Sicherheitsmanagement mit SAP R/3-Systemen[1]

Vorgehensmodell zur Implementierung eines R/3-Berechtigungskonzeptes

Georg Hohnhorst

KPMG Deutsche Treuhand-Gesellschaft AG,
Wirtschaftsprüfungsgesellschaft, Am Bonneshof 35, 40474 Düsseldorf
Abteilung: Information Risk Management

Abstract: Modern business IT applications pose, due to their complexity and their integration into various business processes, several formerly unknown issues and problems. In particular, the need to ensure that the new business processes are in line with implemented software functions, arises. Appropriately defined controls need to be in place in order to protect against unauthorized modification or usage of both, critical data and sensitive programs.

This paper outlines, how a tailored authorization concept can provide support in reaching these targets. It relates to the standard ERP application SAP R/3. A framework which allows for the definition of detailed access controls within R/3 is described. In general, this paper focuses on a 10-step methodology to define and implement an authorization concept which is based on a workplace-approach to meet current security, business and legal requirements.

1 Sicherheitsmanagement für integrierte IT-Systeme

Für die Sicherheit, den Datenschutz und die Wahrung der Integrität eines jeden IT-Systems ist es von zentraler Bedeutung, Programme und Daten vor unerlaubten Zugriffen zu schützen. Um diese Zielsetzung zu erreichen, ist ein umfangreiches Sicherheitsmanagement erforderlich, auf das der folgende Beitrag am Beispiel der Standardanwendungssoftware SAP R/3 eingeht. Diese ERP-Software zeichnet sich dadurch aus, dass komplexe und funktionsübergreifende Geschäftsprozesse innerhalb eines Systems unterstützt werden. Integration ist somit ein entscheidendes Kennzeichen.

Integration bedeutet, dass ein Daten- und Transaktionsmodell der R/3-Software zugrundegelegt ist, bei dem einmal gespeicherte Daten für unterschiedlichste Prozesse nutzbar sind. Durch die Vermeidung redundanter Erfassungen können auf diese Weise positive Effizienz-, Kosten- und Zeiteffekte erzielt werden.

[1] „SAP“ und „R/3“ sind eingetragene Warenzeichen der SAP Aktiengesellschaft Systeme Anwendungen, Produkte in der Datenverarbeitung, Neurottstraße 16, D-69190 Walldorf.

Das hohe Maß an Integration bedeutet gleichsam als Kehrseite der Medaille, dass die vorgehaltenen Informationen durch die Festlegung der Zugriffsrechte auf Datenbestände präzise zu steuern sind. Die R/3-Steuerungsinstrumente stehen über die Elemente des Berechtigungskonzeptes zur Verfügung. Im Folgenden wird das Berechtigungskonzept auf Applikationsebene betrachtet, die für die Erfassung, Speicherung und (Weiter-)Verarbeitung aus betriebswirtschaftlicher Sicht entscheidend ist. Bei R/3-Installationen stehen hierzu eine Vielzahl von sogenannten Berechtigungsobjekten im Standard zur Verfügung.

2 Interne und externe Sicherheitsanforderungen

Beim Einsatz von R/3-Systemen sind sowohl unternehmensinterne als auch –externe Anforderungen abzudecken. Dabei handelt es sich regelmäßig um gleichgerichtete Sicherheitsanforderungen. Unternehmensspezifische Anforderungen können im Ausmaß in Abhängigkeit von der Sensibilität, IT-Abhängigkeit und dem Risikoszenario stark unterschiedlich sein [GGH00]. Als externe und damit rechtliche Anforderungen sind bei rechnungslegungsrelevanten Systemen deutscher Unternehmen als Mindestanforderungen die Bestimmungen gemäß

- Handelsgesetzbuch (HGB),
- Abgabenordnung (AO),
- Gesetz zur Transparenz und Kontrolle im Unternehmensbereich (KonTraG) und
- Bundesdatenschutzgesetz (BDSG)

einzuhalten. Ferner sind die „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) zu nennen. Präzisiert sind die externen Anforderungen z.B. in der IDW-Stellungnahme FAIT 1 „Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie“ [Fa01]. Der Entwurf steht bis zu seiner endgültigen Verabschiedung als Stellungnahme vom Institut der Wirtschaftsprüfer zur Rechnungslegung im Internet (http://www.idw.de) unter der Rubrik Verlautbarungen als Download-Angebot zur Verfügung.

