Ottokar R. Schreiber
Herausgeber

Liebe Leserinnen und Leser,

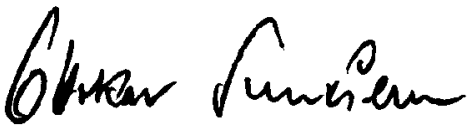
seit KonTraG und Corporate Governance sind "Risikomanagement" und "Aufbau von Früherkennungssystemen" in aller Munde. Meter an mehr oder (mehr) weniger praxisgerechter Literatur sind zwischenzeitlich entstanden, das IDW hat seine Prüfungsstandards dahingehend aktualisiert und erweitert. Die Interne Revision arbeitet seit jeher risikoorientiert; was anderes ist es denn, Risiken bzgl. der Ordnungsmäßigkeit von Prüfobjekten, d.h. Verstöße gegen Gesetze, Regelwerke, Dokumentationspflichten u.a.m. aufzudecken bzw. ihnen vorzubeugen oder Risiken bzgl. der Sicherheit von Prüfobjekten, insbesondere durch die IT-Revision im IT-Umfeld hinsichtlich Datenverlusten und unerlaubter Dateneinsichtnahmen, aufzudecken bzw. ihnen vorzubeugen oder Risiken wertmäßiger Art wie ineffiziente Arbeitsweise oder deliktische Handlungen infolge Betrug, Diebstahl und Korruption aufzudecken bzw. ihnen vorzubeugen? Für die Revision eigentlich alles nichts Neues; aber für Vorstände (!) und Aufsichtsräte (!) musste Risikomanagement aus bekannten Gründen neu thematisiert werden.

Wegen der Aktualität - und die Innenrevision agiert nun einmal im Auftrag des Vorstandes - hat sich ReVision in vorliegender Ausgabe dieses Themas wieder angenommen: in grundsätzlicher Betrachtung im Leitbeitrag "Prüfung des Risikomanagements durch die Interne Revision", in dem Sie auch eine Übersicht nebst WWW-Adressen der maßgeblichen Gesetze, Regelwerke und Prüfungsstandards zu diesem Thema zur eigenen Vertiefung finden, und in spezieller Betrachtung der Risiken und ihrer vorbeugenden Begegnung in SAP R/3®-Systemen.

Aber passen Sie auf; wahren Sie in der Implementierung Ihrer Überwachungssysteme Verhältnismäßigkeit. Denn Übertriebenheit macht Ihr Risikomanagement-System (RMS) ineffizient und ineffektiv; Übertriebenheit wird Ihr Ziel, Ihren Betrieb sicher, innovativ, schlank und flexibel zu gestalten und für alle Mitarbeiter Motivation zu bewirken, konterkarieren, wird Ihren Betrieb "abwürgen". Denn Heerscharen selbsternannter RMS-Spezialisten werden sich auf Sie stürzen (woher haben die eigentlich ihre Erfahrungen?), werden Ihnen zu horrenden Beratungskosten ein umfassendes RMS überstülpen wollen, einen Betrieb im Betrieb erzeugend. Sie als Interne Revision haben die meiste Risikoerfahrung in Ihrem Betrieb, initiieren und beraten Sie Ihr RMS-Controlling!

Viele neue Erkenntnisse und vor allem praktische Hinweise für Ihre Arbeit im Studium von ReVision wünscht Ihnen wie immer

Ihr



Ottokar R. Schreiber

Inhaltsverzeichnis

Verlagshinweis:
Nächste Ausgabe der

ReVision

Juli 2003

Redaktions-/Einsendeschluss für diese Ausgabe: 20.06.2003

ReVision

Fachjournal für Revisoren, IT-Revisoren, Wirtschaftsprüfer, Controller, IT-Sicherheits- und Datenschutzbeauftragte

Erscheinungsweise: ¼-jährlich zum Jan./Apr./Jul./Okt.

Herausgeber: Ottokar R. Schreiber

Verlag: OSV Ottokar Schreiber Verlag GmbH
Friedrich-Ebert-Damm 145, 22047 Hamburg
Fon: +49(0)40 /69 69 85 -14 Fax +49(0)40 /69 69 85 -31
eMail: sales@osv-hamburg.de
www.revision-hamburg.de

Beiträge

Für unaufgefordert eingesandte Manuskripte wird keine Haftung übernommen. Der Verlag behält sich insbesondere bei Leserbriefen das Recht der Veröffentlichung, der Modifikation und der Kürzung vor. Leserbriefe können in beliebiger Form (handschriftlich, per eMail, Fax usw.) zugesandt werden. Manuskripte sollten uns in Dateiform zugesandt werden, vorzugsweise im RTF- oder Winword-Format, Bildmaterial bitte im TIFF-Format/Auflösung 200 dpi od. JPEG 300dpi. Zur Veröffentlichung angebotene Beiträge müssen von allen Rechten Dritter frei sein. Wird ein Artikel zur Veröffentlichung akzeptiert, überträgt der Autor dem OSV das ausschließliche Verlagsrecht, das Recht zur Herstellung weiterer Auflagen und alle Rechte zur weiteren Vervielfältigung bis zum Ablauf des Urheberrechts. Wird der Artikel Dritten ebenfalls zur Veröffentlichung angeboten, muss dies dem OSV bekanntgegeben werden.

eMail: redaktion@osv-hamburg.de

Anzeigen

Zu den Konditionen rufen Sie bitte unsere aktuellen Mediadaten ab. Zur problemlosen Abwicklung und korrekten Darstellung stellen Sie uns die Anzeigen vorzugsweise als belichteten Film zur Verfügung. Sollte dies nicht möglich sein, bitten wir um Rücksprache hinsichtlich der gelieferten Dateiformate. Telefon 040 / 69 69 85 -14. Design-Erstellung auf Wunsch auch durch unsere Medienabteilung möglich.

Anzeigenleitung: Alexandra Palandrani,
Telefon 040 / 69 69 85 -14
eMail: anzeigen@osv-hamburg.de

Bestellung/Abonnement:
Alexandra Palandrani
OSV Ottokar Schreiber Verlag GmbH
eMail: sales@osv-hamburg.de

DTP-Produktion
Grafik/Illustration: Dirk Kirchner, ibs schreiber gmbh
Layout/Satz: Alexandra Palandrani, OSV Hamburg

Druck: Druckerei Zollenspieker Kollektiv GmbH
Zollenspieker Hauptdeich 54
21037 Hamburg

Printed in Germany.
Gedruckt auf chlorfrei gebleichtem Papier

Prüfung des Risikomanagements durch die Interne Revision

Von Thomas Mohnike
Revisionsleiter bei der Stadtwerke Hannover AG
und Rolf-Dieter Epkenhaus
Personalrevisor bei der Stadtwerke Hannover AG

Einleitung

Der Gesetzgeber hat auf die Schwächen im System der Unternehmenskontrolle reagiert und sah sich gezwungen, die vorhandenen Überwachungs- und Kontrollstrukturen per Gesetz einer Neuordnung zu unterziehen. Daher wurde das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich *(KonTraG)* formuliert, das am 01. Mai 1998 in Kraft getreten ist. Hiermit wurde auch die Einrichtung eines Risikofrüherkennungssystems als Organisationspflicht des Vorstandes fixiert (§ 91 Absatz 2 Aktiengesetz).

Das *KonTraG* sieht vor, dass *"der Vorstand geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten hat, damit der Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden."*

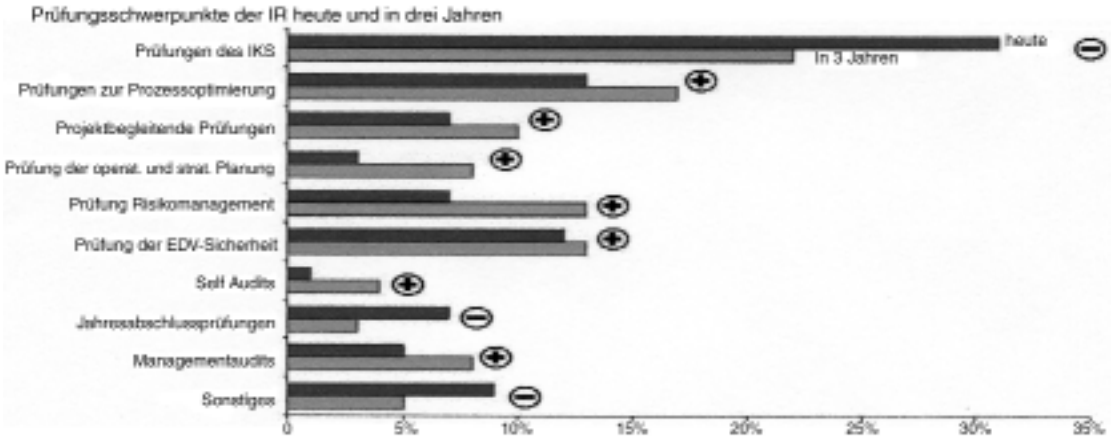
Danach sind die Unternehmen nunmehr ausdrücklich verpflichtet, für ein aktives Risikomanagement und eine angemessene Interne Revision zu sorgen.

Veränderte Rolle der Internen Revision im Unternehmen

Bis zum Jahr 2000 war die Überprüfung des Risikomanagementsystems durch die Interne Revision oder andere unabhängige Überwachungsinstanzen in der Regel noch nicht erfolgt, häufig noch nicht einmal geplant.

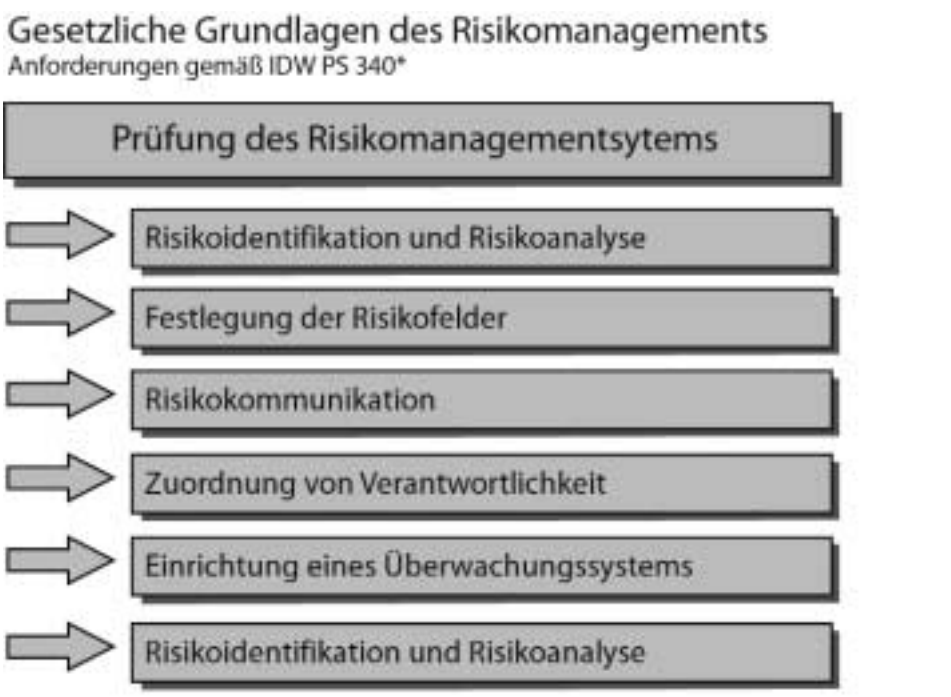
Zwischenzeitlich mussten sich aber durch zunehmende Geschwindigkeit, Kostendruck und neue Risiken nicht nur die Unternehmen verändern, sondern insbesondere auch die Interne Revision. Künftig wird sie sich nicht mehr als "Unternehmenspolizei" vergangenheitsorientiert und isoliert von Unternehmenszielen darstellen können, sondern zur Überwachung der Geschäftsrisiken beitragen, Prozesse optimieren und kundenorientiert denken und arbeiten.

Die Interne Revision prüft im Auftrag der Unternehmensleitung ganz allgemein die Ordnungsmäßigkeit, Rechtmäßigkeit, Zweckmäßigkeit und Wirtschaftlichkeit der übrigen Organisationseinheiten sowie die Abwicklung der Prozesse im Unternehmen.



Gesetzliche Grundlagen des Risikomanagements

Nach § 91 AktG ist der Vorstand zur Einrichtung eines Risikomanagement- und -überwachungssystems verpflichtet. Nach § 317 HGB ist bei einer Aktiengesellschaft, die Aktien mit amtlicher Notierung herausgegeben hat, außerdem im Rahmen der Abschlussprüfung zu beurteilen, ob der Vorstand die ihm nach § 91 Abs. 2 des AktG obliegenden Maßnahmen in einer geeigneten Form getroffen hat und das danach einzurichtende Überwachungssystem seine Aufgaben erfüllen kann.



*IDW PS 340: Prüfungsstandard (PS) des Insituts der Wirtschaftsprüfer (IDW für die Prüfung des Risikomanagement-Systems im Rahmen der Jahresabschlussprüfung

Der Deutsche Rechnungslegungsstandard Nr. 5 regelt die Grundsätze der Risikoberichterstattung für alle Mutterunternehmen, die gemäß § 315 Abs. 1 2 Hs. HGB über die Risiken der künftigen Entwicklung im Konzernlagebericht zu berichten haben und empfiehlt eine entsprechende Anwendung im Lagebericht gemäß § 289 Abs. 1 2 Hs. HGB. Der Standard ist auch anzuwenden auf die Rechnungslegung des § 292a HGB. Ziel der Risikoberichterstattung nach diesem Standard ist es, den Adressaten des Konzernlageberichts entscheidungsrelevante und verlässliche Informationen zur Verfügung zu stellen, die es ihnen ermöglichen, sich ein zutreffendes Bild über die Risiken der künftigen Entwicklung des Konzerns zu machen.

Berichtspflichtig sind alle Risiken, die die Entscheidungen der Adressaten des Konzernlageberichts beeinflussen könnten. Schwerpunkt der Berichterstattung sollten somit die mit den spezifischen Gegebenheiten des Konzerns und seiner Geschäftstätigkeit verbundenen Risiken bilden.

Auch für nicht unter die Gesetzgebung fallende Unternehmen ergibt sich dennoch die Notwendigkeit, sich intensiv mit dem Thema auseinander zu setzen und ein funktionierendes Risikomanagementsystem auszugestalten - zum einen durch die Ausstrahlungswirkung der gesetzlichen Entwicklungen auf den Pflichtenrahmen der Geschäftsführer und ggf. Aufsichtsräte anderer Gesellschaftsformen (Sorgfaltspflicht, Möglichkeit der Exkulpation), zum anderebvor allem aber aus originär betriebswirtschaftlichen Gründen (z.B. als integrierter Bestandteil der Unternehmensführung und als Kriterium für das Rating).

Risiken aus Unternehmenssicht

Jede unternehmerische Entscheidung ist mit Risiken verbunden, da die Auswirkungen dieser Entscheidungen i.d.R. nicht vorhergesagt werden können. Risiken werden jedoch in Kauf genommen, um Chancen wahrzunehmen und Erfolge zu erzielen - es gilt der Grundsatz: Keine Chance ohne Risiko. Für eine erfolgs- und wertorientierte Unternehmensführung ist somit eine zielorientierte, bewusste und systematische Auseinandersetzung mit Risiken und Chancen erforderlich. Daher ist es notwendig, dass in jedem Unternehmen organisatorische Regelungen zur Erkennung wesentlicher Risiken existieren.

Für einen sinnvollen und effektiven Umgang mit Risiken ist es unumgänglich, zunächst die Risikolage des Unternehmens einzuschätzen und zeitnah abbilden zu können. Unternehmen - unabhängig von ihrer Branche und Größe - sind im Rahmen ihrer Geschäftstätigkeit einer unbegrenzten Zahl von Risiken ausgesetzt.

Bei der Beurteilung der (Gesamt-) Risikolage eines Unternehmens ist zu beachten, dass das aggregierte

Unternehmensrisiko aufgrund möglicher kompensatorischer bzw. kumulativer Effekte der Einzelrisiken untereinander nicht unbedingt der Summe der Einzelrisiken entspricht.

Im Zusammenhang mit Risikomanagement denkt man zunächst an den Finanzbereich des Unternehmens und die Risiken in Verbindung mit dem Einsatz von derivativen Finanzinstrumenten. Vorhandene Risikomanagementsysteme beschränken sich meist nur auf diesen Bereich. Die folgende Abbildung zeigt jedoch, wie viel umfangreicher und vielfältiger die Risikolandschaft ist, die es bei der Einrichtung eines Risikomanagementsystems zu berücksichtigen gilt.

Organisation des Risikomanagementsystems

Das Risikomanagementsystem bzw. das Risikofrüherkennungssystem setzt sich aus folgenden Elementen zusammen:

- *Internes Überwachungssystem* mit organisatorischen Sicherungsmaßnahmen, internen Kontrollen und Interner Revision.
- *Controlling* (als Grundlage für eine zielgerichtete Steuerung des Unternehmens) mit den Subsystemen Planungssystem, Informationssystem, Kontrollsystem und Steuerungssystem einschließlich Dokumentationssystem und Reportingsystem.

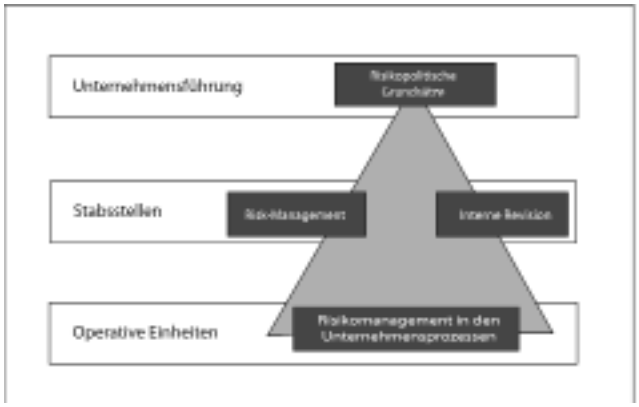
Die angeführten Risiken können sich sehr kurzfristig auswirken (z.B. Systemausfälle, die -kurzzeitig- zu Handlungsunfähigkeit führen), sie können aber auch das Ergebnis langsamer und schleichender Prozesse sein (z.B. die versäumte Anpassung der eigenen Produkte und Dienstleistungen an sich ändernde Kundenwünsche).

Gerade die Risiken aus strategischen Entscheidungen sind diejenigen, die hinsichtlich einer möglichen Bestandsgefährdung eine besondere Beachtung verdienen.

o *Risikomanagementsystem* im engeren Sinne mit Risikostrategie, Risikomanagementprozess und Risiko-Controlling.

Prozess des Risikomanagements

Der Risikomanagementprozess ist das Kernstück des Risikomanagements und stellt dessen Integration in die Abläufe des Unternehmens dar. Der Prozess ist nicht als einmalig zu verstehen. Es handelt sich vielmehr um einen kontinuierlichen Kreislauf, der alle Aktivitäten zum systematischen Umgang mit Risiken umfasst.



Der Prozess beginnt mit der möglichst vollständigen Erfassung aller relevanten Risiken (Risikoidentifikation). Nach der Ermittlung des erforderlichen Handlungs- und Steuerungsbedarfs (Risikobeurteilung) folgt die aktive Beeinflussung aller wesentlichen Risiken (Risikosteuerung). Im nächsten Schritt wird die Durchführung der Maßnahmen zur Risikosteuerung kontrolliert (Risikoüberwachung). Unternehmensgrundsätze zum Risikomanagement sind als risikopolitische Grundsätze zu dokumentieren. Werden während des Risikomanagementprozesses Veränderungen des Unternehmensumfeldes bzw. Veränderungen der das Unternehmen betreffenden Risiken festgestellt, ist evtl. eine Anpassung der Risikostrategie notwendig. Die Überwachung des gesamten Risikomanagementprozesses erfolgt prozessunabhängig, ggf. durch die interne Revision.

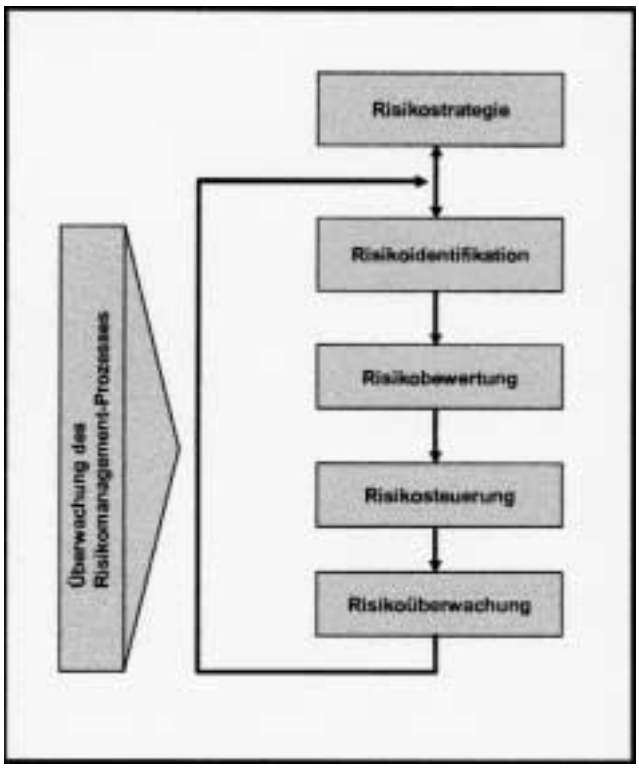
Interne Revision im Risikomanagement

Da die Gesetzesbegründung Risikomanagement und Interne Revision nebeneinander stellt, aber nicht die Beziehung zueinander formuliert, kann weder aus dem Gesetz noch aus der Gesetzesbegründung unmittelbar abgeleitet werden, dass die Interne Revision das Risikomanagement grundsätzlich prüfen muss. Es bleibt dem Vorstand im Rahmen seiner allgemeinen Verantwortung entsprechend § 76 AktG überlassen, in welcher Weise er absichert, dass das Risikomanagement seine Aufgabe erfüllt.

