

SAP R/3 Berechtigungen ...

... eines der vernachlässigten Themen bei SAP Projekten.

Ein Erfahrungsbericht von Thomas Frey, **Senior Consultant** bei der **CSC Ploenzke AG**, Wiesbaden.

Fragen und Anregungen zum Dokument bitte an:

Thomas Frey
Abraham-Lincoln-Park 1
cc-eTechnology / A02

65189 Wiesbaden

Telefon: +49 (0) 611 142 21063
Mobile : +49 (0) 163 25 21 539
Email: tfrey2@csc.com

Thomas Frey
Anne-Frank-Str. 6
55232 Alzey

Mobile: +49 (0) 163 25 21 539
EMail : tfrey_az@web.de

1 Arbeitsabläufe/Prozesse und begleitende Maßnahmen für ein SAP R/3 Berechtigungskonzept

Ein Berechtigungskonzept ist nicht mit dem Erstellen der Berechtigungen auf Rollenbasis im R/3-System abgeschlossen. Die Gründe dafür sind:

In der „Vorbereitungsphase“ stellt das Projektteam die Weichen für den späteren Einsatz. Je detaillierter hier gearbeitet wird, umso einfacher, schneller und genauer können die Rollen erstellt werden. Daraus ergibt sich ein geringerer Aufwand für Nacharbeiten in der Einführung und im produktiven Betrieb.

In der „Einführungsphase“ ändern sich oft die Anforderungen. Ein Prozess läuft eben doch nicht so wie zuerst geplant. Die SAP-Benutzeradministration muss jetzt schnell auf die geänderten Anforderungen reagieren können.

Ein Unternehmen verändert sich: neue Aufgabenbereiche kommen hinzu oder fallen weg. Mitarbeiter treten ein, wechseln den Aufgabenbereich oder scheiden aus. In der „Produktionsphase“ bedarf es Regeln um diese Änderungen schnell und sicher in das Produktionssystem zu bringen.

Es gibt also viele Aufgaben ausserhalb der Arbeiten mit dem Profilgenerator. Diese müssen, nicht zuletzt im Hinblick auf die gesetzlichen Anforderungen an ein System mit Buchhaltungsrelevanz, geregelt sein.

Umfassen müssen solche Verfahren folgende Szenarien:

- Vorbereitungsphase
 - Initialanlage von Rollen, Namenskonventionen für Rollen
 - Passwortregeln
 - besonders schützenswerte Daten identifizieren
 - Regeln für Reporting, Drucken, Downloads, Tabellenzugriffe finden
 - Berechtigungen durch die Systemlandschaft
- Einführungsphase
 - Initialanlage der Benutzerstammsätze
 - Vorgehensweise bei fehlenden Berechtigungen
 - Änderung von Rollen
- Produktivphase
 - Erarbeiten einer Vorgehensweise für die spätere Benutzer- und Berechtigungsverwaltung
 - Urlaubs- und krankheitsbedingte Vertretungen
 - Meldepflicht, beim Wechsel eines Benutzers in anderes Aufgabengebiet (löschen der alten Berechtigungen, erteilen neuer Berechtigungen, Zuordnung zu einer neuen Benutzergruppe)
 - Notfallkonzept, Notfallrolle(n)
 - Einplanen von Jobs zur Überwachung von Benutzerstammsätzen bezüglich letztem Login, Abgleich von Berechtigungen

2 In der Vorbereitungsphase

2.1 Technische Arbeiten

Um den Profilgenerator zu nutzen ist im Instanzprofil der folgende Parameter zu setzen:

Auth/no_check_in_some_cases = Y

Da Änderungen an Rollen und damit verbundene Transporte in die angeschlossenen Systeme dazu führen, dass die Rollen neu generiert werden müssen, gilt dies für alle Systeme in denen der Profilgenerator genutzt wird. In der Regel für das Entwicklungs-, das Qualitätssicherungs- und das Produktivsystem

Anschließend ist ein Durchstarten des R/3-Systems notwendig.

