SAP_Berech_1.doc

Vorgehensmodell zur Prüfung des Berechtigungswesens in einer SAP R/3™-Umgebung

Roger Odenthal

1 Vorbemerkung

Mit der Einführung von SAP R/3™ wird eine *äußerst komplex aufgebaute Softwareumgebung* in die Unternehmen geholt. Vielfach geschieht dies mit der ausdrücklichen Erwartung, daß die Installation der Software zu einer Restrukturierung von Bearbeitungsprozessen beiträgt. Hierbei werden die automatische Abwicklung von Bearbeitungsvorgängen, der beleglose Datenaustausch mit anderen Unternehmen sowie die Bearbeitung digitaler Dokumente ebenso unterstützt, wie Internetaktivitäten, die – bildlich gesprochen – z.B. den Schreibtisch des Außendienstmitarbeiters in die Geschäftsräume der Kunden verlagern.

Diese neue, prozeßorientierte Betrachtungsweise des SAP-R/3-Systems, die komplexe Integration von Verarbeitungsvorgang, Geschäftsvorfall und weitgehend automatischer Aufzeichnung der hiermit verbundenen Daten und Buchungsvorgänge, muß durch *geeignete differenziert gestaltete Berechtigungsvergabe* begleitet werden. SAP R/3™ unterstützt ein solches Berechtigungssystem. Dessen Gestaltung und Prüfung ist jedoch nach Aussage vieler Administratoren und Revisoren sehr aufwendig.

Das nachstehend näher beschriebene Vorgehensmodell zur Analyse und Beurteilung *individuell gestalteter SAP R/3™-Berechtigungssysteme* verbindet sowohl methodisches Vorgehen, als auch die praktische Erfahrung aus einer Vielzahl von Prüfungen in Unternehmen unterschiedlicher Größen und Branchen. Zur Reduzierung des mit der Prüfung verbundenen personellen Aufwandes ist es stufenförmig aufgebaut und kann an jeden gewünschten Detaillierungsgrad angepaßt werden. Es orientiert sich an risikobehafteten EDV- und Betriebsprozessen. Bei der Prüfung steht die *Funktionsfähigkeit des Internen Kontrollsystems* im Vordergrund. Ziel ist es, die SAP R/3™-unterstützten Betriebsprozesse so zu beurteilen, daß sie sowohl den formalen und gesetzlichen *Anforderungen zur Ordnungsmäßigkeit* gerecht werden, als auch die *speziellen Anforderungen* des jeweiligen *Unternehmens an ein funktionierendes IKS* sowie an Schutz und Sicherheit der Daten berücksichtigen. Auf dieser Grundlage können im Ergebnis der Prüfung Verbesserungen vorgeschlagen werden, die die Akzeptanz der administrativen Mitarbeiter, der Fachabteilungen sowie der In- und Externen Revision finden.

2 Darstellung des Vorgehensmodells

2.1 Aufnahme der Randbedingungen

Es gibt keine Vorgabe für ein „richtiges“ SAP-Berechtigungssystem. Es ist vielmehr individuell auf die zu prüfende Systemumgebung abzustimmen und muß die *jeweilige Führungsphilosophie*, von der Arbeit nach Vorgaben bei strikter Funktionstrennung, bis zur weitgehend eigenverantwortlichen, vertrauensbasierten Aufgabenerledigung berücksichtigen.

In einem ersten Schritt ist daher zunächst die zu prüfende Systemumgebung aufzunehmen. Ziel ist es, festzustellen, wie die Unternehmensstruktur innerhalb des SAP R/3™-Systems abgebildet wurde. Welche Firmen werden bebucht und welche Module genutzt? Des weiteren interessieren die in das System eingehenden Daten, einschließlich der Schnittstellen zu vor- und nachgelagerten Systemen. Der Prüfer sollte versuchen, sich einen Eindruck davon zu verschaffen, welche Funktionalitäten genutzt werden und wie manuelle Arbeitsprozesse und EDV-System miteinander verknüpft sind. Interessant sind für ihn die handelnden Personen, insbesondere aus dem EDV-administrativen Bereich, den jeweiligen Fachabteilungen und dem Beraterumfeld.