Demnach müssen "sicher" genannte IT-Systeme als Voraussetzung für eine ordnungsmäßige Rechnungslegung bestimmte Anforderungen erfüllen. Das Berechtigungskonzept im R/3-System kann bei sachgerechter Implementierung die folgenden Anforderungen abdecken:

- Datensicherheit und Datenschutz: Logische Zugriffsschutzmaßnahmen (Passwortschutz) verhindern unberechtigte Zugriffe auf Daten und Informationen.
- Vertraulichkeit: Die Zugriffsrechte kontrollieren die Weitergabe von Daten, die von Dritten erlangte werden. Die sachgerechte Steuerung der Zugriffsrechte ist vor allem bei der Übermittlung von personenbezogenen Daten zur Gewährleistung der datenschutzrechtlichen Anforderungen von Relevanz.
- Integrität: Das Berechtigungskonzept kann hier ungewollte Änderungen und Manipulationen von Daten und Programmen verhindern. Dabei ist das Test- und Freigabeverfahren z.B. für Customizingaktivitäten durch die Vergabe restriktiver Berechtigungen in ein funktionsfähiges internes Kontrollsystem einzubinden.

- Verfügbarkeit: Die Maßnahmen, die gewährleisten, dass Hardware, Software, Daten und Informationen in angemessener Zeit funktionsfähig zur Verfügung stehen, werden durch das Berechtigungskonzept in Teilen unterstützt. So können sachgerecht definierte Zugriffsrechte verhindern, dass Daten bzw. Programme unberechtigter Weise gelöscht werden.
- Autorisierung: Die Anforderung bedeutet, dass ausschließlich Berechtigte die Rechte wahrnehmen können, die für das System definiert sind. Sie wird maßgeblich durch das Berechtigungskonzept abgedeckt.
- Authentizität: Auch diese Anforderung, dass ein Geschäftsvorfall eindeutig einem Verursacher zugeordnet werden kann, wird über das Berechtigungskonzept abgedeckt.
- Verbindlichkeit: Hierunter wird die Eigenschaft von IT-Systemen verstanden, gewollte Rechtsfolgen bindend herbeizuführen. Das Berechtigungskonzept kann hierzu einen Beitrag leisten, da durch Protokollierung der Benutzer-ID die eindeutige Zuordnung von Transaktionen zu dem Veranlasser eines Geschäftsvorfalls gegeben ist.

Des Weiteren ist es bedeutsam, dass Teile dieser Anforderungen durch ein an Funktionstrennungsgesichtpunkten ausgerichtetes Berechtigungskonzept abgedeckt und zu einem effizienten internen Kontrollsystem ergänzt werden können.

3 Zugriffsschutz-Architektur bei R/3-Systemen

Die R/3-Software beinhaltet verschiedene Instrumente zur Steuerung der logischen Zugriffe aller Anwender. Die Aufgabe des R/3-Berechtigungskonzeptes liegt einerseits darin, unzulässige Zugriffe auf R/3-Informationen sicher auszuschließen. Andererseits soll jeder Anwender nach Maßgabe seines Arbeitsplatzes auf alle benötigten Informationen ungehindert Zugriff erhalten. Als technische Elemente stehen in R/3 vor allem Rollen, Profile, Berechtigungen und Berechtigungsobjekte zur Verfügung.
Entscheidend ist, dass die Berechtigungsobjekte als Schutzmaßnahme (Schloss-Funktion) integraler Bestandteil der Software sind. Die konkrete Ausgestaltung der weiteren Elemente (Schlüssel-Funktion) ist Gegenstand der unternehmensspezifischen Implementierung des Berechtigungskonzeptes [Be00].