Im Instanzprofil können auch die Einstellungen für die maximalen Anmeldeversuche, die Größe des Benutzerpuffers etc. eingestellt werden.

Eine weitere Voraussetzung ist das Generieren des spezifischen Unternehmens-Implementations-Guides (IMG).

Weitere Hinweise zu diesem Thema finden sich in den Installationsanweisungen für SAP R/3 Systeme.

2.2 Organisatorische Arbeiten

2.2.1 Initialanlage der Rollen

Nachdem die technische Vorarbeit abgeschlossen ist, oder bereits parallel dazu, ist es die Aufgabe der Projektteams und Fachabteilungen die Prozesse zu definieren. Rollen basieren idealerweise auf bestehenden Prozessen und erlauben einem Benutzer seine Aufgaben im Tagesgeschäft durchzuführen. Letztendlich bilden die Rollen die Aufgabenbeschreibungen oder Prozessabläufe ab. Hilfreich sind neben den Arbeitsablaufbeschreibungen auch die Stellenbeschreibungen der Personalabteilung.

Rollen werden in der Regel mit dem Profilgenerator angelegt. Dieses SAP-Tool vereinfacht das Erstellen von Rollen.

Wichtig: Rollen können sich in Ihren Berechtigungen überschneiden, wenn sie das gleiche Berechtigungsobjekt enthalten. Dann gilt immer die höhere Berechtigung.

2.2.2 Namenskonventionen für Rollen

Eigenerstellte Rollen dürfen nur außerhalb des SAP Namensraumes, also im kundeneigenen Namensraum liegen. Um die spätere Administration der Rollen zu vereinfachen, sollte die Namensgebung nach unternehmensspezifischen Regeln erfolgen.

2.2.3 Die Benutzer-Minimal-Berechtigungsrolle

Unabhängig von den Rollen für das Tagesgeschäft sollte jeder Benutzer über eine allgemeine Berechtigung, zum Beispiel für das Pflegen des eigenen Benutzerstammsatzes, die Anzeige von Berechtigungsproblemen oder die SAP Officefunktionen, verfügen.

Umfassen kann eine solche Rolle folgendes:

S00	Short Message
SM02	System Messages
SMX	
SO00	SAPoffice: Short Message
PPOS	Display Organizational Plan
SO01	SAPoffice: Inbox
SO02	SAPoffice: Outbox
SO03	SAPoffice: Private Folders
SO04	SAPoffice: Shared Folders
SO05	SAPoffice: Private Trash
SO06	SAPoffice: Substitution on/off
SO07	SAPoffice: Resubmission
SO10	SAPscript: Standard Texts
SO12	SAPoffice: User Master
SO13	SAPoffice: Substitute
SO15	SAPoffice: Distribution Lists
SP02	Display Output Requests
SU53	Display Check Values
SU56	Analyze User Buffer
SIN1	SAPBPT: Inbox
SWI3	Workflow Outbox
SWI7	Workflow resubmission
SWLO	Display work items for objects
SWX1	Create notification of absence
SWX2	Change notification of absence
SWX3	Display notification of absence
SWX4	Approve notification of absence
SWXF	Form Uses: Initial Screen

2.2.4 Besonders schützenswerte Daten identifizieren

Was sind besonders schützenswerte Daten? Diese Frage muss sich jedes Unternehmen stellen. In der Regel fallen Personaldaten, Rezepturen oder ähnliches darunter. Diese Daten dürfen nur eingeschränkten Benutzergruppen zugänglich sein und unterliegen somit einer strengen Berechtigungsprüfung.

2.2.5 Regeln für Reporting, Drucken, Downloads, Tabellenzugriffe erstellen

Kein Benutzer darf auf einem Produktivsystem die Berechtigung zum Starten der ABAP Workbench (Tcode SE38) haben. Diese Berechtigung kann man als verstecktes SAP_ALL ansehen, da der Benutzer damit alle Reports bearbeiten kann.