Ein Teil der notwendigen Informationen kann innerhalb des SAP™-Systems erhoben werden. Daneben sind bereits vorliegende Unterlagen, wie z.B. Organigramme und Arbeitsablaufbeschreibungen nutzbar. Wertungen und individuelle Sachverhalte werden mit Interviews aufgenommen.

Ergebnis dieser ersten kurzen Aufnahme ist eine Risikomatrix, in der EDV-bezogene Arbeitsvorgänge unter Risikogesichtspunkten eingestuft werden. Gleichzeitig werden Prüfungsstrategie und –tiefe sowie der damit verbundene Arbeitsaufwand beziffert.

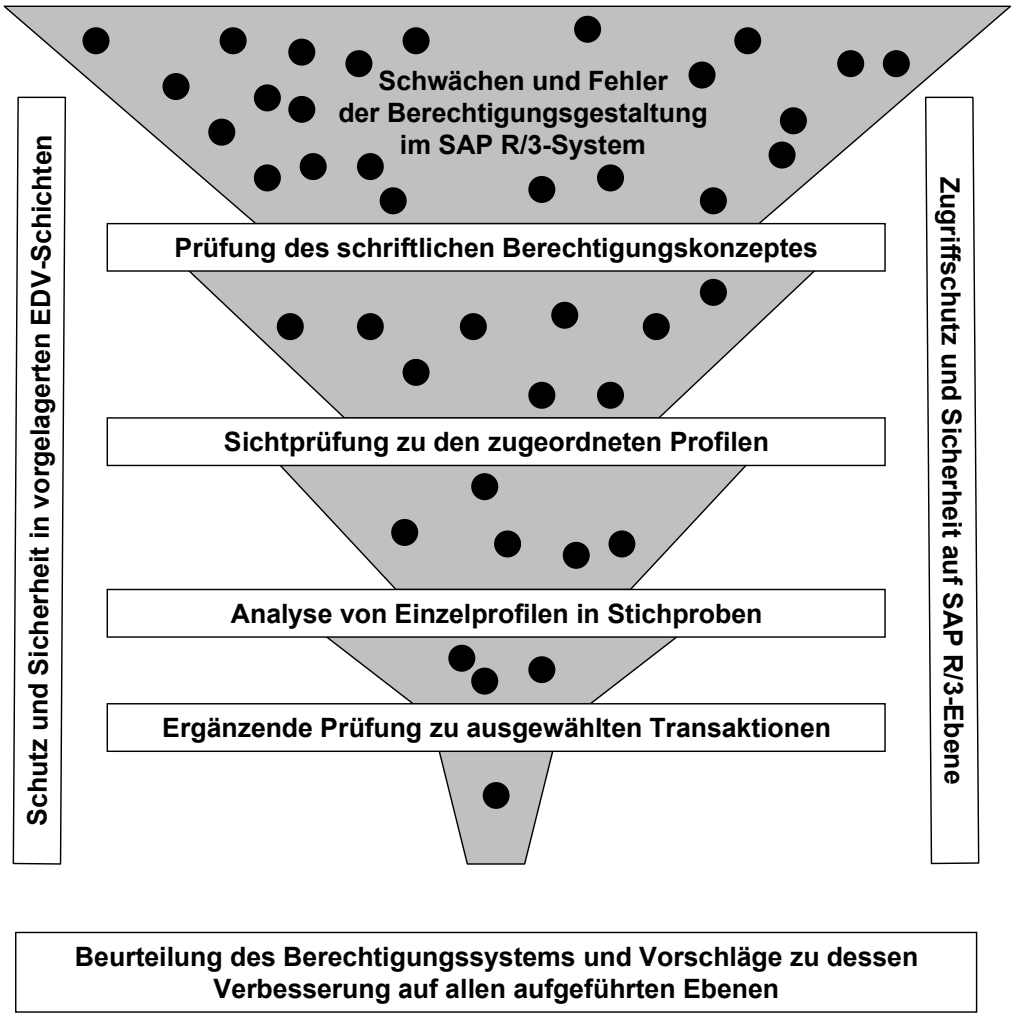

Abbildung 1 Stufenförmig aufgebautes Prüfungskonzept für ein SAP R/3™-Berechtigungssystem

2.2 Die Prüfung des Berechtigungskonzeptes

Eine einwandfreie, gedankliche Vorplanung, die sich in einem geschlossenen, klaren, widerspruchsfreien und *schriftlichen Berechtigungskonzept* dokumentiert, ist eine der notwendigen Voraussetzungen dafür, daß die Unternehmen auch nach Einführung eines SAP R/3™-Systems über ein funktionierendes IKS verfügen. Das Vorhandensein eines solchen Berechtigungskonzeptes, seine inhaltliche Ausgestaltung, die Verständlichkeit und Aktualität sind ebenso Gegenstand der Prüfung, wie dessen Umsetzung und die hiermit in Verbindung stehende Berechtigungs- und Benutzeradministration.