Es ist davon auszugehen, dass zumindest in Großunternehmen die notwendige Überwachung des Risikomanagementsystems ohne eine leistungsfähige Revision nicht sichergestellt werden kann und der Internen Revision aufgrund ihrer allgemeinen Aufgabenstellung sowie ihrer neutralen Position auch die unternehmensinterne Überwachung der Funktionsfähigkeit der Risikomanagementsysteme zu übertragen ist.

Sollte aufgrund der Größe u/o der Struktur eines Unternehmens keine interne Revisionsfunktion vorhanden sein, hat die Geschäftsleitung in geeigneter Weise die Prüfung des Risikomanagements sicherzustellen.

Die Interne Revision kann wie bisher schon bei der Einführung neuer Systeme bereits bei der Konzeption und Einführung des Risikomanagementsystems beratend tätig sein. Die laufende Verantwortung für das Risikomanagement kann aber wegen des bestehenden Interessenkonfliktes nicht der Internen Revision übertragen werden.



Die Interne Revision bewertet das Risikomanagement, unterstützt das Unternehmen bei der Identifizierung und Bewertung wesentlicher Risikopotentiale und leistet Beiträge zur Verbesserung der Risiko- und Kontrollsysteme. Überwachung, Qualität und Effizienz des Risikomanagements gehören in diesem Zusammenhang untrennbar zusammen. Dabei ist jedoch zu beachten, dass ihre Möglichkeiten von Art und Umfang ihres Auftrags durch die Geschäftsleitung bzw. den Aufsichtsrat begrenzt sind. Bestimmte Überwachungsaufgaben im strategischen Bereich können letztlich nur durch den Aufsichtsrat wahrgenommen werden, während im operativen Bereich insbesondere die Unternehmensleitung gefordert ist.

Ausgangspunkt der Prüfung des Risikomanagementsystems ist die Risikomanagementstrategie. Hierbei ist insbesondere sicherzustellen, dass das Risikomanagement von der Unternehmensleitung als Teil der

Corporate Governance gesehen wird und ein entsprechender Beschluss der Unternehmensleitung hinsichtlich der Einrichtung und des laufenden Erhaltes des Risikomanagementsystems existiert. Die Revision hat festzustellen, ob

- ein fundiertes, von der Unternehmensleitung getragenes und dokumentiertes Risikomanagementsystem existiert.
- der Risikomanagementprozess umfassend und kontinuierlich durchgeführt wird und die Ergebnisse in geeigneter Weise dokumentiert und kommuniziert werden.
- die festgelegten Maßnahmen tatsächlich umgesetzt wurden.

Darüber hinaus ist die Risikoidentifikation, die Risikobewertung und die Zweckmäßigkeit der Maßnahmen inhaltlich zu beurteilen. Intensität und Häufigkeit der Prüfungen sind u.a. in Abhängigkeit von der Komplexität der Wertschöpfung, Unternehmensgröße und Dynamik der Unternehmensentwicklung festzulegen.

Prüfung der Konzeption und Organisation des Risikomanagements

Die Interne Revision hat zu prüfen, ob eine klare Konzeptbeschreibung und eindeutige Regelungen hinsichtlich Zuständigkeiten und Dokumentation für alle Unternehmensbereiche vorliegen. Im Einzelnen sind folgende Punkte zu untersuchen:

- Existiert ein Risikomanager (u/o eine andere Stelle oder Funktion im Unternehmen), der (die) für die Koordination und Unterstützung hinsichtlich des Risikomanagements verantwortlich ist ?
- Gibt es eine Organisations-Richtlinie, ein Handbuch oder Arbeitsanweisungen, in denen die organisatorischen Regelungen und Maßnahmen des Risikomanagementsystems einschließlich der Implementierung und der Durchführung geregelt sind ?
- Ist im Unternehmen geregelt, dass die Verantwortung für ein funktionierendes Risikomanagementsystem bei den Geschäfts- / Organisationseinheiten liegt ?
- Wurden adäquate Schwellenwerte hinsichtlich der Risikozuordnung zu verantwortlichen Bereichen definiert ?
- Wird die Risikolage des Unternehmens im Rahmen einer vorgegebenen Systematik regelmäßig mindestens jährlich auf Aktualität geprüft ?
- Ist sichergestellt, dass bei plötzlichen unvorhergesehenen Veränderungen in der Risikolandschaft des Unternehmens eine Aktualisierung der Risiken hinsichtlich Organisation, Verantwortlichkeit und Dokumentation in angemessenen Zeitabständen erfolgt ?
- Werden Risiken mit gleicher Ursache kumuliert ?

Die Risikoidentifikation stellt den ersten Schritt eines Risikomanagementprozesses dar. Dieser Phase obliegt die vom KonTraG geforderte systematische Identifikation aller auf das Unternehmen einwirkenden Risiken - insbesondere der bestandsgefährdenden Risiken. Dabei sind neben den Kerngeschäftsprozessen (z.B. Forschung und Entwicklung, Einkauf, Produktion, Marketing und Vertrieb, Kundendienst) auch die Unterstützungsprozesse (z.B. Finanzen, Personal, Informationstechnologie, Logistik) einzubeziehen.

Risikoidentifikation

Bsp. Risikoinventar

Risiko	**Risikofeld**	
Neue Wettbewerber	Marktrisiken	Marktposition und Wettbewerbs
Abhängigkeit von XYZ AG	Wertschöpfungskette	Akquisition
Haftpflichtschaden bei Kunde Z	Rechtliche Risiken	Produkthaftung
Kalkulationsfehler	Wertschöpfungskette	Angebote, Kalkulation und Preissetzung
Absatzpreis-schwankung	Marktrisiken	Absatzmengen und Absatzpreise
Anstieg der Tariflöhne	Spezielle Risiken	Personalwirtschaft und Personalauswahl
Ausfall der ABC-Anlage	Spezielle Risiken	Business Continuity Plan
Wachstumsbedingter EK-Mangel	Strategische Risiken	Finanz- und Kostenstruktur
Übernahme der Muster AG	Finanzmarktrisiken	Beteiligungen, Unternehmenskäufe
Fehlende Kompetenz	Strategische Risiken	Kernkompetenzen und kritische Erfolgsfaktoren
Motivationspro-bleme im Vertrieb	Risiken aus Corporate Governance	Betriebsklima und Motivation
Störfall im Werk C	Spezielle Risiken	Arbeitssicherheit

Die Identifikation von Risiken wird im Idealfall von den Prozessverantwortlichen im Unternehmen durchgeführt. Diese sind in die operativen Geschäftsprozesse eingebunden und sollten in der Lage sein, entsprechende Frühwarnindikatoren zu definieren und danach auch korrekt zu deuten.

Als Ergebnis der Risikoidentifikation werden die identifizierten Risiken bzw. Risikobereiche in einem

Risikokatalog dokumentiert, der als Grundlage für die anschließende Risikoanalyse dient. Bei der Dokumentation sollten die Unternehmensstrukturen und -prozesse berücksichtigt und die Risiken soweit wie möglich zu einem Risikoprofil zusammengefasst werden.

Bei der Prüfung der Risikoidentifikation ist im Wesentlichen auf die verwendete Methodik, die Vollständigkeit, die zeitnahe Erfassung und die regelmäßige Aktualisierung zu achten.

Risikoanalyse

Zur Ableitung von angemessenen Steuerungsmaßnahmen müssen die identifizierten Risiken weiter untersucht und bewertet werden. Ziel der Risikoanalyse ist die qualitative Beurteilung bzw. quantitative Messung der Risiken, um das Risikoportfolio des Unternehmens abzubilden. Dabei sollten die Wirkungszusammenhänge einzelner Risiken berücksichtigt werden. Für die Risikoanalyse empfiehlt es sich, zunächst eine grobe Beurteilung des originären Risikos, d.h. der Risikosituation vor Kontrollen und Risikomanagement, durchzuführen.

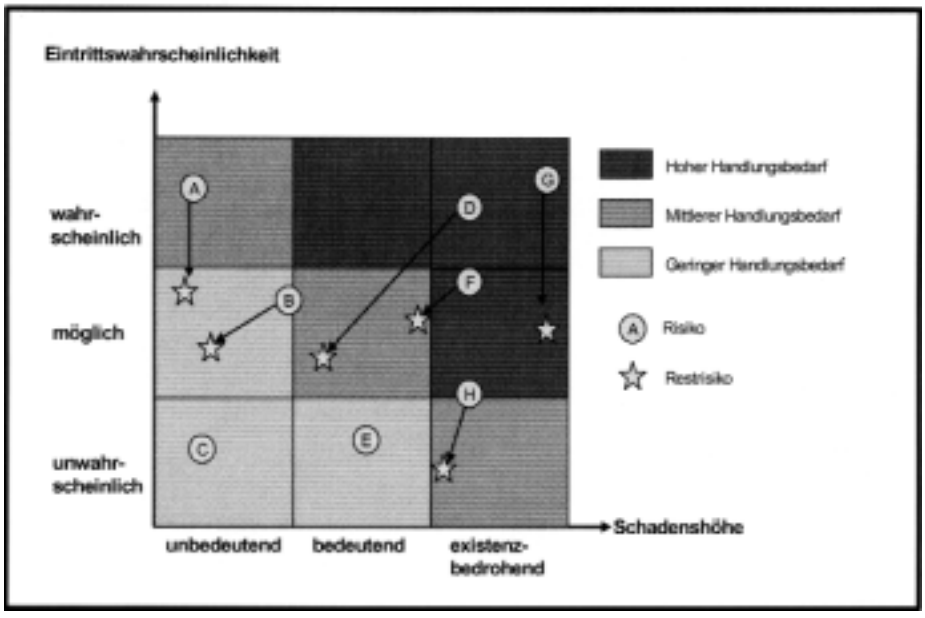
Die Ergebnisse dieser ersten Analyse können ergänzend in den Risikokatalog aufgenommen werden. Dieser sollte als Ergebnis der Risikoidentifikation bereits die erkannten Risiken einschließlich einer kurzen Beschreibung enthalten. Ergänzt wird er nun um weitergehende Erläuterungen zur Risikoursache, die Häufigkeit des Auftretens (Eintrittswahrscheinlichkeit) sowie eine Bewertung der Schadenhöhe. Schließlich werden Risikoverantwortliche festgelegt sowie notwendige Maßnahmen u/o Empfehlungen festgehalten.

Als Grundlage für die Risikosteuerung sind die Ergebnisse der Risikoanalyse kontinuierlich zu erfassen und durch eine angemessene Berichterstattung den Entscheidungsträgern zeitnah zur Verfügung zu stellen. Dabei sollte im Zweifel der Grundsatz Aktualität vor Genauigkeit gelten. Soweit wie möglich sollten die Risiken quantifiziert werden. Dies kann beispielsweise in Form von Risikomaßzahlen, z.B. dem "Value-at-Risk", d.h. dem mit mathematisch-statistischen Verfahren bewerteten Verlustpotential aus einem Geschäft oder einer Aktivität, erfolgen.

Während sich die finanziellen Risiken eines Unternehmens weitgehend exakt quantifizieren lassen, gilt dies kaum für die Gesamtheit der Risiken, denen das Unternehmen ausgesetzt ist. Insbesondere die Quantifizierung von Risiken, die sich aus den strategischen Entscheidungen der Unternehmensleitung ergeben, ist nur begrenzt möglich. In der Regel ist sie im hohen Maße von der subjektiven Einschätzung der Entscheidungsträger abhängig.

Die Interne Revision hat im Zusammenhang mit der Risikoanalyse und -bewertung insbesondere zu prüfen, welche Methoden zur Quantifizierung und Klassifizierung der Risiken angewandt werden, wie die Bestandsgefährdung bestimmt wird und ob Abhängigkeiten und kumulative Effekte festgestellt werden.

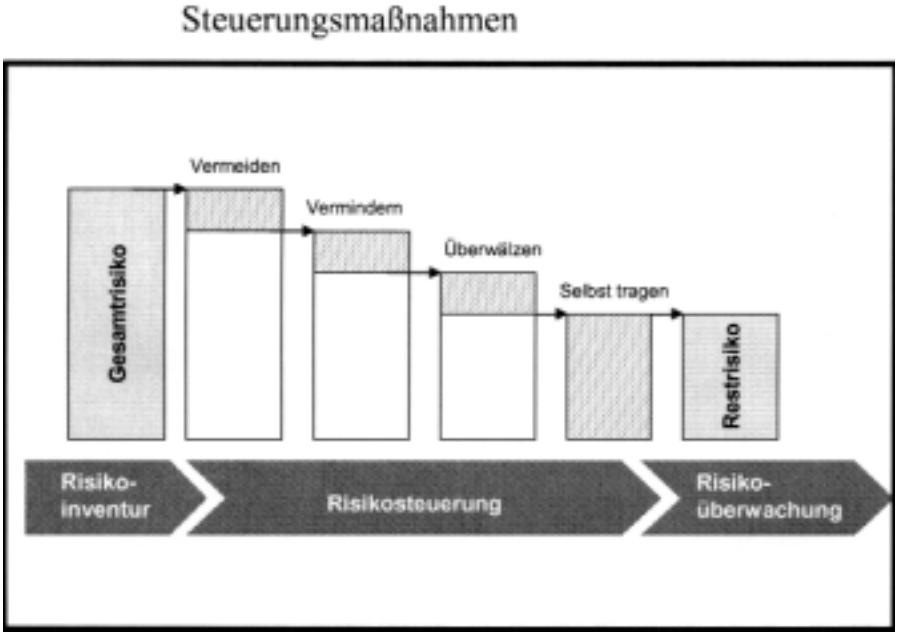
Risikoportfolio



Risikosteuerung

Gegenstand der Risikosteuerung ist die aktive Beeinflussung der im Rahmen von Risikoidentifikation und Risikoanalyse ermittelten Risikopositionen. Sie muss in Einklang mit den Unternehmenszielen und den daraus abgeleiteten Zielen des Risikomanagements stehen. Steuerungsmaßnahmen zielen dabei auf eine gezielte Verringerung der Eintrittswahrscheinlichkeit (z.B. durch Kontrollen oder andere Präventivmaßnahmen) oder aber eine Begrenzung der Auswirkungen von Risiken (z.B. durch

Versicherungen). Sie müssen dazu führen, dass für das Unternehmen nicht akzeptable Risiken vermieden und nicht vermeidbare Risiken auf ein akzeptables Maß reduziert werden können. Hierzu sind die Einzelrisiken gemäß der für ihre Risikokategorie festgelegten Risikostrategien zu steuern. Dies setzt allerdings voraus, dass die Entscheidungsträger kontinuierlich über ihre Risikosituation bzw. ihr Risikoportfolio unterrichtet sind.



Wesentliche Fragestellungen bei der Prüfung der Risikosteuerung sind:

- Welche Frühwarnindikatoren mit welchen quantitativen und qualitativen Limits / Schwellenwerte gibt es ?
- Welche Maßnahmen existieren und sind Maßnahmenverantwortliche benannt ?
- Werden die Maßnahmen umgesetzt, kommuniziert und sind sie wirksam ?

Risikoüberwachung

In der letzten Phase des Prozesses soll sichergestellt werden, dass durch die Risikoüberwachung die Risikolage des Unternehmens jederzeit der angestrebten Risikosituation entspricht. Alle Risikopotentiale und die Wirksamkeit der Maßnahmendurchführung werden kontinuierlich überwacht. Es soll so festgestellt werden, ob die Maßnahmen zur Risikobewältigung optimal eingesetzt wurden. Aufgrund der Veränderung einzelner Risikopositionen ist zu überprüfen, ob die jeweilige risikobewältigende Maßnahme angepasst werden muss.

Die Aufgabe des Risikocontrollings im Rahmen der Überwachung besteht in der optimalen Koordination der Prozessphasen, insbesondere der Identifikation und Beurteilung. Die Koordination erfolgt, indem die Schritte und Elemente des Risikomanagements in zeitlicher und sachlicher Hinsicht aufeinander abgestimmt werden. Dadurch soll sichergestellt werden, dass ein permanenter Überwachungsprozess entsteht, d.h. erkannte Risiken ständig überwacht und neu auftretende Risiken sofort aufgenommen werden. Außerdem überwacht das Risikocontrolling die Einhaltung der Grenzwerte und Limits und analysiert Risikokennzahlen auf der Basis eines Soll-/Ist-Vergleichs. Es versorgt dann das Management mit Informationen über die gewonnenen Ergebnisse. Organisatorisch ist das Risikocontrolling beim Controlling als zentrale und koordinierende Funktion für Planung, Steuerung und Kontrolle anzusiedeln. Solch eine prozessunabhängige Controllingabteilung existiert i.d.R. im Unternehmen bereits.

Die Überwachung des Risikomanagementsystems bezieht sich dagegen auf die Beurteilung der Effektivität der gesamten Organisation sowie auf die Angemessenheit der Berichterstattung. Diese Überwachung soll die Funktionsfähigkeit des Systems aufrechterhalten. Sie kann durch prozessunabhängige Organe (Interne Revision, Abschlussprüfer) wahrgenommen werden.

...„Die Überwachung des Risikomanagementsystems bezieht sich dagegen auf die Beurteilung der Effektivität der gesamten Organisation sowie auf die Angemessenheit der Berichterstattung.“...

Risikoorientierte Prüfungsplanung

Der Gesamtprüfungsplan enthält alle Betriebs- und Geschäftsabläufe, welche Prüfungsfelder im Sinne der Revision darstellen können. Dieser Plan wird auch als Prüfungslandkarte bezeichnet. Jedoch können aufgrund der steigenden Komplexität der

Prozesse nicht mehr alle Felder geprüft werden - es muss eine Auswahl getroffen werden. Von daher führt die Interne Revision eine Risikoanalyse aller Prüffelder durch, um das Prüfungsprogramm für die nächste Periode zu erstellen. Dazu werden die potentiellen Bereiche anhand von Risikokriterien beurteilt. Solche Kriterien können beispielsweise lauten:

...„Die von allen Revisionsmitarbeitern gemeinsam erarbeiteten Prüfungskriterien werden mit einer Gewichtung und mit einer Punktbewertung versehen.“...

- Zeitabstand zur letzten Prüfung
- Ergebnis der letzten Prüfung
- Organisationsänderungen
- Personalveränderungen
- Relevanz für die Bilanz und Gewinn- und Verlustrechnung
- ...

Weitere Faktoren können die Ergebnisse aus dem Risikomanagement sein:

- Identifizierte Risiken
- Entwicklung in der Zukunft
- Eintrittswahrscheinlichkeit und Schadenshöhe.

Die von allen Revisionsmitarbeitern gemeinsam erarbeiteten Prüfungskriterien werden mit einer Gewichtung und mit einer Punktbewertung versehen.

Aus dem risikoorientierten Gesamtprüfprogramm wird das Jahresprüfprogramm abgeleitet und mit den zur Verfügung stehenden Kapazitäten unter Berücksichtigung der Qualifikationen abgeglichen. Natürlich sind jährlich fixierte Prüfungen (z.B. Finanz- und Energiehandel) in den Jahresprüfplan aufzunehmen. Dieser Jahresprüfplan wird durch den Vorstand genehmigt. Daraus abgeleitet werden die individuellen Prüfungspläne der jeweiligen Revisoren. Die Berichterstattung der Internen Revision erfolgt durch Einzel-, Quartals- und Jahresberichte an den Vorstand.

Schlussbetrachtung

Neue Aufgaben und neue Herausforderungen gehen mit dem Management der Risiken einher. Immer dynamischer werdende Märkte machen einen systematischen Umgang mit den Risiken des Unternehmens notwendig. Das aktive Identifizieren, Gestalten und Steuern der Risiken ist ein wichtiges Mittel zur Sicherstellung der Existenz und des zukünftigen Erfolges. Das Risikomanagementsystem schafft die Voraussetzungen, Risiken frühzeitig zu erkennen, zu bewerten und zu steuern und kann zudem bei richtiger Ausgestaltung als nachhaltiges Chancenmanagement verstanden werden. Im Kontext der Unternehmensüberwachung fällt der Internen Revision eine wichtige Rolle zu. Die Zielsetzungen des Risikomanagements und der Internen Revision stimmen weitgehend überein. Beide unterstützen die Unternehmensleitung und -bereiche bei der Erreichung der Ziele sowie die dezentralen Führungsebenen bei der eigenverantwortlichen Selbststeuerung. Weiterhin sollen durch Risikomanagement und Interne Revision Vermögensverluste vermieden sowie die Vorschriften des KonTraG erfüllt werden.

...„Neue Aufgaben und neue Herausforderungen gehen mit dem Management der Risiken einher“....

Insgesamt ist festzuhalten, dass der Erfolg von Risikomanagementprojekten - nämlich die Steigerung des Unternehmenswertes durch die Verbesserung der Risikoposition des Unternehmens - durch eine Reihe häufig beobachteter Fehlerquellen bedroht ist.

Für sämtliche Phasen eines Risikomanagementprojektes bestehen schwerwiegende methodische Gefahren. Diese können dazu führen, dass Risikomanagementprojekte in der Praxis trotz massiven Einsatzes an Zeit- und Mitarbeiterressourcen keinen befriedigenden Erfolg zeigen und oft die in sie gesetzten hohen Erwartungen nicht erfüllen. Gründe hierfür können z. B. sein, dass der Bezug zur Unternehmensstrategie und zu den Erfolgsfaktoren fehlt, dass Fachexperten bei der Risikoanalyse und einheitliche Risikobewertungseinheiten fehlen, dass das Risikomanagementsystem mangelhaft dokumentiert ist und dass keine Trennung von Risikomanagement und Interner Revision besteht.