Es ist zu klären wie die Benutzer Reports ausführen dürfen. Ein Großteil von Transaktionen endet in Listaufgaben auf dem Bildschirm. Dürfen die Benutzer diese Listen drucken? Dürfen sie die Listen auf den lokalen PC laden? Ergebnisse die auf den lokalen Rechner heruntergeladen sind, können Dritten (zum Beispiel per Email) zugestellt werden.

Oder enthalten die Listen sensible Daten und sind vor einer Weiterverarbeitung zu schützen?

Das SAP R/3 System bietet vielfältige „Informationssysteme“ an, über die Standardlisten erzeugt werden können. Weiterhin besteht die Möglichkeit Reports über eigenerstellte Tcodes zu starten. Diese Tcodes können dann über Berechtigungsprüfungen im Zugriff eingeschränkt und bestimmten Rollen zugeordnet werden.

2.2.6 Passwortregeln

Es ist sinnvoll die Passwortregeln bereits in der Vorbereitungsphase zu definieren und spätestens in der Einführungsphase aktiv zu setzen. Erfolgt die Einführung erst nach einiger Zeit im Produktivbetrieb ist der Sinn dieser Regeln den Benutzern schwerer zu vermitteln.

Eventuell gibt es bereits Passwortregeln im Unternehmen, diese sind natürlich zu berücksichtigen.

Folgende Fragen sollten behandelt werden:

- Haben Sie ein Kennwortkonzept ausgearbeitet?
- Welche Mindestlänge haben die Kennwörter?
- Müssen die Benutzer ihre Kennwörter regelmäßig ändern?
- Verwenden die Systemverwalter komplexere Kennwörter?
- Verbietet Ihr Kennwortkonzept best. Zeichenkombinationen?
- Sind nicht zu benutzende Kennwörter in der Tabelle UST40 eingetragen?
- Verwenden Sie ein externes Sicherheitsprodukt mit R/3?
- Haben Sie Kennwörter der SAP Standarduser geändert?
- Überwachen Sie regelmäßig (tgl.) erfolglose Anmeldeversuche?
- Verwenden Sie das Security-Audit-Log?
- Haben Sie den Abbruch der Sitzung eingestellt?
- Haben Sie die autom. Abmeldung inaktiver Benutzer aktiviert?
- Sperren Sie Benutzer nach x erfolglosen Anmeldeversuchen?
- Hebt Ihr R/3-System Benutzersperren um Mitternacht auf?
- Überprüfen Sie das System regelmäßig auf gesperrte Benutzer?
- Verwenden Ihre Endbenutzer Bildschirmschoner m.Kennwörtern?

Weitere Hinweise hierzu finden sich auch in den Sicherheitsleitfäden Band I – III der SAP AG.

2.2.7 Berechtigungen in den verschiedenen Systemlandschaften

Hier gilt: Je produktionsnäher das System ist, umso geringer müssen die Berechtigungen für die Benutzer sein.

Das heißt: ein Benutzer kann auf einem Testsystem mehr Rechte haben, als auf einem Produktivsystem.

Customizing-Rechte, die Rechte bestimmte Tabellen zu ändern, sollten im allgemeinen nicht vergeben werden.

Das Umfeld der Entwickler, die ABAP/4 Workbench, sollte auf produktiven Systemen nur einem sehr eingeschränkten Benutzerkreis zugänglich sein. Das Starten von Reports birgt ein hohes Sicherheitsrisiko, da selbst Standardreports oft keiner geeigneten Berechtigungsprüfung unterliegen.

Dies gilt auch für die Administration der SAP Datenbanken. Das SAP R/3 Berechtigungskonzept ist an dieser Stelle ausgeschaltet. Auch diese Berechtigungen sollten nur einem kleinen, gut geschulten Benutzerkreis zugeordnet sein. Wenn es die Unternehmensgrösse erlaubt, sollte die Datenbank-Administration (im Sinne der Funktionstrennung) von der SAP-Administration getrennt sein.