Ein Schutzsystem für die SAP R/3™-Software hat vielfältige Elemente, die – bevor sie in einem Berechtigungssystem abgebildet werden können – vorgedacht werden müssen. Hierzu gehören z.B.

- ❏ Tabellen, deren Zuordnung zu **Tabellengruppen** und Zugriffsberechtigungen,
- ❏ **Transaktionen** und deren Zuordnung zu Rollen (Aufbauorganisation),
- ❏ Ausführbare ABAP/4™-Programme, deren Zuordnung zu **Programmgruppen** und Zugriffsberechtigungen,
- ❏ Benutzerkennungen, deren Zuordnung zu **Benutzergruppen** und Berechtigungsadministration,
- ❏ Konten, deren Zuordnung zu **Kontengruppen** und Zugriffs- bzw. Buchungsberechtigungen,
- ❏ **Belegarten**, deren Zuordnung zu Berechtigungsgruppen und Zugriffsberechtigungen
- ❏ **Betragsberechtigungen** (für Rechnungen, Belege, Zahlungen) und deren Zuordnung zu Benutzergruppen,
- ❏ **Toleranzgrenzen** (Rechnungsabweichungen, Rundungen, etc.) und deren Zuordnung zu Benutzergruppen,
- ❏ SAP™-Objekte, wie z.B. Material, Lieferanten, etc., deren Zuordnung und **Schutzklassen** und Zugriffsberechtigungen.

Für alle Elemente **kann** ein differenzierter Schutz aufgebaut werden. Dies setzt allerdings voraus, daß man sich über die vorgenannten Mechanismen **vorab** Gedanken macht und diese bereits beim Customizing berücksichtigt. Hierzu müssen die Schutzmechanismen mit den Fachabteilungen diskutiert, geplant und abgestimmt werden. Unterbleibt dieses, so können sie später innerhalb des Berechtigungssystems nicht sinnvoll genutzt werden, mit der Folge, daß die Systemsicherheit unnötig beeinträchtigt wird.

Weiterhin ist innerhalb des Berechtigungskonzeptes festzulegen, auf welchen *Aggregationsstufen* (Arbeitsvorgang, Arbeitsplatz, Rolle des Mitarbeiters) jeweils Berechtigungen formuliert werden, bzw. mit welchem *Berechtigungsgehalt*, Berechtigungen, Profile oder Aktivitätsgruppen auszugestalten und wie diese zu *benennen* sind. Feste und bis zur letzten Stelle definierte Namenskonventionen sind nötig, damit das System prüfbar bleibt, mit vertretbarem Aufwand administriert werden kann und ausschließlich berechtigte Mitarbeiter die jeweils in ihren Arbeitsbereich fallenden Profile pflegen können.

Innerhalb des Berechtigungskonzeptes muß die Berechtigungspflege geregelt und organisatorischen Stellen zugeordnet werden. Des weiteren muß es etwas über eine *zentrale oder dezentrale Benutzeradministration* aussagen.

Das schriftliche Berechtigungskonzept ist die wesentlichste Grundlage für eine geordnete Einführung eines Berechtigungssystems und die entsprechende Administration im laufenden SAP™-Betrieb. Es ist gleichzeitig Maßstab für die Prüfung. Fehlt ein entsprechendes Konzept oder weist es wesentliche Schwächen auf, so werden sich nachfolgend zwingend Sicherheitslücken ergeben. Die Erhebungen innerhalb des Systems können sich dann auf Stichproben beschränken, um diese aus der Praxis abgeleitete Hypothese zu bestätigen.