Mit besonderem Dank an Herrn Christoph Wildensee.

Anforderungen an ein Risikomanagementsystem

Die Randbedingungen aus den relevanten Interessenslagen zur Umsetzung eines RMS in Form von Gesetzen, Verlautbarungen und Empfehlungen, Prüfungsstandards und Zertifizierungsmöglichkeiten sind im Folgenden zusammengestellt mit Quellangaben (Internet-Adressen) zur vertiefenden Information. Von diesen kann man nach Belieben weiter verzweigen:

Vorgaben des **Gesetzgebers:**

- KonTraG / AktG
  Lehrstuhl für Betriebswirtschaftslehre insbesondere Revisions- und Treuhandwesen
  http://www.uni-regensburg.de/Fakultaeten/WiWi/scherrer/edu/opi/kontrag.html
- Corporate Governance
  Deutscher Corporate Governance Kodex
  http://www.corporate-governance-code.de/
- TransPuG
  http://217.160.60.235/BGBL/bgbl1f/bgbl102s2681.pdf
- HGrG (Haushaltsgrundsätze-Gesetz)
  http://www.lrh-mv.de/Informationen/Gesetze/HGrG.htm
- Anforderungen der Bundesanstalt für Finanzdienstleistungsaufsicht
  http://www.bafin.de/

Anforderungen der **Gesellschafter:**

- Shareholder Value

Anforderungen an/durch **Kreditinstitute:**

- Basel II
  Corporate-Consulting.Network
  http://www.basel-ii.info/

Umsetzung durch den **Vorstand**:

- Aufbau eines Überwachungssystems nach KonTraG
  Lehrstuhl für Betriebswirtschaftslehre insbesondere Revisions- und Treuhandwesen
  http://www.uni-regensburg.de/Fakultaeten/WiWi/scherrer/edu/opi/kontrag.html
- Zertifizierung nach ISO 9001 ff (Qualitätsmanagement))
  Ruhr-Universität Bochum
  http://www.iso.bifak.de/
  Universität Leipzig
  http://ais.informatik.uni-leipzig.de/download/2002s_v_sqm/2002s_sqm_v_04.pdf
- Zertifizierung nach ISO 17799 (IT-Security)
  Datensicherheit nach ISO/IEC 17799
  http://www.tokon.net/sec/iso.htm
  (Empfehlungen zum Aufbau eines Sicherheitssystems)
- Darstellung der Risken im Lagebericht (siehe IDW PS 350)
- IKS - Internes Kontrollsystem (siehe IDW PS 260)
- Die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB (siehe IDW PS 340)
- Prüfung des RMS durch die Interne Revision
  IDW Institut der Wirtschaftsprüfer in Deutschland e.V. / IDW-Verlag GmbH
  http://www.idw-verlag.de

OSV/os

Bemerkungen 2002 des Bundesrechnungshofes zur Haushalts- und Wirtschaftsführung des Bundes

Zusammengestellt von Frank Haub
Geschäftsführer HAUB + PARTNER GmbH

Die jährlichen "Bemerkungen" des Bundesrechnungshofes - in der Öffentlichkeit besser bekannt als Prüfungsbericht des Bundesrechnungshofes - wurden im November 2002, in einem 293 Seiten umfassenden Bericht, der Öffentlichkeit zugänglich gemacht. Die jährlichen Bemerkungen geben lediglich einen Ausschnitt der gesamten Tätigkeit des Bundesrechnungshofes wieder. Seine Prüfungstätigkeit schlägt sich in einer Vielzahl weiterer Mitteilungen an die geprüften Stellen nieder. Dem ausführlichen Berichtsteil ist eine Kurzfassung vorangestellt. Im Folgenden werden daraus einige interessante Feststellungen teilweise unter Hinzuziehung des Hauptberichtes dargestellt:

Feststellung Nr. 8:

Festsetzung und Erhebung eines deutschen C1-Visums. Diese Feststellung betrifft das Bundesministerium Auswärtiges Amt. Nach der Umsetzung des Schengener Abkommens kostete ein deutsches Visum nur 40 DM, während die übrigen Schengen-Staaten den vereinbarten Höchstsatz von umgerechnet 50 DM verlangten. Die Einnahmeausfälle hieraus summieren sich seit dem Jahre 1996 auf mindestens 66 Mio. DM.

Weitere Gebühren für verschiedene andere konsularische Amtshandlungen führten durch verspätete Anpassung ebenfalls zu Mindereinnahmen.

Insgesamt beläuft sich der Einnahmeausfall aus verschiedenen geschilderten Sachverhalten auf mind. 270 Mio. DM.

Feststellung Nr. 23: Liguiditätsplanung und kurzfristige Mittelaufnahme des Bundes

Diese Feststellung betrifft das Bundesministerium der Finanzen. Der Bundesrechnungshof hat festgestellt, dass insbesondere die Planungsdaten für den täglichen Kassenausgleich vom Bundesministerium aufwendig und nicht mehr zeitgemäß erhoben werden. Er hat ferner festgestellt, dass das Bundesministerium bisher nur Tages- und Termingeld einsetzt, um den täglichen Zahlungsmittelbedarf zu decken. Weitere Geldmarktinstrumente, die eventuell kostengünstiger gewesen wären, wurden nicht genutzt. Das Bundesministerium hat ausgeführt, dass nunmehr der Einsatz neuer Instrumente am Geldmarkt geprüft worden sei; mit ersten Einsätzen werde noch im Jahre 2002 zu rechnen sein. Der Bundesrechnungshof hält es für erforderlich, die neuen Instrumente kurzfristig einzusetzen, damit mögliche Zinskostenersparnisse ausgeschöpft werden.

Feststellung Nr. 24: Prägung von Zahlungsverkehrs-, Sammler- und Gedenkmünzen

Diese Feststellung betrifft ebenfalls das Bundesministerium der Finanzen. Hohe Prägeaufträge bei den 1-DM- bis 5-DM-Münzen führten in den Folgejahren seit 1989 zu überhöhten Münzbeständen. Der Bund hat damit die Prägemengen im Hinblick auf die Währungsumstellung nicht bedarfsgerecht angepasst. Es fehlte ein langfristiges Konzept, um Überbestände an Münzen abzubauen oder zu vermeiden und Münzen bis zum Euro-Umstellungstag nur noch im benötigen Umfang zu prägen. Die nicht absetzbaren Mengen wurden prägefrisch vernichtet. Zudem mussten Überbestände an Münzplättchen vernichtet werden. Durch langfristige Planung und Anpassung der Prägemengen hätten insgesamt zweistellige Millionenbeträge eingespart werden können.

Feststellung Nr. 28: Laufzeitmessungen im Briefdienst

Diese Feststellung betrifft das Bundesministerium für Wirtschaft und Technologie. Die Regulierungsbehörde für Telekommunikation und Post führt für rd. 3,3 Mio. EUR im Jahr eigene Messungen durch, um entscheiden zu können, ob die im Briefdienst einzuhaltenden Brieflaufzeiten erreicht werden. Diese Kosten hätten weitgehend eingespart werden können, wenn die Regulierungsbehörde auf in einem zertifizierten

Verfahren ermittelte Messergebnisse der Deutschen Post AG zurückgreift und nur bei Bedarf eigene Laufzeitmessungen in Auftrag gibt.

Aus dem Einzelbericht des Rechnungshofes geht hervor, dass die Regulierungsbehörde Laufzeitprüfungen durchführt und jährlich ca. 300.000 Testbriefe versendet. Während die Deutsche Post AG ebenfalls Laufzeitmessungen durchführt, welches vom TÜV Rheinland zertifiziert wird. Dabei versendet die Post rund 755.000 Testbriefe und wertet diese Ergebnisse monatlich aus. Nach Ansicht des Bundesrechnungshofes ist die Laufzeitmessung nicht Aufgabe der Regulierungsbehörde, sondern z.B. die Einhaltung der Vorschriften des Postgesetzes und der Postuniversaldienstleistungsverordnung.

Feststellung Nr. 33: Wirtschaftlichkeit der Rentenauszahlung durch die Deutsche Post AG

Diese Feststellung betrifft das Bundesministerium für Arbeit und Sozialordnung. Nach geltender Rechtslage sind die Träger der gesetzlichen Rentenversicherung verpflichtet, die Renten durch die Deutsche Post AG auszuzahlen. Die gesetzliche Aufgabenübertragung hat allein historische Gründe.

Sie geht zurück auf das Jahr 1891 seit Gründung der Rentenversicherung. Damals verfügte nur die Post über das erforderliche flächendeckende Zahlstellennetz, um die seinerzeit allein übliche Barauszahlung der Renten realisieren zu können. Die Anzahl der Barauszahlungen beträgt heute jedoch weniger als 0,5%. Weder die Umstellung auf den bargeldlosen Zahlungsverkehr noch die Privatisierung der Post und deren Umwandlung in eine privatrechtliche Aktiengesellschaft waren bislang Anlass, das historisch begründete Rentenauszahlungsmonopol der Post aufzuheben.

Sowohl die Bundesknappschaft als auch die Bundesversicherungsanstalt für Angestellte (BfA) erklärten sich bereit und in der Lage, das gesamte Rentenzahlverfahren einschl. aller damit zusammenhängenden Aufgaben zu übernehmen. Sie errechneten Kostenvorteile in Höhe von 23,5 Mio. EUR jährlich, wenn die Auszahlung der Renten in die Zuständigkeit der Rentenversicherungen überführt würde.

Feststellung Nr. 43: Baumaßnahmen an Bundesfernstraßen

Diese Feststellung betrifft das Bundesministerium für Verkehr, Bau -und Wohnungswesen. Der Bundesrechnungshof hat bundesweit insgesamt rund 3000 Bauverträge mit über 7000 Nachtragsvereinbarungen ausgewertet, die in den Jahren 1995 bis 1999 im Auftrage des Bundes abgerechnet wurden. Er hat festgestellt, dass die Ämter die verschiedenen Regelwerke, wie Verdingungsordnung für Bauleistungen etc. oftmals nicht ausreichend beachteten. Sie vereinbarten Nachträge in den meisten Fällen erst, nachdem die Leistungen erbracht waren oder Schlussrechnungen vorlagen. Nachdem die Baufirmen ihre Schlussrechnungen verspätet vorgelegt hatten, verging weitere Zeit, bis die Ämter sie prüften.

Dies führte dazu, dass die Ämter die Schlusszahlung erst viele Jahre nach Fertigstellung einer Maßnahme leisteten. Vielfach überschritt das jährlich zugewiesene Budget die Baumaßnahmen um ein Vielfaches. Durch Auftragserweiterungen oder Änderungen von Bauverträgen kam es teilweise zu Kostensteigerungen von mehr als 30%. Ursache für Nachträge waren insbesondere unzureichende Leistungsverzeichnisse.

Feststellung Nr. 52: Korruptionsprävention in der Bundeswehr

Diese Feststellung betrifft das Bundesministerium der Verteidigung. Die Bundesregierung hatte Mitte des Jahres 1998 eine Richtlinie zur Korruptionsprävention in der Bundeswehr erlassen. Der Bundesrechnungshof stellte fest, dass bei 137 Dienststellen der Bundeswehr über die Hälfte der Geprüften keinen Korruptionsbeauftragten benannt hatten. Die vorhandenen Korruptionsbeauftragten beschränkten sich darauf, ihre Benennung bekannt zu machen und gelegentlich über Inhalte der Richtlinie zu informieren. Die Differenzierung in korruptionsgefährdete und besonders korruptionsgefährdete Bereiche unterblieb weitgehend. Ganze Bereiche und Teilstreitkräfte im Geschäftsbereich waren der Auffassung, nicht von der Richtlinie betroffen zu sein.

Die geprüften Dienststellen verzichteten darauf, Beschäftigte in korruptionsgefährdeten Bereichen regelmäßig auszuwechseln.

Die Interne Revision des Bundesministeriums, der in der Richtlinie wichtige Aufgaben der Korruptionsprävention zugewiesen sind, war auf diesem Gebiet wenig aktiv.

Es wurde eindringlich beanstandet, dass das Bundesministerium die Richtlinie drei Jahre nach deren

Erlass in der Bundeswehr nur unzureichend und lückenhaft umgesetzt hat. Nach seiner Auffassung können aufgrund der jährlichen, in Milliardenbeträgen für die Ausrüstung der Streitkräfte aufgewandten Haushaltsmittel erhebliche Schäden durch Korruptionsfälle entstehen.

Feststellung Nr. 57: Nicht nutzbare Depotbestände des Heeres

Diese Feststellung betrifft ebenfalls das Bundesministerium der Verteidigung. In den Depots des Heeres lagerte Material mit einem Beschaffungswert von weit über 4 Mrd. DM, das als nicht ausgabebereit oder reserviert gekennzeichnet war. Das ist solches Material, das z.B. unvollständig oder defekt ist oder aus technischen Gründen nicht an die Truppe ausgegeben werden darf.

Stichproben zeigten, dass die Bundeswehr in vielen Fällen nichts unternahm, um die Ausgabebereitschaft oder eine Verwertung dieses Materials herbeizuführen. Das Material konnte trotz Bedarfs nicht genutzt werden, konnte aber auch nicht verwertet werden. Vermeidbare Kosten für die Lagerhaltung, nicht erforderliche Neubeschaffungen und eine Verringerung der Verwertungserlöse waren die Folge.

Feststellung Nr. 58: Lagerung von Kultgeräten

Diese Feststellung betrifft ebenfalls das Bundesministerium der Verteidigung. Für den Einsatz im Verteidigungsfall lagerten jahrzehntelang mehr als 300 unvollständige Kultgeräte für Feldgeistliche (z.B. Kreuze, Kelche und Gewänder) mit einem ursprünglichen Beschaffungswert von mehr als 2 Mio. DM in einem Heeresdepot. Der Lagerungscode kennzeichnete den Zustand der Ausstattungen als "nicht bekannt", weshalb deren Ausgabe gesperrt war. Es war nicht geklärt, warum sie unvollständig waren, ob überhaupt noch Bedarf für diese Ausstattung bestand und wie sie weiter verwendet werden sollten.

Feststellung Nr. 63: Kraftfahrerlöhne bei militärischen und zivilen Dienststellen

Diese Feststellung betrifft ebenfalls das Bundesministerium der Verteidigung. Im Jahre 2001 waren in den Fahrbereitschaften der Bundeswehr fast 5000 Zivilkraftfahrer beschäftigt, bei denen häufig Überstunden wegen Bereitschafts- und Schichtdiensten anfiel. Die Kraftfahrer waren jedoch während der Bereitschaftsdienste nur bis zu etwa 8 Stunden ausgelastet. In den Nacht- und Wochenendschichten waren sie ebenfalls oft nicht ausreichend beschäftigt. Von der Möglichkeit, Überstunden durch Freizeit auszugleichen, machten die Dienststellen grundsätzlich keinen Gebrauch. Der Bundesrechnungshof hat auf ein jährliches Einsparungspotential von bis zu 13 Mio. EUR. hingewiesen, wenn Überstunden verstärkt durch Freizeit ausgeglichen, eine versetzte Schichteinteilung eingeführt und unwirtschaftliche Bereitschaftsdienste gestrichen werden.

Feststellung Nr. 82: Verwaltungsausgaben der Bundesanstalt für Arbeit

Diese Feststellung betrifft die Bundesanstalt für Arbeit. Der Bundesrechnungshof hat verschiedene Vorschläge zur Senkung der jährlichen Verwaltungsausgaben in Höhe von rd. 4,6 Mrd. EUR (ohne Investitionen) unterbreitet. Er hat z.B. empfohlen, die kleinsten der 181 Arbeitsämter zu größeren Einheiten zusammenzufassen. Ferner hat er festgestellt, dass das Nebeneinander von sechs Arbeitsämtern in Berlin die Aufgabenwahrnehmung erschwert und den Verwaltungsaufwand erhöht. Er hat deshalb vorgeschlagen, die Zahl der Arbeitsämter in Berlin bis hin zu einem Arbeitsamt zu verringern und die aufzulösenden Arbeitsämter in Geschäftsstellen umzuwandeln.

Die Bundesanstalt hat nur einen Teil der Empfehlungen aufgegriffen. Bei vollständiger Umsetzung kann bei den Verwaltungsausgaben jährlich ein zweistelliger Millionenbetrag eingespart werden.

Feststellung Nr. 96: Einsatz von Instandhaltungstrupps und Hausmeistern in der Bundesvermögensverwaltung

Diese Feststellung betrifft das Bundesministerium der Finanzen. Die Anzahl der als Instandhaltungstrupps und Hausmeister eingesetzten rund 790 Verwaltungsmitarbeitern ist in den letzten Jahren weitgehend unverändert geblieben, obwohl der Bund seit dem Jahre 1994 rd. die Hälfte seines Wohnungsbestandes verkauft hat. Es wurde festgestellt, dass die Bundesvermögensämter sowohl die Arbeitserledigung als auch die Auslastung und Wirtschaftlichkeit des Einsatzes dieser Mitarbeiter nicht hinreichend kontrollierten. Um die Auslastung zu erhöhen und zuverlässige Arbeits- und Kapazitätsplanungen aufzustel-

len, könnten z.B. allein bei der Vergabe von Aufträgen an Fremdfirmen jährlich mind. 2 Mio. EUR eingespart werden.

Feststellung Nr. 111: Nutzung der Hubschrauber BÖ 105 in der Bundeswehr

Diese Feststellung betrifft das Bundesministerium der Verteidigung. U.A. werden 95 Verbindungs- und Beobachtungshubschrauber bei der Bundeswehr eingesetzt. Sie haben die Aufgabe, im Krisen- und Kriegsfall Aufklärungs-, Beobachtungs- und Verbindungsflüge durchzuführen. Die jährlichen Betriebskosten belaufen sich auf rd. 90 Mio. DM, wovon rd. 45 Mio. DM auf den Personentransport entfielen. Die Kosten einer Flugstunde betragen 4.280 DM. Auch angesichts der unzureichenden Ausstattung für die Aufgaben im Krisen- und Kriegsfall und eines unwirtschaftlichen Einsatzes der Hubschrauber als "Luft-Taxi" für Dienstreisen hat der Bundesrechnungshof die baldige Aussonderung empfohlen, wodurch jährliche Betriebskosten von bis zu 88 Mio. DM eingespart werden können.

Feststellung Nr. 114: Reisebeihilfen für Familienheimfahrten der Soldaten

Diese Feststellung betrifft ebenfalls das Bundesministerium der Verteidigung. Wehrsoldempfänger erhalten einen Berechtigungsausweis, mit dem sie kostenlos zwischen dem Dienstort und dem Familienwohnort mit der Bahn reisen können. Bei Benutzung anderer regelmäßig verkehrender Beförderungsmittel sowie bei Benutzung eines eigenen Pkw werden Reisebeihilfen bis zu fünf Familienheimfahrten im Kalendermonat gewährt. Grundsätzlich sollte der eigene Pkw wegen des allgemein erhöhten Unfallrisikos im Straßenverkehr bei einer Entfernung von über 300 km zwischen Dienstort und Wohnort nicht benutzt werden. Es wurde festgestellt, dass seit Mitte der 90er Jahre Reisebeihilfen ohne überzeugende sachliche Gründe mit eigenem Pkw gewährt wurden. Die Ausgaben haben sich seitdem auf über 12 Mio. EUR pro Jahr verdoppelt. In zahlreichen Fällen gewährten die Dienststellen auch dann Reisehilfen bei Benutzung eines eigenen Pkw, wenn die Entfernung zwischen Wohnung und Dienststelle mehr als 300 km betrug.

ibs-Roadshow 2003

GRATIS!!!

- **IT-Revision - eine kurze Einführung**
- **Prüfen von SAP R/3® mit CheckAud for SAP R/3® Version 2.5**
  Pause
- **Prüfen von Windows2000®-Umgebungen mit CheckAud for Windows2000®**
- **Prüfen von Hard- and Software mit CheckAud for Hard- and Software**

Orte und Termine:

❑ **Nürnberg 19.05.2003**
Le MERIDIEN
Grand Hotel Nürnberg
Bahnhofstr. 1 - 3
90402 Nürnberg

❑ **Köln 21.05.2003**
Restaurant am Römerturm
im Kolpinghaus International
St. Apern-Str. 32
50667 Köln

❑ **Frankfurt/Main 20.05.2003**
Holiday Inn
Conference Centre
Mailänder Str. 1
60598 Frankfurt

❑ **Hannover 22.05.2003**
fora HOTEL Hannover
Großer Kolonnenweg 19
30163 Hannover

Empfang mit Kaffee um 13:30 Uhr
Veranstaltung jeweils von 14:00 bis ca. 17:00 Uhr

Ich nehme an oben angekreuzter, KOSTENLOSER Veranstaltung mit _____ Person(en) teil.
Senden Sie mir bitte die Bestätigung nebst Vortragshotel (und Anfahrtsskizze) zu.

Name(n) _____ PLZ/Ort _____

Firma _____ Tel/Fax _____

Straße _____ Ort/Datum _____

ibs schreiber gmbh
international business software

www.ibs-schreiber-gmbh.de
www.checkaud.de

ibs schreiber GmbH
Friedrich-Ebert-Damm 145
22175 Hamburg

Tel. +49 40 69 69 85-18
Fax +49 40 69 69 85-31
E-Mail: sales@ibs-schreiber-gmbh.de

ANZEIGE

Wahrung von Unternehmensrichtlinien in SAP R/3® durch die Nutzung von CheckAud for SAP R/3®

Von Thomas Tiede
Geschäftsführer, ibs schreiber gmbh, Hamburg

CheckAud
for SAP R/3® Systems

Zur realen Ausprägung eines Risikomanagementsystems nach KonTraG in SAP R/3®

Der virtuelle Betrieb, der den realen Betrieb in Form von Daten im IT-System darstellt, wird in seiner Ausprägung immer umfassender. Haben Sie schon einmal geprüft, ob dieser virtuelle Betrieb mit Ihrem realen Betrieb überhaupt noch übereinstimmt?