Eine weitere Schwachstelle in SAP R/3 Systemen verbirgt sich hinter den „externen Betriebssystemkommandos“. Damit können über das SAP-System Betriebssystemkommandos abgesetzt werden. Ursprünglich dienten diese Kommandos dazu sich bestimmte Dateiinhalte oder ähnliches anzusehen. Natürlich können mit diesen Befehlen aber Dateien zerstört oder gelöscht werden

3 In der Einführungsphase

3.1 Initialanlage der Benutzerstammsätze

Bei einer grossen Anzahl von anzulegenden Benutzern ist es sinnvoll ein Tool zur Massenanlage einzusetzen. Eines dieser Tools ist das CATT (Computer Aided Test Tool). Dies macht insbesondere bei der Initialanlage Sinn, da Informationen aus verschiedenen Quellen in einem gemeinsamen Format vorliegen. Oft ist dies zum Beispiel in ein Excel Formular.

Möglich ist es auch, die Benutzer und Berechtigungsverknüpfungen zu den Benutzern mittels Batch Input anzulegen.

Nachdem Benutzer angelegt und mit den notwendigen Berechtigungen ausgestattet sind, können sie sich am System anmelden. Wurden die Benutzer über Massengenerierung angelegt, ist in der Regel ein gleiches Kennwort für alle vergeben. Sie müssen sich jetzt ein neues persönliches Passwort ausdenken.

Hier ist darauf zu achten, das sich ein Benutzer binnen einer Frist von 3 Tagen anmeldet. Benutzer, die dies nicht können, werden in einem ersten Schritt gesperrt und dem verantwortlichen Benutzeradministrator gemeldet. Diese Regel sollte auch für Benutzer gelten, die sich über einen Zeitraum von mehr als 30 Tagen nicht mehr am System angemeldet haben (siehe auch 4.1.4).

Änderungen am Benutzerstammsatz, wie Änderung von Adressdaten, Parametern können, bis zu einem bestimmten Grad, der Benutzer selbst durchführen. Dazu können die Transaktionen SU1 bis SU3 genutzt werden. Änderungen an Berechtigungen müssen einem Genehmigungsverfahren unterliegen und können erst nach der Genehmigung umgesetzt werden.

Sind Benutzerstammsätze zu löschen, können die Benutzerstammverantwortlichen dies veranlassen. Dabei sind, wie oben beschrieben, bestimmte Regeln einzuhalten.

3.2 Vorgehensweise bei fehlenden Berechtigungen

Erhält ein Benutzer bei der Ausführung einer Transaktion die Fehlermeldung „Sie haben keine Berechtigung für Tcode XYZ“, so kann dies verschiedene Ursachen haben:

- Erstens liegt die Transaktion nicht im Aufgabengebiet des Benutzers, somit wäre die Fehlermeldung korrekt
- Zweitens der Benutzer hat die Berechtigung zur Transaktion, die Einschränkung kann dann auf Berechtigungsobjektebene stattfinden. D.h. der Benutzer möchte Daten ändern, für die er gem. Rollendefinition nur Leseberechtigung hat. Auch hier wäre die Fehlermeldung so korrekt
- Ein weiterer Fall kann dann vorliegen, wenn die Zuordnung Rolle/User nicht korrekt ist, das heißt die Rolle ist zwar vorhanden, dem Benutzer auch zugeteilt, der Benutzerstammabgleich jedoch nicht durchgeführt. In diesem Fall genügt der einfache Abgleich im Profilgenerator
- Denkbar ist auch, das die Fehlermeldung „falsch“ ist, da der Benutzer die Berechtigung laut Rollenbeschreibung haben müsste, diese jedoch nicht in der Rolle eingebaut ist

Diese vier Möglichkeiten können wie folgt behandelt werden:

- Alle Benutzer erhalten die Möglichkeit die Transaktion SU53 (Anzeige Berechtigungsprüfung) auszuführen
- Der Benutzer mit der Fehlermeldung, wendet sich bei Auftreten der Fehlermeldung an einen für ihn zuständigen Berechtigungsadministrator. Dieser fordert ihn auf die Transaktion SU53 auszuführen
- Der Administrator ist in der Lage, die Auswertung dieser Transaktion auf seinen Bildschirm zu holen (ab Release 4.6x)
- Erkennbar ist dann welche Art der Berechtigung fehlt

Es muss nun entschieden werden, wie weiter zu verfahren ist. Dabei ist anzumerken, dass auf Grundlage der vorliegenden Daten die technische Umsetzung kein Problem darstellt. Es ist jedoch zu klären, ob die Berechtigung organisatorisch zugeordnet werden darf. Oder ob dem Mitarbeiter mitzuteilen ist, dass diese Berechtigung für ihn nicht vorgesehen ist.