2.3 Schutz und Sicherheit im SAP R/3™-Umfeld

2.3.1 Vorgelagerte EDV-Schichten

Schutz und Sicherheit des gesamten SAP R/3™-Systems ist nicht ausschließlich von einem funktionsfähigen internen Berechtigungssystem abhängig. Vorgelagerte EDV-Schichten, wie z.B. der *administrative (RZ-)Betrieb, die Hardware sowie Betriebssystem- und Datenbankebene* sind ebenso in die Untersuchungen einzubeziehen. Im Einzelnen umfaßt dies Fragestellungen nach:

- ❏ Funktionstrennungen im administrativen Bereich,
- ❏ Sicherheit auf Betriebssystemebene,
  - Betriebssystemnutzer
  - Dateizugriffsrechte
  - Betriebssystemsicherung
- ❏ Sicherheit auf Netzwerkebene
  - Subnetze und Router
  - kritische Netzwerkdienste
- ❏ Sicherheit der Serviceverbindungen zu SAP™,
- ❏ Sicherheit auf Datenbankebene und
  - Standard-Datenbankbenutzer
  - externe Datenbankzugriffe
  - Datenbankadministration
  - SQL-Schnittstelle
  - Datenbanksicherung
- ❏ Sicherheit der Arbeitsplatzstationen.

Die Sicherheitsüberprüfung der dem SAP™-System vorgelagerten EDV-Schichten wird durch die seitens SAP™ zur Verfügung gestellten *Prüfungs- und Sicherheitsleitfäden* unterstützt. Da es sich um einen sehr technisch orientierten Prüfungsteil handelt, sollte ein EDV-Spezialist in die Ausführung einbezogen werden.

2.3.2 Zugriffschutz auf der SAP R/3™-Ebene

2.3.2.1 Analyse der Login-Parameter

Das R/3-System bietet die Möglichkeit, in der Login-Parametern Sicherheitseinstellungen zu definieren, die dem jeweiligen Kunden und seinen Bedürfnissen angemessen erscheinen. Die SAP™-Standardeinstellungen sind erfahrungsgemäß völlig unzureichend, um vor unberechtigten Zugriffen zu schützen. Dieser Teil der Prüfung setzt sich mit den entsprechenden Parametern auseinander und untersucht, inwieweit z.B. die Paßwortlänge, das Änderungsintervall, die Benutzersperre bzw. das zwangsweise Abmelden inaktiver Anwender genutzt werden, um das System vor unbefugtem Zugriff zu schützen. Darüber hinaus wird festgestellt, ob durch eine Spezifikation verbotener Paßwörter und deren Hinterlegung im SAP™-System (Tabelle USR40) eine zusätzliche Schutzmöglichkeit genutzt wird.

Systemparameter	Bedeutung	SAP Standardeinstellungen
login/fails_to_session_end	Fehlerhafte Anmeldeversuche	3 Versuche
login/fails_to_user_lock	Anwendersperre	12 Versuche
rdisp/gui_auto_logout	Bildschirmabdeckung	Nicht aktiviert
login/min_paßwortlng	Paßwortlänge	3 Stellen
login/paßwort_expiration_time	Verfallzeit des Paßwortes	Nicht aktiviert

Abbildung 2 SAP™-Login-Parameter und deren Standardeinstellungen

2.3.2.2 Absicherung der Standardbenutzer

Bei der Installation eines neuen SAP™-Systems werden Standardbenutzer wie z.B. SAP™*, DDIC, SAPCPIC und EARLYWATCH™ mit weithin bekannten Paßwörtern und umfangreichen Zugangsberechtigungen angelegt. Im Rahmen der Prüfung ist, z.B. über den Report RSUSR003, zu ermitteln, ob die Standardbenutzer so geschützt sind, daß ein unberechtigtes Arbeiten über diese Nutzerkennungen verhindert wird und ob diese ausschließlich über einen adäquaten Berechtigungsumfang verfügen.

2.3.2.3 Kritische Nutzerkennungen

Durch eine Reihe technisch und organisatorisch bedingter Umstände können unternehmenseigene Nutzerkennungen selbst zu Schwachstellen werden, die ein unerlaubtes Eindringen begünstigen oder die Nachvollziehbarkeit bestimmter Handlungen erschweren. Im einzelnen handelt es sich um:

- ❏ noch nie angemeldete Anwender,
- ❏ lange inaktive Anwender,
- ❏ Gruppenkennungen,
- ❏ Notfallnutzer,

die mit Hilfe des *Berechtigungs-Infosystems* einer kritischen Sichtung unterzogen werden müssen.