Bei einer Aufnahme der Personalstruktur im virtuellen Betrieb werden z.B. Mitarbeiter gefunden, die real gar nicht mehr vorhanden sind oder die zwischenzeitlich in anderen Abteilungen arbeiten. (Gefahr falscher Autorisierungen und als Folge davon potentielle unerlaubte Datenzugriffe). In der Materialdatei werden z.B. Materialien gespeichert und als Neuwerte deklariert, die real zwar vorhanden sind, aber keinen realen Wert mehr haben (absichtliche oder irrtümliche Fehlbeschaffung?) und die in der Bilanz voll aktiviert werden (Bilanzfälschung?). In der Kreditorendatei werden z.B. Scheinlieferanten geführt und auf Grund fingierter Eingangsrechnungen bezahlt (Betrug). In der Debitorendatei werden Kunden und zugeordnete Verkäufe ausgewiesen, die real gar nicht existieren (zur Ergebnisschönung).

Dies sind nur einige - aus der Praxis gegriffene - Beispiele, die zeigen, wie anfällig der virtuelle Betrieb ist. Diese Beispiele zeigen auch, dass das Hauptgefährdungspotential in den eigenen Mitarbeitern liegt; denn diese sitzen an der Quelle! Präventivmaßnahmen zur Minimierung dieser Risiken sind geboten.

Für SAP R/3®-Umgebungen wurde hierfür Check**Aud** for SAP R/3® Systems entwickelt und von der SAP AG zertifiziert, ein Tool zur umfassenden automatisierten Prüfung des SAP-Berechtigungskonzeptes, der Systemsicherheit, des Customizings u.v.m..

*Check**Aud** for SAP R/3® aus Sicht des Vorstandes und Abschlussprüfers*

Nach dem KonTraG und sukzessive dem AktG §91 (2) hat der Vorstand geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.

Dies ist vom Abschlussprüfer im Rahmen seiner Jahresabschlussprüfung zu testieren. Im PS (Prüfungsstandard) 340 des IDW "Die Prüfung des Risikofrüherkennungssystems" heißt es dazu: Der Abschlussprüfer hat nach § 317 Abs. 4 HGB bei Aktiengesellschaften im Rahmen der Abschlussprüfung zu beurteilen, ob der Vorstand die nach § 91 AktG erforderlichen Maßnahmen in einer geeigneten Form getroffen hat und ob das danach einzurichtende Überwachungssystem seine Aufgaben erfüllen kann.

SOFTWARE™ SAP PARTNER
SAP® Certified Integration

Zu überwachen sind unter anderem die folgenden gesetzlichen Auflagen:

1. §239 Abs. III HGB Radierverbot

   Dieser Paragraph regelt, dass Aufzeichnungen nicht so verändert werden dürfen, dass der ursprüngliche Inhalt nicht mehr feststellbar ist. Aufzeichnungen in diesem Sinne sind z.B. Stammdaten (Debitoren- und Kreditorendaten) und Bewegungsdaten (Buchhaltungsbelege der Finanzbuchhaltung).
   Technisch gesehen werden sämtliche Aufzeichnungen in SAP R/3® in Tabellen gespeichert. Manuelle Manipulationen in diesen Tabellen stellen somit einen Verstoß gegen den § 239 HGB dar. Solche Manipulationen werden "Elektronisches Radieren" genannt.

Die Möglichkeiten zum elektronischen Radieren in SAP R/3® sind vielfältig:

- Durch die Zuordnung falscher Zugriffsrechte ist es z.B. möglich, Programme zu debuggen mit der Möglichkeit, Hauptspeicherinhalte zu verändern (Berechtigungsobjekt S_DEVELOP).
- Durch das Zulassen von Entwicklerschlüsseln (Tabelle DEVACCESS) im Produktivsystem kann es möglich sein, dass Anwendungsentwicklung im produktiven R/3®-System möglich ist.
- Durch direkte Zugriffe auf die Datenbank, in der die R/3®-Daten gespeichert werden, können die Tabellen ohne Nachvollziehbarkeit manipuliert werden.

2. §257 HGB Aufbewahrungsfristen

   Gem. §257 HGB müssen Unterlagen wie Bilanzen, Buchhaltungsbelege, Jahresabschlüsse usw. 10 Jahre aufbewahrt werden. Dazu zählen auch sämtliche Änderungen an den Stamm- und Bewegungsdaten der Finanzbuchhaltung sowie die dazugehörige Verfahrensdokumentation. Alle diese Angaben werden in SAP R/3® in Tabellen gespeichert. Es müssen somit nicht nur die Stamm- und Bewegungsdaten selbst aufbewahrt werden, sondern auch die Änderungsbelege dazu sowie die Customizing-Einstellungen und deren Änderungen (diese stellen die Verfahrensdokumentation dar).

   Verstöße hiergegen sind in SAP R/3® wieder auf vielfältige Weise möglich, z.B.:

   - Durch die Zuordnung des Zugriffsrechtes zum Löschen von Änderungsbelegen mit dem R/3®-Report RSCDOK99.
   - Durch die Zuordnung des Zugriffsrechtes zum Löschen von Tabellenänderungsbelegen mit dem Report RSTBPDEL oder der Transaktion SCU3.
   - Durch die Möglichkeit zur Anwendungsentwicklung im Produktivsystem. Hier können über die Programmiersprache ABAP Protokolle gelöscht werden.
   - Durch direkte Zugriffe auf die Datenbank, in der die Protokolle manuell in den Tabellen gelöscht werden können.

> ...“Gem. §257 HGB müssen Unterlagen wie Bilanzen, Buchhaltungsbelege, Jahresabschlüsse usw. 10 Jahre aufbewahrt werden....“

Die Problematik zur Wahrung dieser Auflagen besteht darin, dass sie jederzeit durch die Zuordnung von Zugriffsrechten wieder umgangen werden können. Es ist daher kein einmaliger Prozess, die Wahrung der Auflagen festzustellen. Vielmehr ist im Rahmen eines Risikofrüherkennungssystems eine ständige Kontrolle zu implementieren, durch die sichergestellt ist, dass diese Auflagen nicht umgangen werden können. Solch eine Risikofrüherkennung kann mit Check**Aud** for SAP R/3® implementiert werden.

*Check**Aud** for SAP R/3® aus Sicht des Datenschutzbeauftragten und Betriebsrats*

Nach dem Bundesdatenschutzgesetz § 9 ist bezüglich personenbezogener Daten u.a. folgende Auflage zu erfüllen: Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind, zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle).

In vielen Modulen eines SAP R/3®-Systems werden personenbezogene Daten verarbeitet. Angefangen mit

den Daten der Benutzer, die mit dem R/3®-System arbeiten, über die Kunden und Lieferanten bis hin zu Mitarbeitern (Modul HR) oder Patienten (Modul IS-H). Der Schutz dieser Daten vor unberechtigten Lese- und Schreibzugriffen muss gewährleistet sein.

Gerade aus Datenschutzsicht stellt hier aber die Komplexität eines R/3®-Systems ein Problem dar. Allein der Zugriff auf z.B. Mitarbeiterdaten kann über die verschiedensten Wege erfolgen. Nachfolgend einige der in SAP R/3® möglichen Zugriffe auf Mitarbeiterdaten:

1. Über den regulären Weg der Stammdatenpflege und -anzeige

   Diese Berechtigungen sind den Mitarbeitern der Personalabteilung zuzuordnen. Allerdings können in SAP R/3® sehr ausgefeilte Zugriffe auf Mitarbeiterdaten vergeben werden, evtl. sogar gesteuert über die Unternehmensstruktur. Auf Grund der Komplexität ist es hier nicht ausgeschlossen, dass diese Zugriffe zu weitreichend ausgelegt sind. Des weiteren zeigt sich in der Praxis immer wieder, dass auch Mitarbeiter außerhalb der Personalabteilung diese Zugriffsmöglichkeit besitzen, z.B. Systemverwalter.

2. Über den Weg der Tabellenanzeige

   Alle Stamm- und Bewegungsdaten werden innerhalb von SAP R/3® in Tabellen gespeichert, welche physisch in einer Datenbank (Oracle, Informix, ADABAS, DB2, ...) abgelegt werden. Innerhalb von SAP R/3® gibt es verschiedenste Wege, sich diese Tabelleninhalte direkt anzeigen zu lassen, z.B. über Transaktionen wie SE16, SE16N, SE17 oder über Reports wie RK_SE16N. In diesen Tabellen befinden sich nun u.a. alle Mitarbeiterdaten, z.B. werden die Basisgehälter der Mitarbeiter in der SAP R/3®-Tabelle PA0008 abgelegt. Benutzer, die sich nun den Inhalt der Tabelle PA0008 anzeigen lassen können, sehen uneingeschränkt für alle Mitarbeiter die Basisgehälter.

   Diese Wege sind natürlich abzusichern, allerdings ist dies auf Grund der Vielzahl von Tabellen (ca. 35.000 Tabellen in SAP R/3® Enterprise) äußerst schwierig und zeitaufwendig. Und genau aus diesem Grund sind Tabellenberechtigungen in jedem R/3®-System ein Problem. Auch wenn von den Berechtigungen her der Zugriff auf Stammdaten eingeschränkt ist, so finden sich doch in jedem System Benutzer, die sensible Tabelleninhalte sehen dürfen. Mit diesem Recht ist es dann Benutzern auch evtl. möglich (mit ein wenig Programmierkenntnissen), die Tabellen per Fernzugriff z.B. mit MS Excel auszulesen und somit gleichzeitig einen Datenextrakt zu erstellen.

3. Über den Weg des Reportings

   SAP R/3® stellt eine Vielzahl von Reports zur Auswertung von Mitarbeiterdaten zur Verfügung. In diesen Reports werden die Zugriffsrechte zum Anzeigen der Mitarbeiterdaten benötigt. Allerdings kann dies auch durch ein einziges zusätzliches Recht umgangen werden. Es besteht die Möglichkeit, Benutzern das Recht zum Ausführen von Reports zu geben, ohne dass sie weitere Zugriffsrechte auf Mitarbeiterstammdaten besitzen. Auch dies sollte unterbunden werden.

4. Durch das Deaktivieren von Berechtigungsprüfungen

   Natürlich kann sehr viel in SAP R/3® konfiguriert werden, so auch, welche Berechtigungsprüfungen überhaupt stattfinden sollen. Im Modul HR wird dies über eine Customizing-Tabelle (Tabelle T77S0) gesteuert. Mit Änderungsrechten auf diese Tabelle können Berechtigungsprüfungen auf Mitarbeiterstammdaten vollständig deaktiviert werden, so dass alle Benutzer diese Daten ohne Zugriffsrechte sehen können. Hieraus ergeben sich noch viele weitere Problematiken, wie z.B. das Protokollieren von Tabellenänderungen, die Möglichkeiten zum Transport von Tabellenänderungen in das Produktivsystem, damit verbundene Freigabeverfahren usw.

Zur Absicherung dieser und vieler weiterer Möglichkeiten sind sehr umfangreiche Maßnahmen zu treffen. Die erste Problematik besteht für einen Datenschützer (und natürlich auch für die verantwortlichen Administratoren) darin, alle diesbezüglichen Möglichkeiten zunächst zu kennen, die abzusichern sind. Im zweiten Schritt tritt dann das Problem auf, dass für alle Möglichkeiten Sicherungsmaßnahmen zu treffen sind. Auch hier stellt sich immer wieder die Frage "Wie sichern wir das jetzt eigentlich ab?". Und nach jeder Absicherung ist natürlich ständig zu überwachen, dass die Sicherheitsmechanismen nicht umgangen, deaktiviert oder manipuliert werden.

...“Ein großer Bereich der Prüfung befasst sich mit der Umsetzung des internen Kontrollsystems der Unternehmung.“...

Allein der Punkt der Absicherung des Zugriffs auf sensible Daten stellt somit einen sehr komplexen und aufwendigen Teil der Gesamtsicherung eines SAP R/3®-Systems dar. Diese Absicherungen können mit Check**Aud** for SAP R/3® vollständig überprüft werden.

...“Ein großer Bereich der Prüfung befasst sich mit der Umsetzung des internen Kontrollsystems der Unternehmung....“

*Check**Aud** for SAP R/3® aus Sicht der Revision*

Die Revision fungiert als Kontrollinstrument des Vorstandes; sie prüft die reale Umsetzung der Vorstandsvorgaben, schaut "noch einmal" hin, ob die Fachbereiche und einzelnen Mitarbeiter in ihrer jeweiligen Arbeit Sicherheits-, Ordnungsmäßigkeits- und Wirtschaftlichkeitskriterien erfüllen und als erste Qualitätsinstanz selbst prüfen. Dies bezieht sich im Zusammenhang mit dem KonTraG auch auf die Planung und integrale Umsetzung eines Risikomanagementsystems.

Ein großer Bereich der Prüfung befasst sich mit der Umsetzung des internen Kontrollsystems der Unternehmung. Nachfolgend sind einige Vorgänge beschrieben, die von der Revision zu prüfen sind:

1. Freigabeverfahren

   Anwendungsentwicklung (und Customizing) findet grundsätzlich nicht im Produktiv-, sondern im Entwicklungssystem statt und wird transportiert. Bevor ein Import der Daten ins Produktivsystem erfolgt, muss jede Änderung oder Neuentwicklung im Qualitätssicherungssystem freigegeben werden. Diese Freigaben gestallten sich in der Praxis teilweise recht schwierig, da zum Freigeben gerade von z.B. ABAP-Programmen ein großes Know-How erforderlich ist, zum einen darüber, was das Programm inhaltlich tun soll, zum anderen über den kodierten Quelltext selbst, in dem sich sowohl Fehler als auch "Hintertürchen" befinden können. Die Unternehmung hat im Rahmen eines funktionierenden internen Kontrollsystems dieses Freigabeverfahren sicher zu implementieren. Die Revision hat die Aufgabe festzustellen, ob dieses Freigabeverfahren korrekt eingeführt und eingehalten ist.

2. IKS in den Fachabteilungen

   Für viele Bereiche innerhalb der Geschäftsprozesse einer Unternehmung werden Kontrollmechanismen implementiert, die teilweise darauf beruhen, dass bestimmte Vorgänge nicht von einer Person allein durchgeführt werden können oder andere Vorgänge explizit freigegeben werden müssen. Einige Beispiele hierfür sind:

   - Bestellanforderungen können generell von vielen Mitarbeitern angelegt werden. Bevor diese eine Bestellung auslösen können, müssen sie aber freigegeben werden. Diese Freigabe sollte dann nicht von dem Mitarbeiter selbst, sondern z.B. von einem Vorgesetzten erfolgen. Dies wird über das Berechtigungskonzept und über das Customizing (Definition von Freigabe-Codes) geregelt.

   - Das Ändern sensibler Eigenschaften von Kreditoren, z.B. die Bankverbindungen, sollte nur nach einem Vier-Augen-Prinzip erfolgen. Wird solch eine Eigenschaft geändert, soll ein zweiter Mitarbeiter diese Änderung kontrollieren und freigeben. Die Implementierung dieses Vorganges erfordert zum einen Einstellungen im Customizing (Definition der sensiblen Eigenschaften), zum anderen die Vergabe der entsprechenden Berechtigungen zum Ändern und Freigeben. Als zusätzlicher Schutz können einzelne Eigenschaften von Kreditoren geschützt werden, so dass nur entsprechend berechtigte Benutzer diese Eigenschaften überhaupt ändern dürfen. Auch hierfür müssen sowohl das Customizing entsprechend durchgeführt werden als auch die erforderlichen Zugriffsrechte vergeben werden.

   - Das Buchen von Kreditorenrechnungen und das Starten des Zahllaufs wird in vielen Unternehmungen personell getrennt. Diese Trennung

erfolgt systemseitig in SAP R/3® ausschließlich über das Berechtigungskonzept. Die Zugriffsrechte zum Buchen und für den Zahllauf werden dann keinem Benutzer in Kombination zugeordnet.

- Das Ändern von Mitarbeiterdaten im Personalwesen soll nach dem Vier-Augen-Prinzip erfolgen. Eine Änderung an einem Mitarbeiter soll durch einen anderen Sachbearbeiter im Personalwesen freigegeben werden. Hierfür bietet SAP R/3® über das Berechtigungskonzept zwei verschiedene Möglichkeiten.

  i. Symmetrisches Vier-Augen-Prinzip

     Dieses Prinzip beruht darauf, dass einige Sachbearbeiter Änderungsrechte besitzen, andere Freigaberechte. Zusammen werden diese Rechte aber nicht vergeben.

  ii. Asymmetrisches Vier-Augen-Prinzip

     Bei diesem Prinzip erhalten die Sachbearbeiter sowohl Änderungs- als auch Freigaberechte, können aber ihre eigenen Änderungen nicht freigeben, nur Änderungen anderer Sachbearbeiter.

3. Kritische Systemeinstellungen und Zugriffsrechte

Um ein produktives SAP R/3®-System abzusichern, müssen viele Einstellungen vorgenommen werden. Mit Zugriffsrechten ist dann abzusichern, dass diese Einstellungen nur von kleinen Personenkreisen vorgenommen werden dürfen. An Einstellungen wären dies z.B.:

- Das System muss sowohl vor Anwendungsentwicklung als auch vor Customizing geschützt sein.

- Änderungen an Tabellen, die als Verfahrensdokumentation gelten, sind zu protokollieren.

- Der Anmeldevorgang ist abzusichern, u.a. durch das Anfordern regelmäßiger Kennwortänderungen, durch Einstellungen zur Nutzung komplexer Kennwörter, durch das Festsetzen von Benutzersperrungen nach einer bestimmten Anzahl von Falschanmeldungen, durch das Hinterlegen verbotener Zeichenketten in Kennwörtern usw..

...“Eine umfassende, lückenlose Prüfung ist für einen Prüfer, auch für Teilbereiche von SAP R/3®, ohne Unterstützung von Prüfwerkzeugen nicht möglich.“...

Kritische Zugriffsrechte sind dann z.B.:

- Freischalten des Systems für Anwendungsentwicklung und Customizing

- Ändern der Systemparameter

- Ändern der Einstellung der Tabellenprotokollierung

- Durchführen von Customizing im Produktivsystem

Zur Prüfung dieser und vieler anderer Vorgänge im R/3®-System ist ein sehr großes Hintergrundwissen erforderlich, über den technischen Hintergrund des R/3®-Systems, das Berechtigungskonzept (es gibt über 1000 sog. Berechtigungsobjekte), die Customizing-Einstellungen (es gibt über 17.000 Customizing-Tabellen) und über die betriebswirtschaftlichen Hintergründe der einzelnen Module und deren Umsetzung in SAP R/3®.

Eine umfassende, lückenlose Prüfung ist für einen Prüfer, auch für Teilbereiche von SAP R/3®, ohne Unterstützung von Prüfwerkzeugen nicht möglich. Zwar bietet SAP hier einige Unterstützung an, aber trotzdem muss der Prüfer wissen, was er zu prüfen hat. Genau das nämlich wird von R/3 nicht vermittelt. Ebenso wenig die Vorgehensweise, wie denn nun ein bestimmter Punkt zu prüfen ist. Diese Problematiken werden durch Check**Aud** for SAP R/3® gelöst.

...“in erster Instanz ist jeder Fachbereich, jeder Mitarbeiter, selbst für sein Qualitätsmanagement verantwortlich.“...

*Check**Aud** for SAP R/3® aus Sicht der SAP-Administration*

Nach dem Ethik-Kodex für die Interne Revision des IIR (Deutsches Institut für Interne Revision e.V.) gel-

ten als maßgebliche einzuhaltende Ethik-Forderungen für Revisoren: Rechtschaffenheit, Objektivität, Vertraulichkeit, Fachkompetenz. Sind dies tatsächlich Spezifika der Revision? Diese Anforderungen sind doch wohl an jeden Mitarbeiter zu stellen!

In erster Instanz ist jeder Fachbereich, jeder Mitarbeiter, selbst für sein Qualitätsmanagement verantwortlich. In diesem Sinne hat er sein Customizing, seine Wartungs- und Pflegarbeiten, seine Arbeitsergebnisse selbst immer wieder in Frage zu stellen und zu prüfen: in der Sicherung seiner Arbeitsprozesse, in der Einhaltung von Gesetzen, Normen, betriebsinternen Regeln und Qualitätsstandards, in der Protokollierung und Dokumentation seines Arbeitsprozesses und in der Wirksamkeit (Effektivität) seiner Arbeitsergebnisse.

Insbesondere gilt dies natürlich auch für die Administratoren der SAP R/3®-Systeme. Diese zeichnen nicht nur verantwortlich für die ständige Verfügbarkeit der Systeme, sondern auch für die Systemsicherheit und die korrekte Umsetzung des Berechtigungskonzeptes. Nachfolgend einige Beispiele aus dem Verantwortungsbereich von SAP R/3®-Administratoren:

...“Eine besondere Problematik stellen die Schnittstellen zum R/3®-System dar, z.B. die RFC-Schnittstelle.“...

1. Negativtests

   Administratoren sind verantwortlich für die Definition der Zugriffsrechte in R/3®, den sog. Rollen. Nach dem Anlegen oder Ändern der Rollen müssen diese von der Fachabteilung entsprechend getestet werden ("Können mit den in der Rolle enthaltenen Berechtigungen alle erforderlichen Arbeitschritte durchgeführt werden?"). Dies ist der Positivtest der Rollen. In einem zweiten Schritt müssen die Verantwortlichen für die Rollen (die Benutzeradministratoren) nun testen, ob in den Rollen nicht zuviel Berechtigungen enthalten sind. Dieser wichtige Schritt ist der Negativtest, der im Verantwortungsbereich der Benutzeradministration liegt.