Für die Administration der Elemente im Berechtigungskonzept hat die SAP AG die zentrale Transaktion PFCG, den Profilgenerator, geschaffen [Si00]. Über sie werden Rollen administriert, die den Benutzern zuzuweisen sind. Die Rollen enthalten über mehrere hierarchisch verknüpfte Elemente die eigentlichen Zugriffsrechte (Berechtigungen mit Schlüssel-Funktion).

4 Zehn-Phasen-Modell zur Implementierung

Im Folgenden wird ein Modell vorgestellt, um das Berechtigungskonzept aufzubauen und sowohl organisatorisch als auch technisch im R/3-System zu implementieren.

1. Projektplanung
   In diesem ersten Projektschritt werden die zeitlichen, personellen und systemseitigen Rahmenbedingungen für das Projekt festgelegt. Ferner werden unterstützende Tools

für den weiteren Projektverlauf, das Vorgehen für das Projektcontrolling sowie die Entscheidungsprozesse innerhalb des Projekts definiert. Letztere sind ausschlaggebend, wenn Interessenkonflikte auftreten, bei denen eine Entscheidung herbeizuführen ist, ob z.B. Zugriffsrechte für Controllingreports exklusiv an die Abteilung „Controlling“ oder auch an weitere dezentrale Stellen zu vergeben sind.

2. Namenskonventionen
   In dieser Phase werden Namenskonventionen für alle Elemente erarbeitet, welche für die Steuerung der Zugriffsrechte relevant sind. Als technische Elemente sind hier vor allem Namenskonventionen für Rollen, Berechtigungen und Profile aufzubauen. Ferner sind z.B. Reports oder Tabellen zu berücksichtigen. Die Namenskonventionen sind von entscheidender Bedeutung für die Transparenz und Revisionsfähigkeit des gesamten Berechtigungskonzeptes. So kann z.B. eine ZHR*-Tabelle mit der Berechtigungsgruppe ZHR1 durch eine dokumentierte Namenskonvention verdeutlichen, dass es sich bei dieser Tabelle um eine eigenerstellte Tabelle mit hoch schützenswerten Informationen zum Modul Human Resources (HR) handelt.
3. Business-Strukturen
   Busines-Strukturen beziehen sich auf die Strukturen, welche die Unternehmensorganisation im R/3-System abbilden. Es sind z.B. die benötigten Geschäftsstrukturen Buchungskreise, Geschäftsbereiche oder Werke zu analysieren. Ferner werden in diesem Projektschritt Dateneigentümer festgelegt.
4. Analyse der Verfahrensabläufe
   Im nächsten Schritt erfolgt die Aufteilung der SAP-Funktionalitäten anhand der genutzten R/3-Module und -Komponenten. Sie können als Ausgangspunkt dienen, um anhand von Template-Rollen die kleinsten Bausteine für die Zugriffsrechte zu identifizieren.
5. Definition der Arbeitsplätze
   In diesem Projektschritt werden die Arbeitsplätze in Interviews erhoben. Je Arbeitsplatz werden ferner die benötigten Rollen aufgenommen. Diese Arbeitsplätze sind als abstrakte Arbeitsplätze zu verstehen. Sie bündeln jeweils sämtliche Zugriffsrechte für einen Funktionsträger nach dem Prinzip der Vergabe geringstmöglicher Rechte.
6. Abbildung der Berechtigungen
   In diesem Projektschritt werden die in Phase 4 gebildeten Template-Rollen aufgrund der Interviews aus der Phase 5 spezifiziert und angepasst. Hierbei sollten möglichst kleine Ausprägungen gebildet werden, was zwar zu einer Erhöhung der Rollenanzahl führt, sich aber vorteilhaft auf die Flexibilität des Gesamtsystems auswirkt.
7. Abbildung der Arbeitsplätze
   In diesem Projektschritt werden die inhaltlich erhobenen Arbeitsplätze (Phase 5) technisch im R/3-System abgebildet. Ausgangspunkt bildet eine Arbeitsplatz-Matrix, in der alle Arbeitsplätze und deren zugehörige Rechte dokumentiert sind. In der Praxis haben sich Matrizen bewährt, die extern des R/3-Systems erstellt werden und deren Informationen dann bei der technischen Implementierung im R/3-System abgebildet werden.