Soll die Berechtigung erteilt werden, ist daran zu denken, dass die Änderung der Rolle auch für alle anderen Benutzer, welche diese Rolle zugeordnet haben, gültig ist (siehe 3.3).

Die Änderung wird in einem Entwicklungssystem durchgeführt und durchläuft anschließend den normalen Transportweg, bevor sie zugeordnet werden kann.

In „echten Notfällen“ kann dem betroffenen Benutzer natürlich eine „Notfallberechtigung“ vergeben werden. Das Thema Notfallrollen wird unter 4.2 noch näher beschrieben.

3.3 Änderung von Rollen

Änderungen an existierenden Rollen müssen einem Genehmigungsverfahren unterliegen, welches eine fachliche Prüfung der Änderungsnotwendigkeit einschliesst. Änderungen dürfen nicht dazu führen, dass die Berechtigungen über die für den Prozess definierten hinausgehen. Wäre dies der Fall muss der Antrag abgelehnt und geprüft werden, ob eine andere Rolle den Anforderungen entspricht.

Änderungen sind grundsätzlich in einem Entwicklungssystem durchzuführen, in einem Qualitätssicherungssystem zu prüfen und erst dann auf die produktiven Systeme zu transportieren. Dort stehen die Berechtigungen dann nach erfolgreichem Benutzerstammabgleich und erneutem Anmelden zur Verfügung.

Der Benutzerstammabgleich sollte als täglicher Job, am besten über Nacht, eingeplant sein. So werden abgelaufene Berechtigungen durch den Job automatisch aus dem Benutzerstammsatz entfernt. Wenn der Benutzer sich morgens anmeldet, stehen ihm die abgelaufenen Rechte nicht mehr zur Verfügung.

Dies gilt sinngemäß auch für das Löschen von Rollen.

4 In der Produktionsphase

4.1 Die Benutzer-, Berechtigungsverwaltung im Produktivbetrieb

Sinnvoll scheint das Einsetzen eines (teil)automatisierten Workflows (zum Beispiel mit SAP, oder Lotus Notes), um einen reibungslosen und schnellen Ablauf zu gewähren.

Da die Berechtigungen und die Benutzer stetigen Änderungen unterliegen, ist das Berechtigungskonzept immer wieder anzupassen.

Es stellt sich also die Frage wie man diesem Prozess begegnet. Ein Ansatz ist: Berechtigungs-, und Rollenbearbeitung nur an einer zentralen Stelle zuzulassen.

Dadurch kann gewährleistet werden, das Rollen im gleichen Stil bearbeitet werden und es ist eine stete Kontrolle vorhanden.

Die Vergabe von Berechtigungen kann dann an verschiedenen Stellen erfolgen, zum Beispiel pro Lokation, pro Modul oder ähnlich. Die Administratoren werden berechtigt diese Verknüpfungen für einen bestimmten Namensraum vorzunehmen.

Gelten kann dies auch für das Rücksetzen eines „vergessenen“ Passwortes. Natürlich erst dann, wenn der Benutzer sich entsprechend authentifiziert hat.

4.1.1 Neue Benutzer

Hier gilt: der Benutzeradministrator kann den Antrag nur dann umsetzen, wenn das entsprechende Genehmigungsverfahren durchlaufen wurde (siehe das Formular im Anhang).

Soll nur ein einzelner User angelegt werden, kann der Genehmigende durchaus einen anderen Benutzer als Referenzuser angeben.