2. Absicherung der Schnittstellen

   Eine besondere Problematik stellen die Schnittstellen zum R/3®-System dar, z.B. die RFC-Schnittstelle. Über diese Schnittstelle ist es möglich, von anderen Programmen aus eine Verbindung zum SAP R/3®-System herzustellen und dort Aktionen auszuführen, sowohl rein lesende als auch ändernde. Solch eine Verbindung kann z.B. von MS Excel aus hergestellt werden. Hierüber ist es dann möglich, Funktionen im R/3®-System auszuführen. Eine spezielle Funktion (RFC_ABAP_INSTALL_AND_RUN) erlaubt es z.B., beliebige Quelltexte der Programmiersprache ABAP (Programmiersprache des R/3®-Systems) an das R/3®-System zu senden und diese dort ungeprüft ausführen zu lassen. Eine weitere Systematik ermöglicht per RFC evtl. einen Brute-Force-Attack auf R/3® ("Knacken" von Kennwörtern). Die Administratoren haben dafür Sorge zu tragen, dass diese Funktionalitäten unterbunden werden.

Gerade die große Komplexität des SAP R/3®-Systems erschwert für die Administration die Absicherung des Systems, ebenso wie der große Aufgabenbereich der Administration.

3. Dokumentationen

   Besonders wichtig ist die Dokumentation der vorgenommenen Einstellungen zur Systemabsicherung, zum Berechtigungskonzept, zum Customizing usw. Jede Änderung sollte nachvollziehbar sein, was zum einen über Protokolle im System möglich ist, zum anderen aber nur über manuelle Dokumentationen, evtl. außerhalb des R/3®-Systems. Dies stellt nicht nur große qualitative Anforderungen, sondern auch quantitative.

Gerade die große Komplexität des SAP R/3®-Systems erschwert für die Administration die Absicherung des Systems, ebenso wie der große Aufgabenbereich der Administration. Hierfür stellt Check**Aud** for SAP R/3® ein unentbehrliches Hilfsmittel dar.

Autor: Thomas Tiede

Auszug aus dem Tagungsband der 2. Hamburger Revisionstagung 2003
Ottokar Schreiber Verlag

Sicherheitskonzeption in SAP R/3® - Regelungsbedarf über die Berechtigungsdefinition und -vergabe hinaus

Von Dipl.-Betriebswirt Christoph Wildensee
IV-Revisor, Stadtwerke Hannover AG

In vielen Unternehmen läuft SAP R/3® reibungslos - gefahren von erfahrenen Administratoren und Systemtechnikern. Änderungen im Customizing werden jedoch auf Zuruf durchgeführt, wenn es die Notwendigkeit durch Fachbereichs- oder Systemerfordernisse gebietet. Ein dokumentiertes Berechtigungskonzept beinhaltet dort meist lediglich Regelungen, die die Vergabe und Verwaltung von Berechtigungen betreffen. Dies ist jedoch beim Betrieb eines solch umfassenden DV-Konstruktes nicht ausreichend, um Revisionsstandards zu erfüllen. Notwendig ist eine Zusammenführung von Regelungen, die den gesamten "Life-Cycle" des SAP-Systems und aller Komponenten dokumentiert, um den Betrieb nachvollziehbar, nachhaltig und mit Soll-Vorgaben zu gewährleisten.

Der SAP R/3® - Rahmen

Ein **Rahmenleitfaden** muss als Basis des Berechtigungskonzeptes gesehen werden, der alle zu regelnden Punkte systematisch aufnimmt und verbindliche Regelungen beinhaltet. Dabei soll er nicht nur für die technische Seite (Administration, Customizing) als Dokumentation und Nachschlagewerk dienen, sondern auch für die Key-User der involvierten Fachbereiche - den Modulnutzern - im Tagesgeschäft und letztlich auch für die nachvollziehenden Gremien (Datenschutz, Revision, Betriebsrat, IT-Sicherheitsbeauftragter etc.) als Dokumentation der Soll-Vorgaben, um sie am IST spiegeln zu können. Es ist z.B. oft feststellbar, dass die DV-Koordinatoren der Fachbereiche zu wenig Ein- und somit Übersicht über das System an sich haben, so dass die Beantragung und der Nachvollzug z.B. über Rechte, aber auch über Einstellungen in den Modulen, erschwert wird. Ein zentral bereitgestelltes Instrument wie der SAP R/3® - Rahmenleitfaden soll somit allen Informationsbedarf der Recherchierenden abdecken. Funktionsbeschreibungen der Module soll er dabei selbstverständlich nicht beinhalten.

Inhalte eines Rahmenleitfadens

Der administrative Aufwand in SAP R/3® ist sehr umfangreich, er reicht vom Einstellen des Systems selbst und der angrenzenden Komponenten wie Betriebssystem, Datenbank etc., dem Verwalten von

> „Der Regelungsbedarf ist mannigfaltig...“

Updates/Patches, dem Anpassen der Funktionalitäten über Eigenentwicklung bis zum Erteilen von Rechten und dem Verwalten von bestimmten Funktionen und Ressourcen. Der Regelungsbedarf ist mannigfaltig. Entsprechend umfangreich ist auch der Leitfaden, der zielführend gegliedert sein muss.

Abb. 1: Beispiel Teilinhaltsverzeichnis Leitfaden

Nachfolgend soll in tabellarischer Form beispielhaft dargestellt werden, welche Themen in einem Rahmenleitfaden eingearbeitet werden sollten (kein Anspruch auf Vollständigkeit).

Customizing, Administration, Dokumentation	
➔	Unterscheidung Produktions- / Test- [Integrations-] / Qualitätssicherungssystem
➔	Schulungssystem: Datenbestand und Anonymisierung / Pseudonymisierung, zu beachten: Kostenstellen (personalführende KSt, KSt von Einzelpersonen), Kostenarten, Reporting etc.
➔	Unterscheidung der Administratoren und Sonderuser (Modul-Administratoren, CPIC, SAP*, DDIC, HotlineSAP / Earlywatch etc. je System: ggf. SAP-Auslieferungsstatus, Kennwörter, Sperrung, Protokollierung usw.
➔	Systemstatus: Systeme, Instanzen, Prozesse, Verbuchung, User- / Transaktions- / Systemsperrungen, Änderbarkeitsstatus und -steuerung etc.
➔	Notfalluser-Konzept: User NOTFALL, Kennworthinterlegung, zweigeteiltes Kennwort, Nutzungserlaubnis, Kennwortdoppelerstellung und -verschluss
➔	Initialkennwortvergabe: Erstellung, Weitergabe zum User, Sperrung nach welcher Zeit bei Nicht-Nutzung
➔	Kennwortkonventionen, unzulässige Kennwörter etc.
➔	Systemparameter: Customizing jedes Systems, Dokumentation und Replik / Sicherung, Einstellungen zur R/3®-Oberfläche der Benutzer, zur Steuerung der Berechtigungsprüfungen, zur Benutzeridentifizierung und -authentifizierung und zum Logging, Dokumentation von Soll-Vorgaben und Ist-Werten, regelmäßiger Delta-Check, Meldewesen bei Systemänderungen
➔	Single-Sign-On (SSO): Parametrisierung, Synchronisation etc.
➔	Definition von Aufgaben / Kompetenzen / Verantwortung / Vorgehen im Customizing, bei Systemkopien u.ä. (z.B. auch Ablauforganisation, Terminierungen etc.)
➔	AIS: Customizing und Dokumentation, Aufbau von aufgabenorientierten bzw. fachbereichsspezifischen, vorparametrisierten Berichtszweigen, Laufzeitbeschränkungsdefinitionen etc.
➔	Organisation / Business-Strukturen: Dokumentation der Einstellungen: BUKRS, KOKRS, Perioden, Belegarten, Nummernkreise, Klassifizierungen von Mitarbeitern, Tabellen, ABAP's etc., Infotypen, Subtypen, Mitarbeitergruppen etc., Namenskonventionen, Namensräume etc.
➔	SAP-Prozesse und Freigaben
➔	Schnittstellen zu anderen R/3®-Systemen und zur weiteren DV-Landschaft, RFC, iDoc etc., Dokumentation und Freigabeverfahren, Funktionsbausteinaufrufe, Unterscheidung kritischer Aufruf- / Ansteuerungsmöglichkeiten, Schnittstellenbeschreibungen
➔	eProcurement: Schnittstellendefinition zwischen externem Tool (z.B. Enterprise Buyer Prof. [EBP]) und SAP R/3®, Verfahrensbeschreibung der Datenübergabe und des Berechtigungskonzeptes, Zugriff für Fachbereiche
➔	Batch-Input: Steuerung der Zugriffe (wer darf Batch-Input nutzen, für welche Systeme, Zwecke, Fachbereiche wird es freigegeben etc.), Namenskonventionen, Berechtigungsobjekteingrenzung, Klassifizierung, Verfahrensbeschreibung, Fachbereichsspezifika,

Customizing, Administration, Dokumentation	
➔	Tabellenpflege: Steuerung der Zugriffe, restriktiver Einsatz, Berechtigungsobjekteingrenzung, Nutzung der Klassifizierung etc.
➔	Debugging: Wer darf im Debugging arbeiten, restriktiver Einsatz des Edit-Modus, Vier-Augen-Prinzip durch unzureichende Protokollierung, nur Einsatz durch Fachbereichserfordernis, Dokumentation revisionssicher (vorher/nachher), zentrale Dokumentation zwecks Nachvollzug und Abgleichmöglichkeit mit SM21 => Meldungskennungen A14/A19
➔	Spool-Verwaltung: Berechtigungsobjekteingrenzung, kritische Ausprägungen, Klassifizierung
➔	Job-Verwaltung: Berechtigungsobjekteingrenzung, kritische Ausprägungen, Klassifizierung, sofern externes Jobsteuerungs- u/o ggf. Druckoutputmanagementsystem zum Einsatz kommt: Definition von Sicherheitsmaßnahmen, auch im Hinblick auf Schnittstellen zum Betriebssystem (Job-Weitergabe, Druck-Server, Vertrauensbeziehungen, auch Archivierung etc.)
➔	Computing Center Management System (CCMS): Monitoring, Leitstand, Datenbanktools, restriktiver Einsatz
➔	Employee Self Service (ESS) / anwendungsübergreifendes Arbeitszeitblatt (cross application time sheet (CATS))
➔	HR: Organisations- und Steuerungsstrukturen der Personalwirtschaft, z.B. Organisation: Personal(teil)bereich, Mitarbeitergruppe / -kreis, Personalabrechnungskreis, Infotypen / Subtypen, Lohnarten etc.; Steuerung: P_ORGIN, P_ORGXX, P_PERNR, P_PCLX, P_PY*, P_ABAP etc.
➔	Human Information System (HIS) - vorparametrisierte Auswertungen für HR
➔	Reporting / Berichtsbäume / Infosysteme der Einzelmodule, Query-Tools (auch externe)
➔	Änderungshistorie, Protokollierung und die Auswertung dieser Informationen: SysLog, AuditLog, Unterscheidung kritischer Meldekennungen, protokollierte User je System etc.
➔	Festlegung von systemkritischen (zu überwachenden) Zuständen, kritische / sensible Daten / Informationen und kritische Berechtigungsobjektausprägungen / -konstellationen (Tabellen, Reports, Transaktionen, Berechtigungsobjekte, Objekteingrenzungen) [...]

Betriebssystem, Datenbank	
➔	Übersicht Betriebssystem- und Datenbankdienste, Ablagestrukturen
➔	kritische Dienste und Verzeichnisse auf den Application-Servern und den Freigaben hierauf
➔	Dokumentation der Betriebssystem- und Datenbankadministratoren
➔	zu überwachende Dienste, Verzeichnisse, Dateien; Vertrauensbeziehungen und deren Wirkung
➔	Remote-Zugriffe und Internet-User etc.
➔	Definition von Sicherheitsmaßnahmen auf Betriebssystem- und Datenbankebene, Einbezug der SAP R/3®-Sicherheitsleitfäden, auch Datenschutzanforderungen integrieren [...]

Changemanagement	
➔	Systemänderungen durch Umgang mit Hot Packages, Legal Change Packages und Eigenentwicklungen incl. Übernahme in die Produktionsumgebungen, Unterscheidung von Fehler korrekturen / Erweiterungen durch Extern-Anstoß und Fehlerkorrekturen / Neue Funktionen durch Intern-Anstoß > kundeneigener Entwicklungs- / Namensraum > Zeitplanung / Terminierungen > Ressourcenplanung > Dokumentation
➔	Definition von Standards bei der Implementierung neuer Funktionen
➔	Testverfahren: Definition, Durchführung, Verantwortung, Abnahme, Dokumentation
➔	Test systemgestützt erleichtern, Automation von Testfällen, sofern möglich
➔	regelmäßige Verifizierung von Testverfahren, Katalog abgestimmter Testverfahren, ggf. prozessbezogen
➔	Notfallplan für Systemstillstand
➔	Entwicklung: Regelung je System, Trennung von Entwicklung und Produktionsumgebung, Transportwesen / -auftrag, Entwickler- und Objektschlüssel
➔	Report-Entwicklung: QS-Maßnahmen > Systemabgrenzung: Welche Systeme werden für welche Aufgaben genutzt ? > Dokumentation / Entwicklerrichtlinie, Namenskonventionen, standardisierte Doku-Pflicht > Abnahmetest der Funktion, Handhabung, Ergebnisse, Zielkonformitätsuntersuchung > Transportwesen > Abgrenzung der Einbindung von Revision / bDSB / IT-Sicherheit in Abhängigkeit des Manipulationsgrades auf Tabellen
➔	Computer Aided Test Tool (CATT) > Ziel: Frühzeitiges Aufzeigen von Fehlerquellen, Vereinheitlichung / Standardisierung und beliebige Wiederholbarkeit von Testabläufen, Automatisierung von Testabläufen, Erzeugung von Schulungsdaten, einheitliche Dokumentation von Tests > beinhaltet: Aufzeichnungstool für Prozesse, Workbench zur Verwaltung von Testprozeduren, Wiedergabebereich für Testprozesse > benötigt: Geschäftsprozessdefinition, beteiligte Transaktionen und zugrundeliegende Daten > Grundsatz: Nicht alle Prozesse und Transaktionen können aufgezeichnet werden => Abgrenzung manuell vs. automatisiert; zu beachten: Öffnung/Änderbarkeit des Systems > Beantragungs- und Freigabedefinition, CATT-Testkatalog [...]

Berechtigungsvergabe und -verwaltung	
➔	Grundsätze der Berechtigungsvergabe und -verwaltung, Funktionstrennungsprinzip, Restriktivhandhabung, Prozessübersicht der B.-vergabe und -verwaltung, Namenskonventionen für die Elemente der B.-verwaltung, Definition von Aufgaben, Kompetenzen, Verantwortung

Berechtigungsvergabe und -verwaltung

➔ Benutzerstammsatz

> Neuanlage: Welche Daten werden gepflegt ? Klassifizierung von Nutzern, wer darf Neuanlage durchführen, welche Rechte sind mit der Steuerung verbunden ? Wie sind diese aufzuteilen auf die Administratoren ?
> Änderung: Stammdatenänderung, Rechtezuweisungsänderung, Kennwortänderung
> Sperren / Löschen: Wer darf eine Sperrung / Entsperrung / Löschung veranlassen und durchführen ? Sonderfall Externe, Befristung, Austritt eines Nutzers aus dem Unternehmen

➔ Rollendefinitionen

> Anlegen / Ändern / Löschen von Rollen
> Fachbereichstest der Rollen, Abnahme- / Freigabeverfahren, Überführen in Produktionsumgebung, Namenskonventionen, Dokumentation der Rollen
> Kontrollverfahren bei der Rollendefinition (z.B. bei Rollenkollisionen)
> Einstellungen zum Transport von Rollen und Benutzerabgleich
> Einbezug von Revision / bDSB / IT-Sicherheit von kritischen Rollen

➔ Profilgenerator (PFCG)

> Wer nutzt den Profilgenerator bei welchen Aufgaben ?
> Profilgenerator ist auch als Nachvollzugsinstrumentarium einsetzbar
> Ausschließlichkeitsprinzip zur Nutzung von PFCG bei der Rollendefinition vs. Grundsatz der PFCG-Nutzung bei der Rollendefinition mit gelegentlicher manueller Rollendefinition im Bedarfsfall (Sonderuser)
> Überprüfung der Profilgenerator-Ergebnisse durch wen, wie, Dokumentation und Veränderungsprozedur
> Grundsatz der Redundanzfreiheit von Berechtigungen in den Rollendefinitionen, Sicherstellung und Nachvollzug

➔ Profile und Berechtigungen

> Namenskonventionen und Dokumentation der Elemente
> Kritische Berechtigungen / Berechtigungsobjektkonstellationen und -kombinationen
> Definition und Dokumentation überwachungsbedürftiger Berechtigungsobjektausprägungen und Transaktionen, bei denen eine restriktive Handhabung notwendig ist
> Zustimmungsverfahren bei Zugriff auf überwachungsbedürftige Berechtigungen
> Übersicht / Dokumentation über Profile / Berechtigungen zu definierten Rollen
> Definition nachgelagerter, regelmäßiger Kontrollen der Rollen / Berechtigungen / Profile

➔ Sonderuser und deren Behandlung

> Systemuser, Notfall, Administratoren, Key-User der Fachbereiche (DV-Koordinatoren, SAP-Modul-Ansprechpartner o.ä.)
> Auszubildende (ggf. als Sammler umfassender Berechtigungen durch das ‚Durchlaufen' in den einzelnen Unternehmensbereichen und dem häufigen Einbeziehen in das Tagesgeschäft, zu beachten: zeitlich befristete Vergaben von Rollen möglich !)
> Externe (Berater, Wirtschaftsprüfung, Betriebsprüfung)
> Sicht-User (Revision, bDSB, IT-Sicherheit, ggf. Betriebsrat), zu regeln: umfassende Sicht, CCMS-Funktionalitäten, Tabellen, ABAP-Workbench etc. [...]

Berechtigungen und Fachbereiche	
➔	Übersicht der Menü- und Modul-Rollen im Unternehmen je Fachbereich
➔	Zur-Verfügung-Stellen eines Nachvollzugsinstrumentariums für die Fachbereiche, z.B. AIS
➔	Definition einer zentralen Anlaufstelle zur Klärung von Fragen zum Berechtigungskonzept, z.B. Revision und bDSB, zusätzliche Funktionalitätsbereitstellung für diese, z.B. Check**Aud** for SAP R/3®

Sonstiges	
➔	Aufbewahrungspflichten und zu beachtende Fristen
➔	Archivierungssysteme (Schnittstellen, Sicherungs- und QS-Maßnahmen)
➔	gesetzliche Anforderungen
➔	Formularwesen
➔	Ansprechpartner und Verantwortliche im Unternehmen
➔	Schulungskonzept
➔	Interne Hotline: Aufgaben, Kompetenzen, Verantwortung, Definition einer Ablauforganisation
➔	Qualifikationsdefinitionen für Key-User [...]

Fazit

Meines Erachtens reicht allein die Festlegung von Rahmenbedingungen für die Berechtigungssteuerung längst nicht aus, um ein solch umfassendes System nachvollziehbar zu fahren. Die unterschiedlichen SAP-Nutzergruppen und deren jeweiliger Informationsbedarf sind so zu berücksichtigen, dass bei einer Zusammenführung von verbindlichen Regelungen zu einem umfassenden SAP R/3®-Rahmenleitfaden ein sinnvolles Betriebsführungs- und Nachvollzugsinstrumentarium zur Verfügung gestellt werden kann. Lediglich systemkritische / sensible Informationen wie IP-Adressen u.ä., die einen Geheimhaltungsstatus genießen müssen, sollten aus dem zentralen Leitfaden herausgelöst werden bzw. bleiben.

Literatur:

Thomas Tiede
Ordnungsmäßigkeit und Prüfung des SAP-Systems (OPSAP),
OSV Ottokar Schreiber Verlag

Geesmann, Glauch, Hohnhorst
SAP R/3® Datenschutz und Sicherheitsmanagement,
OSV Ottokar Schreiber Verlag

Christoph Wildensee
Ausgesuchte Berechtigungsobjekte des SAP R/3®-Systems als Prüfansatz für die IV-Revision,
ReVision III/2001-I/2002

Christoph Wildensee
SAP R/3® - Besonderheiten des Systems bei der Prüfung des Berechtigungskonzeptes, ZIR 4/2002

Christoph Wildensee
www.wildensee.de/veroeff.htm

Revisionsspezifische Ordnungsmäßigkeitskriterien:

u.a. GoB, HGB, AktG, ergänzend KonTraG,
FAMA/ERS FAIT1, EPS330

Crash-Kurs, Teil III: Die Basissicherheit einer SAP R/3®-Systemlandschaft

Von Thomas Tiede
Geschäftsführer, ibs schreiber gmbh, Hamburg

In den ersten beiden Teilen dieses Crash-Kurses wurden Sicherheitseinstellungen behandelt, die alle Systeme einer R/3®-Systemlandschaft sowie die einzelnen Systeme selbst betreffen. Dieser Teil befasst sich mit Sicherheitseinstellungen in den einzelnen Mandanten eines R/3®-Systems, maßgeblich natürlich den Produktivmandanten.
Zu jedem Vorgang sind auch hier wieder die Zugriffsrechte dargestellt, sowohl die Anwendungsberechtigungen als auch (wenn sinnvoll) die notwendigen Transaktionsberechtigungen. Geprüft werden können diese Zugriffsrechte am besten mit dem Report RSUSR002.