2.4 Die Prüfung des Berechtigungssystems

2.4.1 Vorbemerkung

Mit der Prüfung des Berechtigungssystems wird innerhalb von SAP R/3™ analysiert, wie die gedanklichen Vorgaben des Berechtigungskonzeptes in der "lebenden“ Installation umgesetzt wurden. Werden die vereinbarten Vorgaben eingehalten und verfügen die zuständigen Mitarbeiter jeweils ausschließlich über einen adäquaten Berechtigungsumfang? Gibt es Schwachpunkte oder Risiken innerhalb einzelner Profile? Kommt es nach der Zuordnung von Profilen zu Nutzerkennungen, zu Funktionshäufungen, die Schutz, Sicherheit und Ordnungsmäßigkeit gefährden? Welche Alternativen können bei nicht möglicher Funktionstrennung systemseitig oder durch zusätzliche organisatorische Maßnahmen aktiviert werden, um die hieraus resultierenden Gefahren einzugrenzen?

Diese und ähnliche Fragestellungen sind Gegenstand der nachstehend näher erläuterten Untersuchung.

2.4.2 Anwenderstammsätze und zugeordnete Profile

Die angelegten Benutzerstammsätze sowie die dort zugeordneten Einzel- und Sammelprofile werden einer ersten Sichtungsprüfung unterzogen. Hierbei soll festgestellt werden, ob

- ❏ kritische Standardsystemprofile mit Super-, Administrations- und Entwicklungsberechtigung ausschließlich dem sehr engen Kreis der Administratoren vorbehalten bleiben,
- ❏ keine fachlichen Standardprofile, z.B. aus dem Finanzwesen, die Grundsätze eines funktionierenden IKS nicht berücksichtigen, verwendet werden,
- ❏ eigenentwickelte Profile mit ihrer jeweiligen Bezeichnung den Namenskonventionen des Berechtigungskonzeptes entsprechen,
- ❏ den Benutzerkennungen zugeordnete Profile mit der zu erfüllenden Funktion/Benutzergruppe vereinbar sind,
- ❏ die Zuordnung „unvereinbarer“ Profile zu Funktionshäufungen führt.

Werden an dieser Stelle bereits schwerwiegende Schwachstellen oder Abweichungen von dem vorliegenden schriftlichen Konzept festgestellt, so ist zu überlegen, ob nachfolgend näher beschriebene Prüfungshandlungen noch durchgeführt werden müssen, um eine zuverlässige Aussage über Schutz und Sicherheit der Systemumgebung zu ermöglichen.

2.4.3 Inhaltliche Analyse ausgewählter Einzelprofile

Die inhaltliche Analyse ausgewählter Einzelprofile kann – je nach dem, ob ein Berechtigungskonzept vorliegt und die vorstehend beschriebene Sichtung keine wesentlichen Abweichungen von diesem Konzept ergeben hat – *in Stichproben* erfolgen. Hierbei werden Profile entweder in einem Zufallsverfahren oder entsprechend ihrer Kritikalität ausgewählt und einer analytischen Sichtung unterzogen. Der Revisor sollte feststellen, ob ein beschriebenes Profil tatsächlich den aufgeführten Inhalt hat und ob es sich bei Heranziehung der gesetzlichen Grundlagen zu Schutz und Ordnungsmäßigkeit der Daten ein aus seiner Sicht unangemessener Berechtigungsumfang ergibt.

Die analytische Sichtung der einzelnen Profile ist zeitaufwendig. Sie gibt aber einen sehr zuverlässigen Hinweis darauf, ob das beschriebene *System der Berechtigungsgestaltung und –vergabe* eingehalten wird. Zeigen sich bei einer hinreichend großen Stichprobe keine wesentlichen Abweichungen oder problematische Tatbestände, so kann zuverlässig davon ausgegangen werden, daß das Berechtigungssystem funktioniert. Im Einzelfall besteht bei den nicht in die Stichprobe aufgenommenen Profilen weiterhin die Gefahr eines kritischen Berechtigungsumfanges, das Risiko bleibt jedoch überschaubar. Je nach Art und Umfang der festgestellten Abweichungen von dem Berechtigungskonzept muß der Stichprobenumfang für eine zuverlässige Aussage erhöht werden. Im Zweifel kann, mit erhöhtem Aufwand, eine *detaillierte Analyse aller Profile*, z.B. der Finanzbuchhaltung vorgenommen werden.