4.1.2 Urlaubs- und krankheitsbedingte Vertretungen

Auch hier müssen im Vorfeld klare Regelungen getroffen werden. Durch Übernahme von Vertretungen können sich die Berechtigungen eines Benutzers stark verändern. Das 4-Augen-Prinzip kann so eventuell umgangen werden.

4.1.3 Meldepflicht, beim Wechsel eines Benutzers in anderes Aufgabengebiet

Wechselt ein Benutzer das Aufgabengebiet oder die Abteilung ist dies den Benutzeradministratoren mitzuteilen, da ein solcher Wechsel in der Regel Änderungen an den Berechtigungen mit sich bringt.

Scheidet ein Benutzer aus dem Unternehmen aus, sollte wie beim oben beschriebenen Vorgang „Benutzer sperren“ vorgegangen werden. Der Benutzer sollte einer Benutzergruppe zugeordnet werden, die nur die Administratoren ändern können. Sein Kennwort sollte geändert und die Berechtigungen entzogen werden.

Damit ist gewährleistet dass der Benutzer sich nicht mehr am System anmelden kann.

4.1.4 Verfahren für Benutzer die sich nicht mehr anmelden

Benutzer die sich 30 Tage nicht mehr am System angemeldet haben, werden in einem ersten Schritt gesperrt und dem verantwortlichen Benutzeradministrator gemeldet.

Benutzer die sich länger als 60 Tage nicht mehr angemeldet haben, sollten deaktiviert werden. Das bedeutet: zusätzlich zur Sperre werden die Berechtigungen entzogen. Hilfreich kann es auch sein, diese Benutzer in eine eigene Benutzergruppe zu transferieren. Dadurch können die Administratoren oder die Revisoren über das Berechtigungsinformationssystem jederzeit die aktuellen Daten einsehen.

Benutzer die mehr als 90 Tage nicht mehr am System waren können eventuell gelöscht werden. Hierbei sind jedoch die gesetzlichen Bestimmungen zur Nachvollziehbarkeit zu beachten, deren Einhaltung die Revision oder die Wirtschaftsprüfung überwacht.

4.2 Notfallkonzept, Notfallrolle(n)

Wie bereits erwähnt unterliegt die Benutzer- und Berechtigungswchsel einem stetigen Wandel. Damit dringende Arbeiten in der Produktionsphase nicht an einer fehlenden Berechtigung scheitern, sollte festgelegt sein, wie in diesen Fällen zu verfahren ist. Diese Vereinbarungen müssen es dem Berechtigungsadministrator ermöglichen schnell und möglichst zielgenau zu agieren.

Ein klares Genehmigungsverfahren für solche, in der Regel weitreichende Rollen, muss vorliegen. Die erteilten Rollen sollen nur für einen befristeten Zeitraum gültig sein, längstens bis das ursprüngliche Problem gelöst ist.

Der Profilgenerator bietet die Möglichkeit Rollen mit einem „gültig bis“ Datum zu versehen. Der nächste volle Benutzerstammabgleich entfernt diese Berechtigung dann aus dem Benutzerstammsatz.

Sinnvoll erscheint es solche Rollen je Modul anzulegen, SAP_ALL sollte in der Regel nicht vergeben werden.

Darüber hinaus muss die Benutzeradministration die erteilten „Notfallberechtigungen“ dokumentieren. Die Revision sollte die Prüfung der Notfallberechtigungen in ihren Prüfungsplan aufnehmen.

5 Anhang

R/3 Benutzerstammsatz Änderungsantrag für :			
Name	System / Mandantenummer	Entwicklung	100 200 300
Abteilung		QAS	100 200 300
		Prod	100
Antragsteller			
Antragsteller Position			
Antragsteller Telefon	Art der Änderung		
Begründung			
Genehmigung Antragsteller	_____ Unterschrift	_____ Datum	
Genehmigung Manager	_____ Unterschrift	_____ Datum	
Genehmigung Mitarbeiter	_____ Unterschrift	_____ Datum	
Genehmigung Sicherheits- beauftragter	_____ Unterschrift	_____ Datum	