Die Benutzerverwaltung

Benutzer werden in SAP R/3® mandantenbezogen angelegt. In jedem Mandanten, in dem ein Benutzer arbeiten soll, muss ein Benutzerkonto für ihn definiert werden. Administratoren benötigen daher u.a. Zugriff sowohl auf den Produktivmandanten, als auch auf den Systemmandanten 000, da von dort aus z.B. Support-Packages eingespielt werden müssen. Prüfungen von Zugriffsrechten von Benutzern sind daher immer mandantenbezogen durchzuführen. Zugriffsrechte auf betriebswirtschaftliche Vorgänge, z.B. im Einkauf oder der Finanzbuchhaltung, sind grundsätzlich mandantenbezogen. Administrative Zugriffsrechte gehen teilweise darüber hinaus, z.B. beim Zugriff auf den Drucker-Spool (siehe Teil 2).

Zur Verwaltung von Benutzern in SAP R/3® können die Transaktionen SU01, OIBB, OPCA und OOUS sowie der Report SAPMSUU0 genutzt werden. Durch den Report SAPMSUU0 ist somit die Benutzerpflege z.B. auch mit den Transaktionen SA38, SE38 und START_REPORT möglich. Zusätzlich stellt R/3® noch alte Transaktionen zur Benutzerpflege zur Verfügung, mit der keine Rollen zu Benutzern gepflegt können, sondern nur Profile. Dies sind die Transaktionen OPF0, OPJ0 und OVZ5. Eine reine Anzeige der Benutzerdaten ist mit der Transaktion SU01D möglich. Diese Transaktion sollte Prüfern generell zur Verfügung stehen.

Benutzer werden für die Rechterverwaltung in Gruppen eingeteilt. Für diese Gruppen können dann Zugriffsrechte vergeben werden. Welche Benutzer in welcher Gruppe Mitglied sind kann entweder über die Transaktion SU01D ermittelt werden oder über die Tabelle USR02. In dieser Tabelle werden die Anmeldedaten aller Benutzer gespeichert, u.a. auch die Benutzergruppe. Sie können sich diese Tabelle z.B. mit den Transaktionen SE16 oder SE16N anzeigen lassen.

Zur Überprüfung, welche Benutzer Aktionen innerhalb der Benutzerverwaltung ausführen dürfen, müssen folgende Zugriffsrechte überprüft werden:

Berechtigungsobjekt S_USER_GRP (Benutzergruppen)

Aktivität: 01 (Anlegen)
02 (Ändern)
03 (Anzeigen)
05 (Sperren / Entsperren / Kennwörter-vergeben)
06 (Löschen)

Benutzergruppe:
<Kann angegeben werden, wenn Aktionen auf bestimmte Benutzer überprüft werden sollen. Die Benutzergruppe ist im Stammsatz (Transaktion SU01D) oder in der Tabelle USR02 einzusehen>

Zur Überprüfung, wer Benutzern Rollen zuordnen darf, sind folgende Zugriffsrechte zu überprüfen:

Berechtigungsobjekt S_USER_GRP (Benutzergruppen)

Aktivität: 02 (Ändern)
22 (Zuordnen)

Benutzergruppe:
<Kann angegeben werden, wenn Aktionen auf bestimmte Benutzer überprüft werden sollen>

Berechtigungsobjekt S_USER_AGR (Rollen)

Aktivität: 22 (Zuordnen)
Rolle:
<Kann angegeben werden, wenn das Zuordnen bestimmter Rollen überprüft werden soll>

Zur Auswertung von Benutzereigenschaften können u.a. folgende Reports genutzt werden:

Der Report RSUSR002 - Benutzer nach komplexen Selektionskriterien

Einige Fragestellungen zu Benutzern können mit dem Standardreport RSUSR002 abgedeckt werden. In diesem Report werden als Ergebnis immer die Benutzer mit ihren Gruppen und zugeordneten Profilen angezeigt. Folgende Selektionsmöglichkeiten stellt der Report zur Verfügung:

- Gruppenzugehörigkeiten
- Zugeordnete Profile
- Abrechnungsnummer
- Startmenü
- Ausgabegerät
- Benutzer mir einem bestimmten Ablaufdatum
- Gesperrte Benutzer
- Benutzer mit CATT-Kennzeichen

Der Report RSUSR006 - Benutzer mit Falschanmeldungen

Dieser Report zeigt Benutzer an, die Falschanmeldungen haben, die somit bei der Anmeldung ein falsches Kennwort eingegeben haben. Ebenso werden Benutzer angezeigt die durch einen Administrator oder durch Falschanmeldungen gesperrt sind. Der Report zeigt diese Informationen mandantenübergreifend für alle Mandanten des Systems an.

Der Report RSUSR200 - Liste der Benutzer nach Anmeldedatum und Kennwortänderung

Dieser Report bietet folgende Auswertungsmöglichkeiten:

- Benutzer mit Initialkennwort
- Benutzer seit x Tagen nicht mehr angemeldet
- Benutzer, die seit x Tagen ihr Kennwort nicht mehr geändert haben

Die Selektionen können eingeschränkt werden auf aktive Benutzer und Dialog-Benutzer.

Referenzbenutzer

Den Benutzertyp Referenz gibt es seit dem R/3®-Release 4.6C. Sie dienen dazu, Zugriffsrechte an andere Benutzer weiterzugeben. Einem Referenzbenutzer werden Rechte zugeordnet. Jedem Benutzer kann genau ein Referenzbenutzer zugeordnet werden, dessen Rechte er bei der Anmeldung zusätzlich zu seinen eigenen erhält. Referenzbenutzer können sich nicht ans System anmelden. Sie werden maßgeblich dazu genutzt, Internet-Benutzer mit identischen Rechten auszustatten.

Wichtig: Die durch einen Referenzbenutzer zugeordneten Rechte werden bei der Auswertung von Zugriffsrechten bei SAP R/3® (z.B. mit dem Report RSUSR002) nicht beachtet!

Die Zuordnungen von Referenzbenutzern zu Benutzern werden in der Tabelle USREFUS gespeichert. In dieser Tabelle sind allerdings alle Benutzer aufgelistet. Um die Benutzer anzuzeigen, denen ein Referenzbenutzer zugeordnet wurde, müssen Sie im Feld Referenzbenutzer (REFUSER) die Selektionsoption Ungleich auswählen und das Feld leer lassen (siehe Abb. 1).

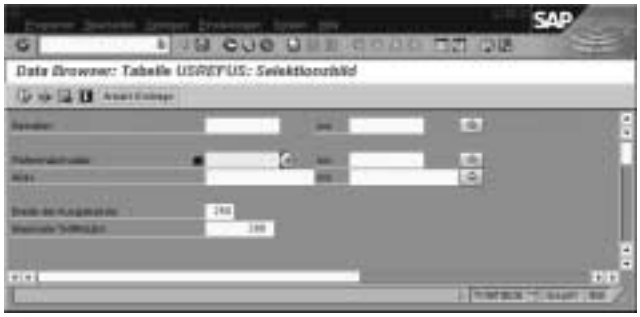


Abb. 1: Tabelle USREFUS - Selektion von Benutzern mit Referenzzuordnung

Existieren Referenzbenutzerzuordnungen, so ist dies bei der Auswertung von Zugriffsrechten zu beachten. Hier gilt dann:

Wird beim Auswerten von Zugriffsrechten ein Referenzbenutzer als Berechtigter angezeigt, so besitzen außerdem alle Benutzer, denen er zugeordnet wurde, ebenfalls dieses Recht.

Das Ergebnis der Berechtigungsprüfung ist dann um den Auszug aus der Tabelle USREFUS mit den zugeordneten Benutzern zu erweitern.

Es können allerdings nicht nur Referenzbenutzer, sondern auch normale Benutzer (Dialog, Kommuni-

kation, System) anderen Benutzern als Referenz zugeordnet werden. Da dies meist nicht gewünscht ist kann diese Funktion deaktiviert werden. Hierzu ist in der Tabelle PRGN_CUST der Schalter REF_USER_CHECK auf den Wert E zu setzen (siehe auch OSS-Hinweis 513694). Um zu überprüfen, wie dieser Schalter konfiguriert ist, lassen Sie sich die Tabelle PRGN_CUST mit der Transaktion SE16 anzeigen. Ist der Schalter REF_USER_CHECK gar nicht in der Tabelle eingetragen, so können auch Dialog-Benutzer als Referenz zugeordnet werden.

In vielen Systemen sollen Referenzbenutzer nicht genutzt werden. Hier besteht die Möglichkeit, dies über eine Transaktionsvariante zur Transaktion SU01 zu deaktivieren. Wie dies funktioniert ist im OSS-Hinweis 330067 beschrieben. Nach der Implementation dieses Hinweises sind Referenzbenutzer entweder gar nicht mehr möglich oder nur noch für bestimmte Personenkreise, je nach Notwendigkeit für die Unternehmung.

Protokollierungen der Berechtigungsverwaltung

Änderungen an Benutzern und Berechtigungen müssen nachvollziehbar sein. Daher werden diese Änderungen automatisch von R/3® aufgezeichnet. Folgende Änderungen am Benutzerstammsatz werden protokolliert:

- Kennwortänderungen
- Änderungen der Benutzergültigkeit (Ablaufdatum)
- Änderungen des Benutzertyps
- Ändern der Zuordnung zur Benutzergruppe
- Sperren des Benutzers durch Falschanmeldungen
- Sperren des Benutzers durch einen Administrator
- Entsperren eines Benutzers

Diese Änderungen werden in der Tabelle USH02 (Änderungshistorie für Logon-Daten) gespeichert. Zu jeder Änderung werden Datum und Uhrzeit der Änderung sowie der Name des Änderers angegeben.

Die Zuordnung von Profilen zu Benutzern sowie das Anlegen und Löschen von Benutzern wird in der Tabelle USH04 (Änderungshistorie Berechtigungen) gespeichert. Hier wird protokolliert, wenn

- ein Benutzer angelegt wird,
- ein Benutzer gelöscht wird,
- Profilzuordnungen des Benutzers geändert werden.

Ausgewertet werden diese Änderungen mit dem Report RSUSR100 In der Selektionsmaske des Reports kann der auszuwertende Zeitraum eingeschränkt werden sowie die Anzeige bestimmter Benutzer. Durch die Kontrollkästchen Änderungen an Rechten (Auswertung der Tabelle USH04) und Änderungen an Headerdaten (Auswertung der Tabelle USH02) wählen Sie aus, was dieser Report anzeigen soll. Für verschiedene Fragestellungen sollte dieser Report mehrfach aufgerufen werden, da ansonsten zu viele (nicht mehr auswertbare) Informationen angezeigt werden.

Es empfiehlt sich, diesen Report für folgende Fragestellungen einzeln aufzurufen:

- Welche Benutzer wurden neu angelegt?
- Welche Benutzer wurden gelöscht?
- Welchen Benutzern wurden kritische Profile (SAP_ALL, SAP_NEW, S_A.SYSTEM, S_A.DEVELOP, Z_ANWEND, ...) zugeordnet?
- Welchen Benutzern wurden kritische Profile entzogen?
- Welche Benutzer wurden durch einen Administrator gesperrt?
- Welche Benutzer wurden durch Falschanmeldungen gesperrt?
- Wann wurden gesperrte Benutzer wieder entsperrt?

Abb. 2 zeigt beispielhaft die Selektion zum Anzeigen aller Benutzer, die im Jahr 2002 das Profil SAP_ALL zugeordnet bekommen haben.

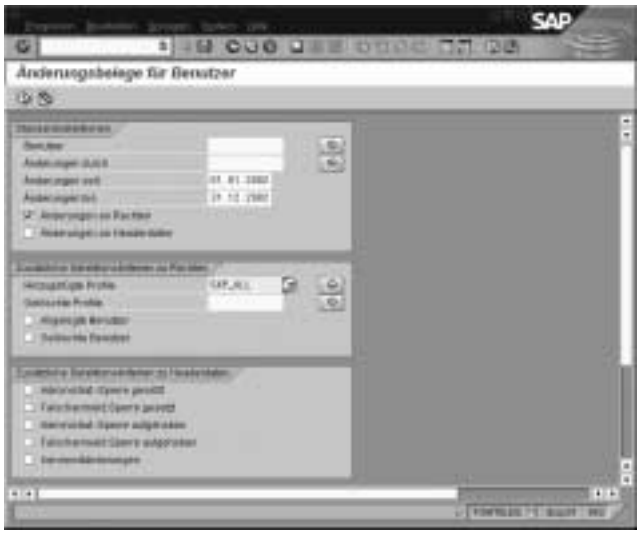


Abb. 2: Report RSUSR100 - Benutzer, denen das Profil SAP_ALL zugeordnet wurde

Nicht ausgewertet werden können die Zuordnungen von Benutzern zu Rollen, da hierüber keine Ände-

rungsbelege erzeugt werden. Dies ist allerdings in vielen Fällen wünschenswert, da häufig für die Profile zu Rollen die von R/3® vorgeschlagenen Standardnamen verwendet werden und darüber die Zuordnungen nur mit viel Aufwand herauszufinden sind. In diesem Fall ist die Tabelle AGR_USERS der Tabellenprotokollierung hinzuzufügen (zur Tabellenprotokollierung siehe Teil 1). In dieser Tabelle werden die Benutzerzuordnungen zu Rollen gespeichert.

Ebenfalls nicht protokolliert werden Zuordnungen von Referenzbenutzern. Um dies auswerten zu können, muss die Tabelle USREFUS ebenfalls in die Tabellenprotokollierung mit aufgenommen werden.

Die SAP R/3® Sonderbenutzer

Bei der Installation eines R/3®-Systems werden in den einzelnen Mandanten einige Standardbenutzer angelegt, die teilweise über weitgehende Rechte verfügen. Diese Benutzer sind mit Standardkennwörtern ausgestattet, die allgemein bekannt sind. Die Kennwörter sollten sofort nach der Installation geändert werden. Nachfolgend sind diese Benutzer und ihre Absicherungen beschrieben.

SAP*

Der Benutzer SAP* existiert nach der Installation eines R/3®-Systems in allen Mandanten. Er besitzt das Profil SAP_ALL und somit alle Berechtigungen des Systems. Er ist ein fest codierter Initialbenutzer. Wird der Benutzer SAP* gelöscht, so ist danach trotzdem noch eine Anmeldung mit dem Standardkennwort PASS möglich. Zugriffsrechte werden in dem Fall für diesen Benutzer nicht überprüft. Lediglich die Anwendungsentwicklung ist mit ihm nicht möglich. Es stellt daher eine große Sicherheitslücke dar, wenn dieser Benutzer gelöscht wird.

Standardkennwort:	In den Mandanten: 6071992 Initialkennwort wenn er nicht existiert: PASS

Zur Verhinderung einer Neuanmeldung des SAP* nach einem Löschen kann der Parameter login/no_automatic_user_sapstar genutzt werden. Wird der Wert dieses Parameters auf 0 gesetzt, so ist eine Neuanmeldung möglich. Bei dem Wert 1 ist eine Anmeldung nach dem Löschen nicht mehr möglich.

Mit dem Benutzer SAP* soll folgendermaßen verfahren werden:

SAP* wird deaktiviert. Hierzu werden dem Benutzer alle Berechtigungen entzogen, er wird gesperrt und der Parameter login/no_automatic_user_sapstar wird auf "1" gesetzt. Außerdem wird er der administrativen Gruppe des SAP-Systems (in den meisten Fällen die von SAP vorgegebene Gruppe SUPER) als Mitglied zugeordnet. Somit wird eine Nutzung dieses Benutzers verhindert. Die Verwaltung dieser Gruppe sollte nur nach dem Vier-Augen-Prinzip erfolgen.

Sehr kritisch ist das Zugriffsrecht zum Löschen des Benutzers SAP*, da nach diesem Vorgang eine Anmeldung mit dem Kennwort PASS möglich ist. Folgendes Recht ist hierfür notwendig:

Berechtigungsobjekt S_USER_GRP

Aktivität:	06 (Löschen)
Benutzergruppe:	<Benutzergruppe des Benutzers SAP*, standard mäßig SUPER>

DDIC

DDIC ist mit den vollständigen Rechten zur Verwaltung des Repositories (die Entwicklungsumgebung) von R/3® ausgestattet. Der Zweck des Benutzers DDIC ist es, sich während Installations- oder Releasewechselarbeiten anzumelden und als einziger Änderungen am Data-Dictionary vornehmen zu können. Lediglich die Benutzung des Korrektur- und Transportwesens ist ihm nur im Anzeigemodus gestattet, womit zwangsläufig Eigenentwicklungen ausgeschlossen sind. Er ist bei der Installation nur in den Mandanten 000 und 001 angelegt. Ebenso existiert er in den Produktivmandanten. Dieser Benutzer wird in allen Mandanten für Importe genutzt und darf nicht gelöscht werden. Er wird allerdings nur im Mandanten 000 als Dialog-Benutzer benötigt, in allen anderen Mandanten sollte er auf den Benutzertyp System gesetzt werden, da es sich hier um einen nicht personifizierten Sammelbenutzer handelt. Damit sind Anmeldungen unter seiner Kennung insbesondere im Produktivmandanten ausgeschlossen.

Standardkennwort:	**19920706** **SAPCPIC**

Der Benutzer SAPCPIC ist ein Benutzer vom Typ Kommunikation und wird ebenfalls während der

Installation des Systems angelegt und dient zur EDI-Nutzung. Die Standardberechtigungen dieses Benutzers beschränken sich auf RFC-Zugriffe.

Der Benutzer SAPCPIC wird allerdings im ABAP-Programm LSXPGU01 verwendet, wo auch sein Standardkennwort in Klarschrift hinterlegt ist. Dieses Programm muss bei einer Kennwortänderung ebenfalls geändert werden.

Standardkennwort: **ADMIN**

TMSADM

Der Benutzer TMSADM wird bei der Einrichtung des Transport Management Systems automatisch im Mandanten 000 angelegt. Er ist ein Benutzer vom Typ Kommunikation und wird vom TMS für Transporte genutzt. Standardmäßig verfügt er über das Profil S_A.TMSADM, über welches er Schreibrechte im Dateisystem, notwendige RFC Ausführungsberechtigungen für das TMS und Anzeigeberechtigungen für die Elemente der Entwicklungsumgebung und für Stücklisten erhält. Weitere Rechte müssen ihm nicht zugeordnet werden.

Standardkennwort: **PASSWORD**

Prüfen der Sonderbenutzer mit dem Report RSUSR003

Der Report RSUSR003 (Abb. 3) überprüft mandantenübergreifend, ob die oben beschriebenen Benutzer (außer dem Benutzer TMSADM) in den einzelnen Mandanten vorhanden sind, und ob ihre Standardkennwörter geändert wurden. Das Ausführen des Reports ist mit Prüferberechtigungen (nur Anzeigen) nicht möglich. Benötigt werden das Recht zum Ändern mandantenunabhängiger Tabellen sowie das Recht zum Ändern der Gruppe SUPER. Daher kann dieser Report nur von einem entsprechend berechtigten Administrator aufgerufen werden.

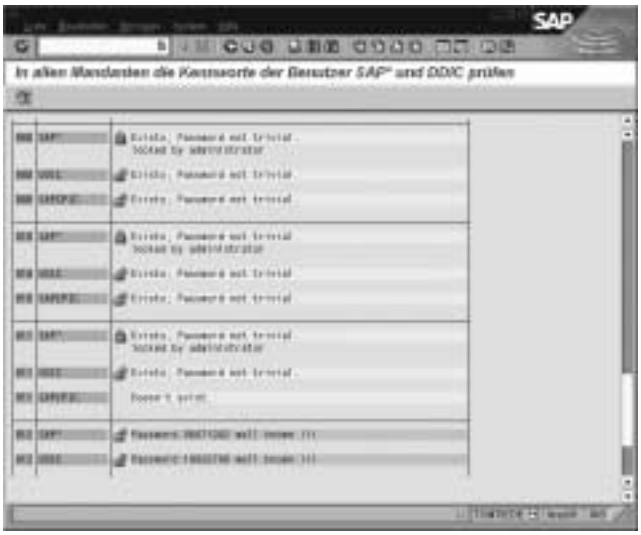


Abb. 3: Report RSUSR003 - Kennwörter der Sonderbenutzer prüfen

Abb. 3 zeigt einen Ausschnitt aus diesem Report. In der ersten Spalte wird der Mandant angezeigt. Für den Mandanten 800 ist zu erkennen, dass der Benutzer SAP* existiert, sein Standardkennwort geändert wurde und er von einem Administrator gesperrt wurde. Für den Mandanten 812 ist zu erkennen, dass er dort noch sein Standardkennwort 06071992 besitzt.

Deaktivieren von Berechtigungsprüfungen

In SAP R/3® besteht die Möglichkeit, Berechtigungsobjekte (und damit die Berechtigungsprüfungen) zu deaktivieren. Dies sollte im Produktivsystem bzw. -mandanten unterbunden werden. Folgende Möglichkeiten zur Deaktivierung sind möglich:

Vollständiges Deaktivieren von Berechtigungsobjekten

Berechtigungsobjekte können pro Mandant vollständig deaktiviert werden. Das bedeutet, dass in den Vorgängen, in denen ein Berechtigungsobjekt normalerweise überprüft wird, dieses nun nicht mehr benötigt wird.

Z.B. werden zur Verwaltung von Kreditoren Berechtigungen auf Berechtigungsobjekten benötigt, die mit F_LFA1* beginnen. Werden all diese Berechtigungsobjekte nun deaktiviert, so sind zur Kreditorenverwaltung keinerlei Zugriffsrechte mehr notwendig und alle Benutzer können diese Aktionen durchführen (Transaktionsberechtigung voraus gesetzt).