2.4.4 Ergänzende Prüfung zu ausgewählten Transaktionen

Das durch die Stichprobenprüfung verbleibende Restrisiko wird in einem letzten Schritt dadurch gemindert, daß festgestellt wird, ob *ausgewählte, kritische Transaktionen*, wie z.B.

- ❏ die Änderung von Debitoren- und Kreditorenstammdaten,
- ❏ das Buchen von Belegen,
- ❏ die Änderung von Bankverbindungen,
- ❏ Rechnungsprüfung und Zahlungslauf,
- ❏ die Berechtigungsadministration und
- ❏ die Benutzerverwaltung,

Nutzerkennungen oder Profilen zugeordnet sind, die diese nicht enthalten sollen. Die auf die Transaktionen gerichteten Prüfungen sind ebenfalls zeitaufwendig und sollten daher nur für einige als risikobehaftete angesehene Funktionen ausgeführt werden. Unstimmigkeiten, insbesondere in den bisher nicht analysierten Profilen fallen hiernach zuverlässig auf und führen in einem rekursiven Arbeitsschritt dazu, daß betroffene Profile noch einmal einer detaillierten Analyse unterzogen werden, um ggf. festzustellen, ob es sich um einen kurzfristig zu beseitigenden Einzelfall handelt, oder um eine bisher nicht erkannte Systemschwäche.

3 Werkzeuge für die Berechtigungsprüfung

Werkzeuge für die Berechtigungsprüfung innerhalb des SAP™-Systems finden sich an unterschiedlichsten Stellen. Zunächst ist hier das Berechtigungs-Infosystem zu nennen, welches über die Befehlsfolge

Werkzeuge / Administration / Benutzerpflege / Infosystem

aktiviert werden kann. Hier finden sich eine Vielzahl spezieller Auswertungen, die Systemschwächen aufzeigen.

Weitere Informationen finden sich in *Tabellen* (Transaktion SE16), wie z.B.

-	USR02	User-Logon-Daten	Diese Tabelle enthält u.a. die letzten Anmeldedaten des Anwenders, den Anleger und das Datum der letzten Paßwortänderung.
-	USR40	verbotene Paßwörter	Diese Tabelle nimmt triviale Paßwörter auf, die anschließend von den Anwendern nicht verwendet werden können.
-	USOBT	Zusammenhang von Transaktion und Berechtigungsobjekt	Die Einträge in dieser Tabelle vermitteln einen Eindruck davon, welche Berechtigungsobjekte im Regelfall beim Aufruf einer Transaktion geprüft werden.

Es gibt eine Reihe zusätzlicher interessanter Tabellen, z.B. zu den voreingestellten *Toleranzen* im Finanzbuchhaltungsbereich, zu den *Programm- und Tabellenklassen*, die der SAP™-Dokumentation zu entnehmen sind.

Da die Authorisationsprüfungen des SAP™-Systems innerhalb der Programme verankert sind, setzt eine zuverlässige Analyse des zur Ausführung einer Transaktion notwendigen Berechtigungsumfangs das Verfolgen einzelner Programmschritte (TRACE) voraus.[1]

Dieser technische Vorgang ist normalerweise dem EDV-administrativen Bereich vorbehalten. Es kann ggf. durch einen erfahrenen EDV-Revisor durchgeführt werden, wenn er über die hierzu notwendigen Berechtigungen verfügt.

4 Zusammenfassung

Das dargestellte Vorgehen beinhaltet sowohl die Elemente einer risikoorientierten Betrachtung, als auch einer Systemprüfung. Es entspricht somit einem zeitgemäßen prüferischen Vorgehen, sichert die Qualität für das betrachtete Unternehmen in die Zukunft und hält den hiermit verbundenen Prüfungsaufwand in Grenzen.

[1] Eine genaue Beschreibung des TRACE findet sich in dem Leitfaden des Autors zur Prüfung in einer SAP R/3™-Umgebung, der für entsprechende IIR-Seminare verwendet wird.