8. Zuordnung von Mitarbeitern zu Arbeitsplätzen
   In diesem Projektschritt wird eine Verfahrensanweisung und ein Formular für die Zuordnung von Mitarbeitern zu Arbeitsplätzen erarbeitet. Anschließend erfolgt die Zuweisung der entsprechenden Arbeitsplätze zu Mitarbeitern durch die jeweiligen Dateneigentümer.
9. Anwendertest mit Abnahme
   In diesem Projektschritt sollen die Anwender ihre neuen Berechtigungen hinsichtlich des benötigten Funktionsumfangs testen. Bei diesem Positivtest erfolgt die Abnahme, ob die Arbeitsplätze tatsächlich alle benötigen Zugriffsrechte enthalten. In einem Negativtest wird kontrolliert, ob sensible Bereiche durch das Berechtigungskonzept hinreichend geschützt sind.
10. Vorbereitung für den Produktivstart
    Das Berechtigungskonzept wird nun ohne Beeinträchtigung des Tagesgeschäfts unter Einsatz des R/3-Korrektur- und Transportwesens (KTW), auch „Transport Organizer“ genannt, in das Produktionssystem übertragen. Abschließend ist das gesamte Berechtigungskonzept als Bestandteil einer vollständigen Verfahrensdokumentation gemäß GoBS zu dokumentieren.

    Dabei hat sich eine Kombination aus konzeptioneller Darstellung (z.B. Dokumentation der Namenskonventionen) und systemseitig hinterlegter Dokumentation (z.B. Arbeitsplatzmatrix bzw. R/3-Rollenübersicht) bewährt.

5 Arbeitsplatz-Konzept

Dem dargestellten Vorgehensmodell liegt ein arbeitsplatzorientiertes Konzept zugrunde. Dabei vereinigt ein Arbeitsplatz sämtliche Zugriffsrechte, die ein Aufgabenträger für seine Arbeiten mit dem R/3-System benötigt.

Beispiel für einen Arbeitsplatz ist der „Debitorenbuchhalter im Buchungskreis 2000“. Damit werden direkt die Dimensionen deutlich, die ein Arbeitsplatz aufweist:

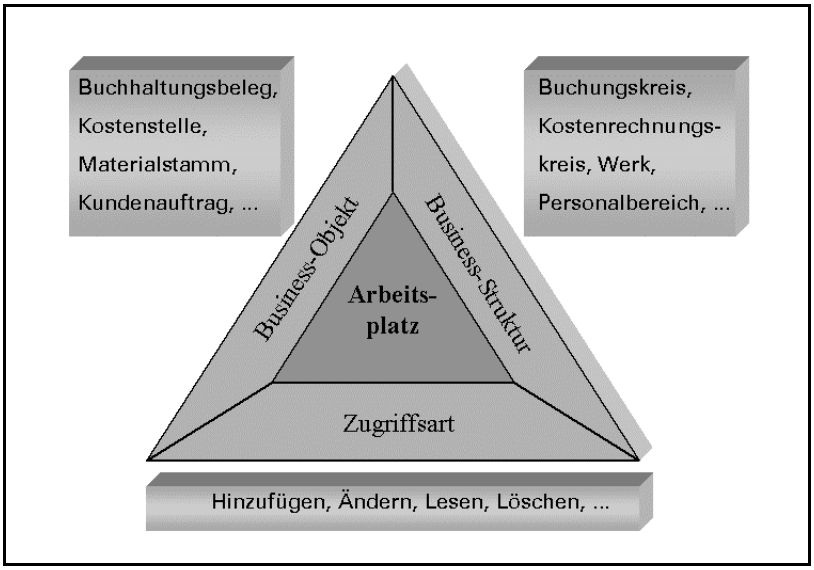
- Business-Objekte
  Hierbei handelt es sich um die zu schützenden betriebswirtschaftlichen Informationen, wie z.B. den FI-Beleg, die CO-Kostenstelle oder einen SD-Kundenauftrag. Bewusst wird hier von Business-Objekten gesprochen und nicht von Berechtigungsobjekten, da z.B. für den FI-Beleg alleine bis zu 9 Berechtigungsobjekte „zuständig“ sind.
- Business-Strukturen
  Sie bilden die Unternehmensstruktur ab und werden im Rahmen des Customizings eingestellt. Hier wird beispielhaft hinterlegt, welche Buchungskreise, Kostenrechnungskreise, Verkaufsorganisationen oder Personalbereiche genutzt werden. Die Business-Strukturen müssen stets unternehmensspezifisch im Berechtigungskonzept angegeben werden.
- Zugriffsarten
  Logische Zugriffsrechte können des Weiteren dahingehend unterteilt werden, ob lesende, schreibende, löschende usw. Rechte gewährt werden.

Für eine detaillierte Analyse der Arbeitsplätze stellt sich regelmäßig die Frage, nach welchen Kriterien die Zugriffsrechte differenziert werden können. Ein Ansatzpunkt sind die R/3-Transaktionen bzw. -Berechtigungsobjekte. Angesichts ihrer großen Zahl (ca. 45.000 Transaktionen und ca. 900 Objekt im Releasestand 4.6) ist eine alternative Herangehensweise empfehlenswert. Bei ihr wird analysiert, auf welche Business-Objekte ein Arbeitsplatz Zugriff erhalten soll. Für den Beispiel-Arbeitsplatz „Debitorenbuchhalter im Buchungskreis 2000“ sind dies primär der Beleg im Finanzwesen (FI-Beleg), der Faktura-Beleg, der Kundenstamm sowie der Materialstamm.

Je Business-Objekt wird dann aufgezeigt, welche Differenzierungsmöglichkeiten zur Verfügung stehen. Zugriffe auf den FI-Beleg können somit z.B. auf einzelne Kontoarten (Debitoren, Kreditoren und Sachkonten) beschränkt werden. Ferner stehen optionale Einschränkungen zur Verfügung, die nur bei entsprechendem Customizing von Belegarten oder Debitoren wirksam werden. In Bezug auf die Business-Struktur sind Festlegungen auf den Buchungskreis, die kleinste bilanzierungsfähige Einheit, und den Geschäftsbereich möglich.

Somit kann der Beispielarbeitsplatz auf den Buchungskreis „2000“ festgelegt werden. Schließlich stehen zu der Zugriffsart Optionen wie das Hinzufügen (=Buchen), Ändern, Anzeigen oder Löschen zur Verfügung (Bild 1).