Einzige Einschränkung: Berechtigungsobjekte der Basis (S*) und des Personalwesens (P*) können hier nicht deaktiviert werden. Von allen anderen Modulen ist dies möglich.

Das Deaktivieren erfolgt entweder über die Transaktion AUTH_SWITCH_OBJECTS oder den Report BERE_GLOBAL_SWITCH_OF_OBJECTS. Die Zugriffsrechte hierauf sind sehr restriktiv zu vergeben. Folgende Anwendungsberechtigung ist für diesen Vorgang erforderlich:

Berechtigungsobjekt S_USER_OBJ
(Berechtigungsobjekte global ausschalten)
Aktivität: 02 (Ändern)
07 (Aktivieren)
Objekt: <Name der Berechtigungsobjekte, die deaktiviert werden dürfen. Hier ist besonders auf den Wert "*" zu prüfen>

Zur Absicherung dieses Vorganges im Produktivmandanten sind (zusätzlich zur restriktiven Vergabe des Zugriffsrechtes) folgende Einstellungen vorzunehmen:

- Für den Produktivmandant ist in den Mandanteneigenschaften (Tabelle T000) die Eigenschaft `Rolle des Mandanten´ auf `Produktiv´ zu setzen. In dem Fall ist das Deaktivieren von Berechtigungsobjekten nicht mehr möglich.
- Der Systemparameter auth/object_disabling_active ist auf den Wert N zu setzen. Dies unterbindet in allen Mandanten des Systems die Möglichkeit für diesen Vorgang.

Zur Überprüfung, welche Berechtigungsobjekte aktuell deaktiviert sind, kann die Tabelle TOBJ_OFF genutzt werden. Hier sind alle deaktivierten Objekte gespeichert. Werden die Objekte dann wieder aktiviert, so werden sie aus dieser Tabelle wieder gelöscht.

R/3® führt eine Historie über die Deaktivierungen und Aktivierungen mit. Diese wird in der Tabelle TOBJ_CD gespeichert. Hier wird gespeichert, wer wann welche Objekte deaktiviert und aktiviert hat. Wichtig ist hier das Feld Customized Menü (INS_DELE), in dem folgende Werte enthalten sein können:

¨ I (Insert in table TOBJ_OFF) Dieser Eintrag zeigt an, dass das betreffende Objekt deaktiviert wurde.
¨ D (Delete in table TOBJ_OFF) Dieser Eintrag zeigt an, dass das betreffende Objekt wieder aktiviert wurde.

..."Neben dem vollständigen Deaktivieren von Berechtigungsobjekten ist es auch möglich, einzelne Berechtigungsprüfungen pro Transaktion zu deaktivieren."...

Insbesondere ist in der Tabelle TOBJ_CD daher zu prüfen, ob Objekte im Mandanten bereits deaktiviert wurden.

Deaktivieren von einzelnen Berechtigungsprüfungen in Transaktionen

Neben dem vollständigen Deaktivieren von Berechtigungsobjekten ist es auch möglich, einzelne Berechtigungsprüfungen pro Transaktion zu deaktivieren. Dies erfolgt über die Transaktion SU24, mit der u.a. die Tabelle USOBX_C geändert wird.

Über die Tabelle USOBX_C werden jeder Transaktion verschiedene Berechtigungsobjekte zugeordnet, welche beim Aufruf der Transaktion überprüft werden können. Zu jeder Kombination aus Berechtigungsobjekt und Transaktion wird im Feld OK-Kennzeichen (OKFLAG) ein Kennzeichen gesetzt, welches angibt, wie das Berechtigungsobjekt in der Transaktion genutzt werden soll. Folgende Kennzeichen sind möglich:

- PP Das Berechtigungsobjekt wird innerhalb der Transaktion überprüft. Zusätzlich sind in der Tabelle USOBT_C Werte zu den Feldern des Berechtigungsobjektes vorgegeben. Dieses Berechtigungsobjekt wird grundsätzlich in der Transaktion überprüft.
- P Das Berechtigungsobjekt wird innerhalb der Transaktion überprüft. Es werden keine Werte zu den Feldern des Berechtigungsobjektes vorgegeben.
- N Das Berechtigungsobjekt wird innerhalb der Transaktion nicht überprüft.
- U Es wurde keine Vorgabe vorgenommen. Dieser Eintrag wird behandelt wie der Eintrag P.

Das Kennzeichen N stellt hier den prüfungsrelevanten Eintrag dar. Standardmäßig sind bereits viele Kombinationen deaktiviert, indem im Feld OK-Kennzeichen (OKFLAG) ein N von SAP vorgegeben wurde. Dies wurde explizit so eingerichtet und stellt keine Gefahr für das System dar. Kritisch zu betrachten sind diejenigen Einträge, die von der Unternehmung selbst auf N gesetzt wurden. Um dies zu ermitteln muss die Tabelle USOBX_CD genutzt werden, in der eine Historie über die Änderungen an den Kennzeichen gespeichert wird. Die Selektionskriterien für diese Fragestellung sind folgendermaßen zu setzen (siehe auch Abb. 4):

- Feld OK-Kennzeichen (OKFLAG_NEW): N
- Transaktionscode (TCODE): SU24
- Änderungskz. (CHNGIND): U

Abb. 4: Tabelle USOBX_CD: Selektionskriterien

Zum Ändern dieser Prüfkennzeichen sind folgende Zugriffsrechte notwendig:

Berechtigungsobjekt S_TCODE
(Transaktionsberechtigung)
Transaktion: SU24
Berechtigungsobjekt S_USER_GRP
(Benutzergruppen)
Aktivität: *
Benutzergruppe: *
Berechtigungsobjekt S_DEVELOP
(Anwendungsentwicklung)
Aktivität: 03 (Anzeigen)
Objekttyp: SUSO (Berechtigungsobjekte)

Deaktivieren von Stammdatenberechtigungen im Personalwesen

Eine Besonderheit beim Deaktivieren von Berechtigungsprüfungen stellen die Mitarbeiterstammdaten im Personalwesen dar. Diese Berechtigungsobjekte können explizit über das Customizing aktiviert und deaktiviert werden. Betroffen sind folgende Berechtigungsobjekte:

P_ORGIN	HR:	Stammdaten
P_ORGXX	HR:	Stammdaten - erweiterte Prüfung
P_PERNR	HR:	Stammdaten - Personalnummernprüfung

Das Deaktivieren aller drei Objekte würde bedeuten, dass keine Rechte mehr beim Zugriff auf Mitarbeiterstammdaten erfolgen und daher jeder Benutzer alle Stammdaten anzeigen und ändern kann. Daher sind die Zugriffsrechte für diesen Vorgang sehr restriktiv zu vergeben.

Gespeichert werden diese Einstellungen in der Tabelle T77S0. Zur Überprüfung, welche Objekte deaktiviert sind, ist die Tabelle T77S0 anzeigen zu lassen (Transaktion SE16 oder SE16N). In der Selektionsmaske ist im Feld Gruppenname (GRPID) der Wert AUTSW einzutragen. Es wird das Ergebnis wie in Abb. 5 angezeigt.

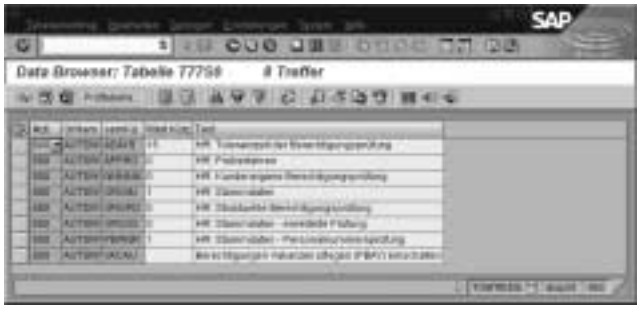


Abb. 5: Tabelle T77S0 - HR-Berechtigungsprüfungen

Im Feld Semantisches Kürzel (SEMID) sind die drei Berechtigungsobjekte ersichtlich:

ORGIN = Berechtigungsobjekte P_ORGIN
ORGXX = Berechtigungsobjekte P_ORGXX
PERNR = Berechtigungsobjekte P_PERNR

Im Feld Wert seman. Kürzel (GSVAL) ist hinterlegt, ob das Objekt aktiviert oder deaktiviert ist:

Wert 0 = Objekt ist deaktiviert
Wert 1 = Objekt ist aktiviert

Bei der Konzeption des Berechtigungskonzeptes für das Personalwesen ist festzulegen, welche Berechtigungsobjekte wie zu nutzen sind. Die Einstellungen in dieser Tabelle müssen mit diesem Konzept übereinstimmen.

Als Zugriffsrecht zum Ändern dieser Einstellungen wird das Änderungerecht für die Tabelle T77S0 benötigt:

Berechtigungsobjekt S_TABU_DIS
Aktivität: 02
Berechtigungsgruppe: PS

Dieser Crash-Kurs sollte Einblicke geben in wesentliche abzusichernde Elemente in einer SAP R/3®-Umgebung. Natürlich erhebt er auf Grund der Komplexität einer R/3®-Systemlandschaft keinen Anspruch auf Vollständigkeit. ✣

TCPA / Palladium oder „Wer schützt wen“?

Von Arne Marcus Strohmann
ibs schreiber gmbh

Sicher haben auch Sie von TCPA (Trusted Computing Platform Alliance) gehört oder gelesen. Auch das von Microsoft erst kürzlich in Next-Generation Secure Base Computing (NGSBC) umbenannte Palladium taucht immer wieder in verschiedenen Meldungen im Internet oder als Schlagzeile einschlägiger Fachliteratur auf. Meistens wird in diesem Zusammenhang dann auch der sogenannte Fritz-Chip (siehe Kasten) bzw. die LaGrande-Technologie von Intel erwähnt.

Aber was ist ein 'Fritz-Chip', was steckt hinter TCPA und Palladium/NGSBC, und warum haben manche Leute Angst vor der neuen Prozessorgeneration von Intel (Pentium 4 mit Prescott-Kern) mit integrierter LaGrande-Technologie? Nun, die LaGrande-Technologie ist im Prinzip ähnlich der des Fritz-Chips, aber eben nicht als Extra-Chip auf dem Mainboard des PCs, sondern direkt im Prozessor eingebaut (On-Die, im Prescott aller Voraussicht noch abschaltbar).

Hinter der TCPA verbirgt sich eine von Intel angeführte Initiative der Industrie, deren Ziel es ist, eine Computerplattform für das nächste Jahrtausend zu schaffen, die für größeres Vertrauen in den PCs sorgen soll. Palladium/NGSBC wiederum ist eine Software von Microsoft, die auf TCPA aufsetzt, und in kommende Windows-Betriebssysteme integriert werden soll. Sehr wahrscheinlich wird Palladium/ NGSBC die nativen Eigenschaften von TCPA um einige 'interessante' Features übertreffen. Teile von Palladium/NGSBC arbeiten übrigens inzwischen schon im Microsoft Media-Player 9.

Der Name des Fritz:

Der Chip der TCPA verdankt seinen Namen dem US-Senator Fritz Hollings, der dafür bekannt ist sehr Film-/Musikindustrie-freundliche Gesetzesvorschläge zu unterbreiten. Hierzu gehört auch der 'Security Systems Standards and Certification Act', der vorschreiben soll, dass in jedes unterhaltungselektronische Gerät zwangsweise ein DRM/TCPA-Modul integriert werden muss.

Um ihr Konzept durchsetzen zu können, benötigt die TCPA eine spezielle Hardware. Diese soll den PC überwachen und feststellen, ob an dessen Hardware oder Software manipuliert wird bzw. wurde. Diese Hardware kann nun ein integrierter Chip (Fritz) oder eine in der CPU verankerte Einheit (LaGrande/Intel) sein. Ebenso soll diese TCPA-Hardware Softwarelizenzverletzungen und das unberechtigte Benutzen von Dateien/Dokumenten verhindern.

Genau hierauf baut Microsoft mit Palladium/NGSBC auf. Das in der nächsten Windows-Version (Longhorn) integrierte Palladium/NGSBC wird zentral gesteuert Raubkopien den Start verweigern und ebenso die Wiedergabe illegaler Multimediadateien (Mp3, avi, etc.) verhindern. Bis jetzt war es sehr schwer das Digital Right Management (DRM) durchzusetzen, da die Schutzmethoden meistens innerhalb kürzester Zeit umgangen werden konnten (z.B. das CSS-Verfahren bei DVDs). Mit TCPA könnte sich dies sehr schnell ändern.

Warum das so ist und was TCPA / Palladium (NGSBC) sonst noch alles von Ihnen abverlangt, erkläre ich Ihnen am einfachsten anhand der Funktionsweise der TCPA-Hardware.

Wie funktioniert TCPA / Palladium (NGSBC)?

Die Problemstellung: Die heutigen PCs und deren Software/Betriebssystem sind sicherheitstechnisch

Existierende Sicherheitsmaßnahmen in PCs:

Verschlüsselung:

DVD-Laufwerke: CSS-Verschlüsselung (geknackt); CPPM für DVD-Audio
FireWire: DTCP- Verschlüsselung (Digital Transmission Content Protection)
Fritz Chip: erste TCPA-Implementierung in IBM ThinkPad T23
Memory Sticks: Magic-Gate-Variante (Verschlüsselung / DRM)
Serial ATA: 'Security Flag' in Spezifikation vorgesehen
SPDIF-Anschluss: SCMS-Schutz (Serial Copy Management System)
TFT-Displays: DVI-Schnittstelle sieht HDCP vor (Content Protection)
TV-Ausgang: Macrovision
USB: DTCP-Verschlüsselung vorgesehen
Wechselmedien: CPRM-Schutzbit (Copy Protection for Recordable Media)

Identifikationsmöglichkeiten

Prozessor: Intel-CPUs seit Pentium 3 mit Seriennummer
Bei AMD-CPUs unbekannt
Anwendungen: GUID bei MS Office und anderen Programmen
Betriebssystem: Registrierungs-ID bei Windows XP
Dateisystem: ID bei Erstellung des Dateisystems
Festplatten: Seriennummern
Netzwerkkarten: eindeutige MAC-Adresse

sehr schwer zu schützen, speziell solange es Debugger gibt, die die Betrachtung laufender Software ermöglichen.

Die Industrie hat dieses Problem erkannt und sich zur TCPA zusammengeschlossen. Mit den zusammengefassten TCPA-Standards sollen diese Missstände behoben werden.

Die Sicherheitsüberwachung wandert einfach in die Hardware. Der erste Lösungsansatz dazu war der schon oben erwähnte Fritz-Chip.

Ein Fritz-Chip beherrscht, ebenso wie die ihm noch folgende TCPA-Hardware, mindestens Folgendes:

- Den Anwender identifizieren und authentifizieren.
- Verhindern des Öffnens/Editierens von Dateien aller Art durch unbefugte Benutzer.
- Ver- und Entschlüsseln (asymmetrisch) auf hohem Level (2048 Bit).
- Empfangene Zertifikate auf Gültigkeit überprüfen.
- Erkennen von Hard- und/oder Softwaremanipulationen.

Natürlich lässt sich ein TCPA-Hardware Computer auch ohne TCPA starten. Allerdings läuft in diesem Modus dann keine TCPA-konforme-Software. Ebenso können keine Dateien oder Dokumente, die mit TCPA-konformer-Software bearbeitet wurden, geöffnet oder manipuliert/editiert werden.

Auf den ersten Blick scheint TCPA ein gutes System zu sein, welches den Computer wirklich sicherer macht.

Zum Beispiel kann ein TCPA-konformes-Mail-Programm überprüfen, ob die E-Mail tatsächlich vom Absender stammt. Ebenso können Dokumente aller Art, nicht mehr von unautorisierten Personen bearbeitet, geschweige denn gelesen werden.

Bis hierhin scheint es immer noch so, als wenn TCPA nur Vorteile bringt und die Wünsche, Anregungen, Kritik und Forderungen der Sicherheitsexperten, teilweise auch der Anwender, erfüllt. Doch bei soviel Positivem muss doch irgendwo ein Haken sein?

Funktionsweise bis zur Übergabe an das OS

Um die Problematik von TCPA genau zu erläutern, stelle ich im Folgenden genauer dar, wie die TCPA-Hardware funktioniert und wie sie sich nach dem Einschalten des Computers verhält:

TCPA setzt zuerst im BIOS und später beim Betriebssystem des Computers an.

In der TCPA-Hardware selbst werden zu Beginn 10 bis 20 Schlüssel (2048Bit RSA-Verschlüsselung) gespeichert. Ein Schlüssel davon ist für das Mainboard bestimmt. Dieser speziell für das Mainboard generierte Schlüssel wird dann mit dem Schlüssel des Herstellers signiert, welcher wiederum von einem Master-Key der TCPA abgesegnet ist.

Mit den übrigen Schlüsseln wird später der Benutzer identifiziert. Der Benutzer muss seinen Schlüssel wiederum von einer Prüfstelle signieren lassen. Dies bedeutet auf jeden Fall einen erheblichen Mehraufwand.

Nun zum Verhalten der TCPA-Hardware nach dem Einschalten des Computers (wir gehen dabei von einem TCPA-konformen-PC mit aktiviertem TCPA aus):

1. Überprüfung ob TCPA aktiviert ist -> ja.
2. Überprüfung des BIOS.

3. Starten des CPU-Betriebes.
4. Testen aller BIOS-Erweiterungen der vorhandenen Steckkarten, bevor die CPU darauf Zugriff erhält.

Der SHA1-Hash-Algorithmus berechnet aus den Daten - die die BIOSe der Karten zur TCPA-Hardware senden und jeweils einem Schlüssel - einen 160-Bit langen eindeutigen Wert. Diese eindeutigen Werte werden bei jedem Schritt zwischengespeichert und der Zustand auf TCPA-Konformität des Computers wird daran bewertet.

Ändert nun jemand ein BIOS, tauscht die Hardware oder verwendet einen anderen Schlüssel, entsteht eine falsche Prüfsumme. TCPA schlägt dann Alarm, aber dazu später mehr.

Wenn bis hierher keine Beanstandungen des TCPA vorliegen, startet der Computer in einem fest definierten sicheren Zustand und übergibt die weitere Kontrolle des Bootvorganges an das TCPA-Betriebssystem.

5. Festplatte bzw. Bootmedium wird auf TCPA-Konformität geprüft.
6. Bootsektor wird geprüft.
7. Betriebssystemlader wird geprüft.
8. Der Kernel des Betriebssystems wird geprüft.
9. Die Gerätetreiber werden geprüft.
10. Die restlichen Ressourcen, die nötig sind zum Start des Betriebssystems, werden geprüft.

Wenn das System bis zu diesem Punkt ohne Abweichungen bzgl. der TCPA-Konformität, also ohne Fehler, durchgelaufen ist, wird die Kontrolle an das Betriebssystem in einen fest definierten sicheren Zustand übergeben.

Wenn es aber auch nur an einer einzigen Stelle innerhalb dieses Ablaufes zu einer Unstimmigkeit kommt, zum Beispiel wenn eine Hardwarekomponente ausgetauscht oder gewechselt wurde bzw. etwas hinzugekommen ist, ist das System nicht mehr TCPA-konform und muss neu zertifiziert werden!

Diese Zertifizierung erfolgt dann Online bzw. über spezielle CD-RW-Medien, auf denen Zertifizierungsdaten verschlüsselt gespeichert sind (selbige können von Fachhändlern, voraussichtlich aber auch über das Internet, auf den neuesten Stand gebracht werden).

Ebenso kann natürlich auch jeder zugelassene Fachhändler die Zertifizierungen vornehmen, aber dieser wird ebenfalls auf die erstgenannten Methoden zurückgreifen.

Bei den Daten, die Online bzw. über die Medien abgerufen werden, handelt es sich um Listen mit geprüfter Hardware (HCL) und gesperrten Seriennummern (SRL, auch Blacklist genannt), teilweise um Listen mit den gesperrten/eingeschränkten Dateien/Dokumenten (DRL).

Wenn die TCPA-Hardware die Konformität ihres PC bestätigt hat, übergibt sie wie oben schon erwähnt, die Kontrolle an das Betriebssystem. An diesem Punkt wird wohl bei zukünftigen Microsoft Windows Betriebssystemen die Kontrolle an Palladium (NGSBC) übergeben werden.

Auch Linux-Versionen mit TCPA-Unterstützung sind angedacht, so zum Beispiel von Hewlett Packard (HP-Linux).

Das TCPA-OS übernimmt

Beim Start des TCPA-konformen-Betriebssystems gleicht dieses seinen Timer mit dem sicheren Timer in der TCPA-Hardware ab und, wenn möglich, mit den authentifizierten Zeit-Servern im Internet. Dies geschieht, um Manipulationen an der Systemzeit zu verhindern. Danach werden die neuesten, bereits oben erwähnten, Listen mit kompatibler Hardware (HCL), gesperrten Seriennummern (SRL) und die der allgemein gesperrten/eingeschränkten Dateien/Dokumenten (DRL) aus dem Internet überspielt. Dieses funktioniert bis zu einem gewissen Punkt auch Offline über die schon erwähnten RW-Medien. Sie müssen dafür aber regelmäßig auf den neuesten Stand (validiert) gebracht werden, sonst überschreiten sie nach einer gewissen Zeit (im Gespräch sind 60 Tage) ein "Verfallsdatum", ab dem sie nicht mehr akzeptiert werden. Das Updaten der RW-Medien kann Online oder über Fachhändler ausgeführt werden. Das Verfallsdatum gilt übrigens auch, wenn Sie nichts an Hard- oder Software ändern; spätestens nach 60 Tagen müssen Sie das RW-Medium updaten, oder das System schließt Sie aus.

Das TCPA-Betriebssystem übergibt dann abschließend die Kontrolle an den Benutzer, wiederum in einem fest definierten sicheren Zustand.

