß an Flexibilität zu, unterbindet aber Profilwildwuchs	Administration ist modulübergreifend, d.h. die Administratoren müssen modulübergreifende Kenntnisse besitzen bzw. eng zusammenarbeiten
Bei Änderungen/Zusätzen in der Berechtigung wird das zentrale Rollenprofil angepasst und kein Zusatzprofil definiert	Es bestehen wieder in etwa so viele Aktivitätsgruppen wie Profile, aber siehe Vorteile letzter Punkt !
Redundanz in den Profil- und Berechtigungsobjektzuweisungen nur dort, wo systembedingt notwendig (z.B. K_CCA, K_VRGNG)	Sammelprofilen kommt eine eher untergeordnete Funktion zu
Berechtigungsobjekt definiert zentral im Hauptprofil der Rolle einmalig den höchsten notwendigen Berechtigungswert	Übersicht im Profil ist <u>leicht</u> eingeschränkt
Zusatzprofile nur für steuerungsfeldabhängige Komponenten (BUKRS, KOKRS, EKGRP etc.)	
Optimiertes Beantragungswesen, Fachbereich muss nur die wenigen Profile seiner Rollen und ihre Beschreibung (AktGr.) kennen	
Optimierte Administration durch geringe Anzahl an zu verwaltenden Objekten	
Bei Rollenerweiterungen schnelles und unkompliziertes Handling	
Erheblich geringere Anzahl von Profilen; in einem üblichen größeren Unternehmen dürften nur etwa 300-500 Hauptprofile entstehen	

Tab. 6: Vor- und Nachteile der stellenbezogenen Gruppierung auf Profilebene

Es wäre wünschenswert, wenn Fachbereiche ihre Funktionen/Stellen sowohl prozess- also auch tätigkeitsorientiert analysieren würden, um hieraus Tätigkeiten und bündelnde Rollen abzuleiten, die dann in SAP-Funktionalität adaptiert werden. **Entscheidend ist jedoch, dass Fachbereiche bestrebt sein müssen, Standardisierungen der Funktionsabdeckung/Aufgabenwahrnehmung zuzulassen und der Individualisierung der Berechtigungen entgegenzuwirken.** Dies schließt insbesondere auch Zugriffe im Modul CO ein. Notwendig ist also die Vermeidung der Vergabe von Rechten als Statussymbol für bestimmte Mitarbeiter und stattdessen die Rechtezuweisung nach Notwendigkeit in den Hauptprofilen für Mitarbeitergruppen mit identischen Tätigkeiten.

Darstellung des Berechtigungskonzeptansatzes:



Schlussbetrachtung

Gerade der Ansatz der stellenbezogenen Gruppierung auf Profilebene, der m.E. zu favorisieren ist, kann als das geeignete Beispiel für die Abbildung in größeren Unternehmen gesehen werden, wo Mitarbeiter keine weitgefächerten, sondern eingegrenzte und genau beschriebene Tätigkeitsabbildungen zugewiesen bekommen. Der Wildwuchs an Profilen kann hierüber eingedämmt werden.

Unter www.wildensee.de/veroeff.htm kann eine funktionstüchtige Muster-Rollendefinition eines Einkaufssachbearbeiters heruntergeladen werden, die – customizing-abhängige Einstellungen vorausgesetzt bzw. angepasst – lauffähig vorliegt.

Ausgesuchte Literatur:

- 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 ReVision III/2001 bis I/2002, Ottokar-Schreiber-Verlag, Hamburg
<http://www.osv-hamburg.de>
- Thomas Tiede SAP R/3 Ordnungsmäßigkeit und Prüfung des SAP-Systems (OPSAP) 2000 Ottokar-Schreiber-Verlag, Hamburg
<http://www.ibs-hamburg.com>

* Unter Release 4.6 (EnjoySAP/Easy Access) hat die SAP AG vordefinierte Rollen implementiert, die unter *mySAP.com* weitergepflegt wurden. So stehen vorgefertigte Rollen zur Verfügung (Templates = Vorlagen/Schablonen), die angepasst und genutzt werden können. Unter *mySAP.com* werden Templates auch zur Steuerung benutzerspezifischer Anpassungen genutzt (rollenbasierte Personalisierung).