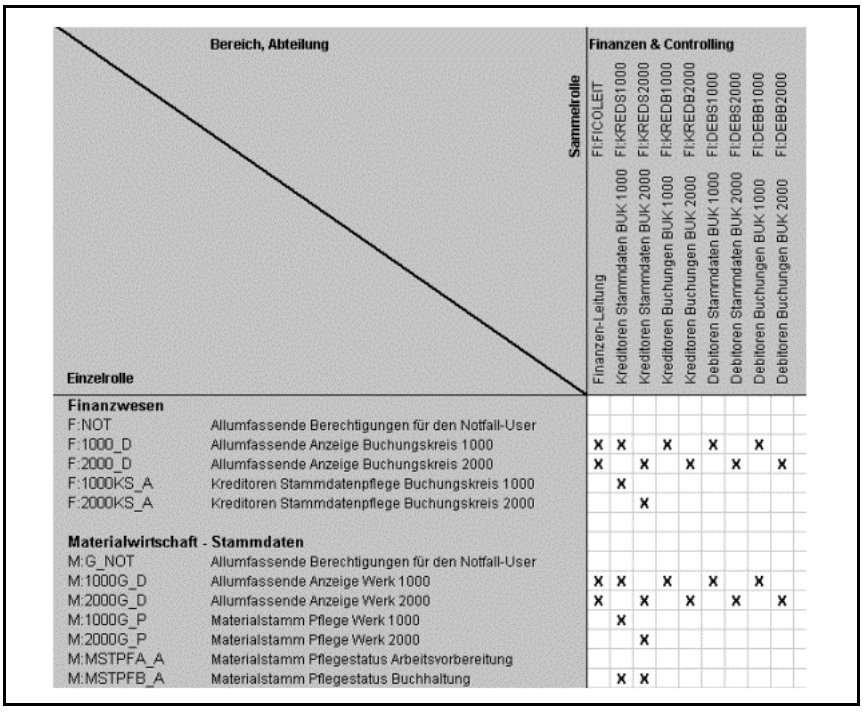
Bild 1: Differenzierungsdimensionen für Arbeitsplätze



Die Analyse auf Arbeitsplatz- und Business-Objekt-Ebene sollte der technischen Implementierung stets vorausgehen. Die bei der Analyse gewonnenen Ergebnisse erleichtert die Arbeit mit dem Profilgenerator, mit dem die Rollen im R/3-System erstellt werden. Ferner wird eine Mehrfachverwendung von Rollen unterstützt. Rollen zur Anzeige des Materialstamms werden in einem integrierten System von einer Vielzahl von Arbeitsplätzen benötigt. Sie reichen von Organisationseinheiten im Einkauf, in der Produktion, im

Lager, im Finanzwesen bis im Controlling und in der Revision. Die Transparenz kann durch die Arbeitsplatz-Matrix herbeigefügt werden, wobei Bild 2 einen exemplarischen Ausschnitt daraus darstellt.

Bild 2: Arbeitsplatzmatrix



Einzelrolle		Sammelrolle	Finanzen & Controlling								
Bereich, Abteilung			Finanzen-Leitung	Kreditoren Stammdaten BUK 1000	Kreditoren Stammdaten BUK 2000	Kreditoren Buchungen BUK 1000	Kreditoren Buchungen BUK 2000	Debitoren Stammdaten BUK 1000	Debitoren Stammdaten BUK 2000	Debitoren Buchungen BUK 1000	Debitoren Buchungen BUK 2000
			FI:FICOLEIT	FI:KREDS1000	FI:KREDS2000	FI:KREDB1000	FI:KREDB2000	FI:DEBS1000	FI:DEBS2000	FI:DEBB1000	FI:DEBB2000
Finanzwesen											
F:NOT	Allumfassende Berechtigungen für den Notfall-User										
F:1000_D	Allumfassende Anzeige Buchungskreis 1000		X	X		X		X		X	
F:2000_D	Allumfassende Anzeige Buchungskreis 2000		X		X		X		X		X
F:1000KS_A	Kreditoren Stammdatenpflege Buchungskreis 1000			X							
F:2000KS_A	Kreditoren Stammdatenpflege Buchungskreis 2000				X						
Materialwirtschaft - Stammdaten											
M:G_NOT	Allumfassende Berechtigungen für den Notfall-User										
M:1000G_D	Allumfassende Anzeige Werk 1000		X	X		X		X		X	
M:2000G_D	Allumfassende Anzeige Werk 2000		X		X		X		X		X
M:1000G_P	Materialstamm Pflege Werk 1000			X							
M:2000G_P	Materialstamm Pflege Werk 2000				X						
M:MSTPFA_A	Materialstamm Pflegestatus Arbeitsvorbereitung										
M:MSTPFB_A	Materialstamm Pflegestatus Buchhaltung			X	X						

Die Arbeitsplatz-Analyse verdeutlicht in einer weiteren Betrachtungsweise die hohe Granularität im R/3-Berechtigungskonzept. Spezifisch für das Unternehmen, dessen Prozesse und die damit verbundenen Funktionstrennungen können die Zugriffsrechte für die relevanten Business-Objekte so fein gesteuert werden, dass ein Risikomanagement softwareseitig nachhaltig unterstützt wird. Voraussetzung hierfür ist eine auch stark konzeptionell geprägte Projektarbeit zum Aufbau des Berechtigungskonzeptes, wie sie in dem Zehn-Phasen-Modell beschrieben ist. Nur so kann der Management-Überblick bezüglich der Zugriffsrechte und ein an Sicherheitsgrundsätzen ausgerichteter Systembetrieb gewährleistet werden.

6 Zusammenfassung

Die Abhängigkeit von funktionsfähigen IT-Anwendungen und zuverlässigen Datenströmen hat im Laufe der letzten Jahre – auch durch Einbeziehung von Anwendern außerhalb der Unternehmensgrenze – signifikant zugenommen. Da IT-Applikationen und die durch diese abgebildeten IT-gestützten Prozesse und Kontrollen erfahrungsgemäß einen sehr

hohen Integrations- bzw. Komplexitätsgrad aufweisen, kommt dem Sicherheitsmanagement solcher Installationen ein hoher Stellenwert zu.

Im Falle von SAP R/3 stellt diese Software Instrumente zur Verfügung, um die logischen Zugriffsrechte nach dem Prinzip der Vergabe geringstmöglicher Rechte an der Benutzer zu vergeben. Der Aufbau des entsprechenden Berechtigungskonzeptes wird durch den R/3-Profilgeneartor unterstützt.

Neben diesem für die Administration ausgerichteten Instrument bildet ein gezieltes und phasenorientiertes Vorgehensmodell den Schlüsselfaktor für die sichere und effiziente Systemnutzung. Der Arbeitsplatz als Mittelpunkt der Betrachtung hat sich dabei in zahlreichen Projekten bewährt. Nach der Aufnahme aller Arbeitsplätze und der Implementierung des Berechtigungskonzeptes bedarf letzteres auch der laufenden Pflege. Sie ergibt sich aus der Einführung neuer Geschäftsprozesse, R/3-Module oder –Releasestände.

Damit stellt das Vorgehensmodell zur Implementierung und zum Betrieb des R/3-Berechtigungskonzeptes einen erheblichen Beitrag für ein aktives Sicherheitsmanagement dar, insbesondere auch als Bestandteil des Risikomanagement- und -früherkennungssystems des Unternehmens.

Literaturverzeichnis

[Be00] Bernd-Striebeck, U. et al.: SAP-Handbuch: Sicherheit und Prüfung; praxisorientierter Revisionsleitfaden für R/3-Systeme. IDW-Verlag, Düsseldorf 2000.

[Fa01] Fachausschuss für Informationstechnologie (FAIT) des IDW: Entwurf IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW ERS FAIT 1). Die Wirtschaftsprüfung, Heft 9/2001 S. 512 ff., Düsseldorf 2001.

[GGH00] Geesmann,W.; Glauch, T.; Hohnhorst, G.: SAP R/3 Datenschutz und Sicherheitsmanagement. Ottokar Schreiber Verlag, Hamburg 2000.

[Si00] Simplification Group SAP Labs, Inc.: Authorizations Made Easy. Palo Alto USA 2000.