Was passiert aber nun, wenn ein Benutzer ein Programm aufrufen will?

Odyssee eines Programms

Nach dem Aufruf eines Programms wird mittels der TCPA-Hardware zunächst die TCPA-Konformität überprüft. Zur TCPA-Konformität gehören eine passende Plattform-ID und eine gültige Lizenz. Die Lizenz wird mit der schon erwähnten SRL abgeglichen, die dank Internet bzw. zwangsaktualisiertem RW-Medium immer auf dem neuesten Stand sein sollte. Falls die Lizenz abgelaufen ist oder der Hersteller die Seriennummer gesperrt hat, startet das Programm nicht und entfernt sich komplett aus dem Speicher.

Wenn dem Programm allerdings volle TCPA-Konformität bescheinigt wurde, holt das TCPA-Betriebssystem nun eine Liste aller gesperrten/eingeschränkten Dateien/Dokumente (DRL) von einem authentifizierten Internetserver (bzw. dem RW-Medium), um zu verhindern, dass der Anwender 'verbotene' Dateien öffnet oder diese in einer anderen unerlaubten Form nutzt.

Hiernach erhält der Anwender endlich die Kontrolle des gestarteten Programms.

Am Anfang werden die TCPA-Betriebssysteme noch den Start von nicht TCPA-konformen Programmen bzw. Dateien erlauben. Wenn allerdings solch eine nicht TCPA-konforme Applikation/Datei gestartet wird, erhalten alle TCPA-konformen Applikationen eine Botschaft darüber, dass das System nicht mehr sicher ist (das System wurde kompromittiert).

Wenn diese Botschaft von den TCPA-Applikationen aufgefangen wird, überschreiben diese ihren Arbeitsspeicher und beenden sich.

Zwischenbetrachtung: Pro und Contra TCPA

Auf den ersten Blick scheinen die benannten Schritte wirklich nur einer besseren Sicherheit zu dienen.

Auch hätten zum Beispiel Bootsektorviren oder Trojaner keine Chance mehr in TCPA-Systemen. Es könnten sich auch keine 0190/0900 Dialer mehr in das DFÜ-Netzwerk einschmuggeln.

Ein TCPA-System bootet immer in genau dem Zustand, den der Benutzer bei der Einrichtung vorgegeben hat. Jede Änderung an Hard- und/oder Software muss explizit bestätigt werden. Sollte tatsächlich erst nachträglich eine von einem Virus infizierte DLL oder Datei gefunden werden, kann das TCPA-Betriebssystem sie spätestens beim nächsten SRL & DRL Update entfernen.

Allerdings haben gerade diese Vorteile auch einige gravierende Nachteile.

Anders ausgedrückt könnte man sagen, dass man die TCPA-Mechanismen natürlich durchaus zum Nachteil des Anwenders nutzen kann. Speziell manchen Datenschützern wird dabei sehr flau im Magen, wenn sie sich ausmalen, was die Industrie über diese Mechanismen alles erreichen kann.

Man könnte 'eigene' Software so zum Beispiel vor 'Konkurrenz'-Software schützen. Office A lässt dann die Installation von Office B aus vorgeschobenen Sicherheitsbedenken nicht mehr zu oder deinstalliert sich, wenn dieses installiert wird. Gefragt werden Sie nicht! Genauso gut könnte sich Malprogramm X plötzlich weigern Bilder von Malprogramm Y zu akzeptieren, nur weil sich die beiden Herstellerfirmen „nicht grün“ sind und Malprogramm X deshalb keine Zertifikate von Y anerkennt. Oder Ihr Mp3-Player öffnet Ihre Musikstücke nicht mehr, da diese keine Zertifizierung haben (woher auch?). Auch der Industriespionage bzw. behördlichen Spionage sind Tür und Tor geöffnet. Durch das Zusammenwirken der TCPA-Hardware und Palladium (NGSCB) könnten Daten von Ihrem Computer entwendet werden, ohne dass es einer Firewall oder einem Datensniffer auffiele. Es wird nur von einer TCPA-Software angefordert, dass solche Programme während des Betriebs dieses Programms ihre Funktion einstellen müssen. Während diese Sicherheitsprogramme deaktiviert sind, sendet das Spionagetool die Daten und beendet sich selbst, was wiederum dazu führt, dass die Sicherheitsprogramme aktiv werden. Aber im Log weder der Firewall noch des Datensniffers wird der Datentransfer auftauchen. Ebenso ist zu beobachten, dass die amerikanischen Behörden keine Einwände gegen TCPA/Palladium (NGSCB) haben. Beobachter werten das als Zeichen dafür, dass die Regierung davon ausgeht, dass in TCPA/Palladium (NGSCB) zumindest für die Geheimdienste eine „Backdoor“ vorhanden ist.

Nicht zu unterschätzen ist, dass Cracker nun ein neues Ziel haben. Nicht mehr der einzelne PC des Anwenders ist dann das primäre Ziel, sondern die zentralen Server, die die gesammelten HCL, DRL und SRL Daten zur Verfügung stellen, werden das neue, in diesem Falle sehr zentrale, Angriffsziel. Der Erste, der es irgendwie schafft, einen Teil der TCPA-Hardware selbst bzw. von

Palladium (NGSCB) auf eine schwarze Liste dieser authentifizierten Server zu bekommen, wäre der König der Hacker und sehr wahrscheinlich kurz danach einer der meistgesuchten Personen dieser Welt. Er hätte durch seine Handlung das Hochfahren bzw. das Benutzen von Millionen PC auf der gesamten Welt unmöglich gemacht (zumindest für einen gewissen Zeitraum) und damit Kosten in Milliardenhöhe verursacht.

Ebenfalls wird der Anwender in einer trügerischen Sicherheit gewiegt. Niemand kann garantieren, dass alle Informationen, die an das TCPA gesendet werden, zu 100% korrekt sind. Gerade Microsoft hat in diesem Zusammenhang ja schon häufig Pech gehabt (vergessene Updates von Passport-Zertifikaten, 'gefälschtes' Veri-Sign Zertifikat).

Außerdem wäre es eine glatte Lüge, zu behaupten, dass es niemals Viren, Trojaner oder andere unerfreuliche Dinge unter TCPA-Systemen geben wird. Niemand kann das garantieren, deshalb werden Sie in den Klauseln von Microsoft auch nie einen diesbezüglich garantierten Schutz vorfinden. Der einzige Effekt, den die von außen per PR suggerierte 'Sicherheit' bringen wird besteht darin, dass die Anwender nur noch fahrlässiger mit ihren Daten umgehen werden als bisher. Es sind wieder die Sicherheitsexperten, die befürchten, dass die Anwender auf den 'TCPA-macht-das-schon'-Zug aufspringen werden, der durch oberflächliche PR-Informationen zu diesem Thema ein falsches Gefühl der Sicherheit durch TCPA/Palladium (NGSCB) vermittelt.

Fast alle Experten sind sich sicher, dass es nicht eine Frage ist ob TCPA/Palladium (NGSCB) unterwandert werden kann, sondern nur, wann es der Erste schafft?

Dazu kommt, dass speziell am Anfang sehr wahrscheinlich noch Fehler bzw. Ungereimtheiten in der Hardware oder Software stecken werden. Eine gerade für Microsoft-Betriebssysteme nicht zu unterschätzende Sicherheitslücke wäre ihr eigenes TCPA-Kernel Palladium (NGSCB). Denn die beste TCPA-Hardware kann nichts gegen Sicherheitslecks machen, die in der TCPA-Software Palladium (NGSCB) stecken.

Die Lizenz zum Geld drucken

Es gibt durch die strengen Sicherheitsmaßnahmen allerdings für Microsoft noch einen anderen kleinen, aber wahrlich nicht zu unterschätzenden Nebeneffekt:

Um die grundlegende Sicherheit des Systems gewährleisten zu können, muss Palladium (NGSCB) außer Dokumenten und anderen Dateien auch Programme per Hardware-ID und Benutzer-ID zumindest teilweise verschlüsseln. Durch diesen Vorgang wird die Software untrennbar mit der vorhandenen Hardware gekoppelt und eine Weitergabe oder ein Weiterverkauf, selbst wenn vom Gesetzgeber autorisiert, unmöglich.

TCPA-kompatible Software kann also nicht einfach weitergegeben werden; dies ginge nur über eine Seriennummernfreigabe, aber davon ist im TCPA-Standard nichts zu finden.

So schaffen Microsoft und Co es nun endlich, unter dem Deckmantel der Sicherheit, was sie vorher mit keinem Mittel, weder Lizenzierungen noch Kopierschutz, geschafft haben: Unübertragbare Software, nebenbei sogar unübertragbare Dateien und Dokumente, was wiederum auch die Unterhaltungsindustrie sehr freuen wird.

Natürlich muss man auch eine Lizenz erwerben, um TCPA-konforme Software herstellen und/oder vertreiben zu können (auch für In-House-Software).

Die Kosten für solch eine Lizenzierung belaufen sich nach Schätzungen auf bis zu 6-stellige Dollarbeträge pro Anwendung. Damit wird ein weiteres Problem von TCPA sichtbar. Open-Source Entwickler, Freeware/Shareware und sonstige Formen der kostenlosen bzw. mit nur relativ geringen Kosten verbundenen Software sowie kleine Softwarefirmen können sich derartige Beträge einfach nicht leisten.

Apropos Lizenzen: unter TCPA/Palladium (NGSCB) sollten Sie sich sehr genau durchlesen was in diesen steht. (Das ist der, meist recht schnell weggeklickte, Teil der Softwareinstallation, bei dem man mit einer Zustimmung bestätigen muss.) Selbige werden nämlich radikal und ohne Nachfragen umgesetzt. Falls demnach ein Teil Ihrer bisherigen Software mit den Lizenzen der neuen Software kollidiert, sollten Sie sehr gründlich überlegen, ob Sie die neue Software wirklich brauchen bzw. ob Sie schon ein Backup der alten Software und der mit ihr erzeugten Dateien gemacht haben.

Und Linux?

Wenn TCPA sich tatsächlich über Microsofts Palladium (NGSCB) durchsetzt, muss Linux sich gezwungenermaßen anpassen, um nicht als unsicher aus allen Netzwerken (inkl. Internet) verbannt zu werden.

Ein großes Problem für Linux wird die Finanzierung von TCPA-Lizenzen sein, da diese, wie bereits oben erwähnt, nicht gerade günstig sind.

Wie ebenfalls schon erwähnt, hat Hewlett-Packard bereits damit begonnen, ein TCPA-konformes Linux zu entwickeln.

Dies könnte zu mehreren Szenarien führen, wobei folgendes am wahrscheinlichsten ist:

Der Quellcode der TCPA-konformen-Software (der gleichzeitig zur Zertifizierung eingereicht wird) bleibt zwar weiterhin frei downloadbar, man kann mit ihm allerdings nicht sehr viel anfangen, da man zum Ausführen des Binärcodes, der aus ihm erzeugt werden kann, eine gültige Signatur benötigt. Und diese kostet dann Geld. Ja, Sie haben richtig gelesen, diese Signatur wird ab einem bestimmten Zeitpunkt wohl nicht mehr kostenfrei sein. Das heißt nichts anderes, als dass TCPA plötzlich doch eine Methode gefunden hat, mit Linux Geld zu verdienen. Außerdem kann man nebenbei die GPL zu Grabe tragen, da diese durch den Zwang des käuflichen Erwerbs einer Signatur ad absurdum geführt wird.

Beweggründe

Warum unterstützen nun viele namenhafte Unternehmen der Industrie wie zum Beispiel Intel, AMD und Sony oder aber auch große Systemhersteller wie IBM, Hewlett-Packard und Dell TCPA?

Ein wahrscheinlich einfacher Grund, so einfach, dass er Keinem auffällt: Verkauf neuer Hardware. Der Markt ist gesättigt. Die Systeme für die typischen Büroanwendungen sind meist bereits total „überpowert“. Wie schafft man also Möglichkeiten für einen steigenden Absatz? Man erfindet 'neue' Hardware, die auf alten Systemen nicht nachgerüstet werden kann. Man verpackt das Ganze unter dem Namen „Sicherheit“ und verkauft zusammen mit dieser technisch relativ kleinen Neuerung (speziell, wenn man die sehr geringen Zusatzkosten für den Hersteller betrachtet) die alte (im Prinzip schon vorhandene) Hardware erneut. Nebenbei schützt man über TCPA Medien, wie CDs und DVDs, vor der Übertragung auf den Computer bzw. verhindert die Verbreitung ihres digitalen Pendants im Internet und anderen Wegen. Das Erste ist großartig für Hardwarehersteller, das Zweite für die Unterhaltungsindustrie und von den Vorteilen für Softwarehersteller habe ich bereits berichtet.

Intel folgt mit seinen TCPA-konformen Prozessoren außerdem endlich dem Ruf der Unterhaltungsindustrie nach einem 'unüberwindbaren' Kopierschutz. Mit den TCPA-Chips hat Intel ein fast unüberwindbares System geschaffen, und die Unterhaltungsindustrie wird sich begierig darauf stürzen. Das wiederum verschafft Intel höhere Absätze und damit strahlende Aktionäre.

Betrachtung und Zukunft

Betrachtet man das Gesamtpaket und blickt in die Zukunft, so muss man leider sagen, dass diese sehr schlecht prognostizierbar ist. Vieles hängt davon ab, wie stark und wie schnell sich die Digital-Rights-Management (DRM) Systeme auf TCPA stützen werden.

Man sollte auch Microsofts Rolle in diesem Spiel nicht ohne Skepsis betrachten. Gerade Microsoft stellt sich bei Palladium (NGSCB) als die absolut 'vertrauenswürdige Person' dar. Als absolute Autorität in Sicherheitsfragen. Wie uns allen bekannt ist, sind es doch aber gerade Microsoft-Produkte, die meistens riesige Sicherheitslöcher aufweisen oder andere eklatante Sicherheitsmängel (besonders bei der Standardkonfiguration) haben.

Die TCPA-Sicherheit ist nur so gut wie ihr TCPA-Betriebssystem. Mit Palladium (NGSCB) soll jetzt alles auf einen Schlag besser werden; wir werden sehen, was von Microsofts Versprechungen zu halten ist. Auf jeden Fall sollte man es sich sehr gut überlegen, ob man die zentrale Authentifizierung tatsächlich Microsoft allein überlassen sollte.

Interessant ist hierzu auch die Definition eines 'vertrauenswürdigen Systems' aus dem US-Verteidigungsministerium. Danach ist ein vertrauenswürdiges System ein System das meine Sicherheitseinstellungen umgehen/überwinden kann. Was auf den ersten Blick etwas unlogisch erscheint, wird beim zweiten Blick klar. Wenden wir das Ganze doch einmal auf ein anderes Beispiel an. Wenn Sie jemandem eine vertrauliche Geschichte erzählen, setzen Sie darauf, dass dieser die Geschichte nicht publik macht. Genau genommen haben Sie diese Geschichte nur deshalb erzählt, weil Sie ihm vertrauen. Er ist also eine vertrauenswürdige Person (wie ein Arzt zum Beispiel). Er macht die Geschichte nicht publik, obwohl er es könnte. Er kann also ohne jedes Problem Ihr 'Sicherheitssystem' umgehen.

Nun ist klar, was das US-Verteidigungsministerium mit einem vertrauenswürdigen System meint: Ein

System, zu dem der Staat oder andere vertrauenswürdige Personen (in diesem Falle Microsoft) ohne Probleme Zutritt haben.

Es kann sein, dass die Palladium-Entwicker (bzw. jetzt NGSCB-Entwicker) tatsächlich so blauäugig sind und die Gefahren von TCPA/Palladium (NGSCB) nicht sehen bzw. an eine solche Anwendung von TCPA wirklich nicht denken. Aber wenn man den kreativen Umgang mit der Realität der Microsoft-PR-Abteilung in der Vergangenheit so betrachtet, fällt es ein wenig schwer, so etwas zu glauben.

Summa summarum spricht Einiges dafür, dass TCPA/Palladium (NGSCB) nicht wirklich zum Schutz des Anwenders konzipiert wurde. Es soll mehr als bloß vor bösen E-Mails, Viren, Hacken und Spam schützen. Es sieht viel mehr aus, als solle TCPA/Palladium (NGSCB) die beiden großen Themen „Raubkopien“ und „Digital-Rights-Management“ mit einem Schlag zu den Akten legen. Nebenbei soll es natürlich zusätzlich das Geldsäckel der Computer- und Hardwareindustrie füllen.

Fazit des Autors

Die Eingangsfrage lautete: 'Wer schütz wen?'.

Und die Antwort?

Nun - ginge es Microsoft/Intel ausschließlich um mehr Sicherheit, wäre dies durchaus anders zu lösen.

Wenn man dann ergänzend das bestimmt nicht unerhebliche Eigeninteresse von Microsoft hinzu zählt und die Tatsache, dass Microsoft scheinbar einen Standard, der weit über dem TCPA Beschluss liegt, durchsetzen will (der dazu komplett in ihrer Hand liegen würde), muss man sich doch fragen, was Microsoft damit erreichen will?

Und wer schützt denn nun eigentlich wen und wovor? Vor wem ist der TCPA-PC eigentlich sicherer? Vor dem lokalen Anwender oder vor einem Angriff von außen? Und warum muss der eigene Computer , der vom Anwender selbst bzw. der Firma gekauft wurde, eigentlich vor diesen geschützt werden?

Was hat der Schutz eines internen Firmennetzwerkes überhaupt noch für einen Sinn, wenn ich im ungünstigsten Fall den Hardware- und Softwarefirmen automatisch, lediglich durch die Verwendung ihrer Produkte, uneingeschränkten und unkontrollierten Zugang zu meinem System verschaffe. Das wäre, als wenn Sony von Ihnen verlangen würde, dass Sie einmal pro Tag vorbeikommen müssten, um zu prüfen, ob Sie Ihren DVD-Player auch richtig bedienen. Falls das nach Meinung der Techniker nicht der Fall ist, nehmen sie Ihnen Ihren DVD-Player einfach wieder ab, allerdings ohne Ihnen das Geld zurück zu geben. (Das könnte mittels TCPA auch gelöst werden. Wenn Sie häufiger als 3x einen Sony-fremden Film in ein Sony-DVD legen, zerstört dieser sich selbst. Lachen Sie nicht, das könnte bitterer Ernst werden.)

Wenn wir diese Fragen und die schon oben erwähnten 'legalen' Möglichkeiten zu den schlimmsten Befürchtungen verdichten, kann es durchaus sein, dass in jedem TCPA-System eine „Backdoor“ vorhanden ist, über die Ihr PC sicher von der Industrie verwaltet wird.

Einigen scheint bis jetzt noch nicht klar zu sein, was man mit TCPA/Palladium (NGSCB) alles anstellen kann. In Amerika diskutiert man schon darüber, TCPA per Gesetz zwingend für alle Computer vorzuschreiben. Was das für Folgen hat, kann man sich ausmalen. Mit TCPA in der 'Endausbaustufe' kontrollieren die Hard- und Softwarefirmen die Computer. Der Benutzer ist nur noch schmückendes Beiwerk.

Bei mir hört der Spaß allerdings schon wesentlich früher auf:

Wenn mir von Softwarefirma X verboten wird, Programme von Softwarefirma Y laufen zu lassen, oder ich, um ein kleines selbstgeschriebenes Programm laufen lassen zu können, eine 1000-Dollar TCPA-Lizenz benötige, wäre ich verstimmt.

Aber freuen wir uns doch auf die schöne TCPA-Zukunft, in der TCPA-Chips in fast jeder Elektronik vorhanden sind. Ihr Auto kann nur noch bei Aral betankt werden, da der KFZ-Zubehör-Hersteller einen Kooperationsvertrag mit Aral abgeschlossen hat. Ihr tragbarer CD-Player ist von Sony und spielt deshalb auch nur CDs von Sony-Music. Und da Sie sich unvorsichtigerweise zum Ausprobieren das neue Office Z installiert haben, hat sich Ihr normales Arbeits-Office beleidigt deinstalliert und vorsichtshalber gleich die gesamten Dokumente, die Sie damit erstellt haben, gelöscht, damit diese nicht von neuen Programmen 'verunreinigt' werden. ✣

Erster kostenloser Sicherheits-Check Ihres SAP R/3®-Systems mit CheckAud for SAP R/3®

Um Ihnen die Leistungsfähigkeit unserer Produkte aufzuzeigen, bieten wir Ihnen eine einmalige Dienstleistung an:

Wir führen vor Ihren Augen einen Sicherheits-Check Ihres SAP R/3®-Systems durch

! Kostenlos und unverbindlich !

Mit der durch die SAP AG zertifizierten Software Check**Aud for SAP R/3®**

Was wir Ihnen hiermit bieten:

- Sie erfahren live und anschaulich, welche Sicherheitslücken möglicherweise in Ihrem SAP R/3®-System existieren (der Sicherheits-Check erfordert wenig Zeit und wird per Beamer vor Ihren Augen durchgeführt).
- Sie erfahren live und anschaulich, ob Ihr Berechtigungskonzept in Ihrem SAP R/3®-System Ihren Anforderungen, Ihrem IKS und den gesetzlichen Auflagen genügt.
- Der Sicherheits-Check wird von uns durch einen qualifizierten Berater durchgeführt
- Sie erfahren, wie einfach die Sicherheitslücken mit Check**Aud** for SAP R/3® aufgezeigt werden und wie die Software Ihnen bei der Beseitigung dieser Mängel hilft.
- Sie gehen keinerlei Verpflichtungen ein, wenn Sie dieses Angebot in Anspruch nehmen!

Und so funktioniert es:

- Sie vereinbaren mit uns einen Termin bei Ihnen im Hause.
- Vor dem Termin bekommen Sie ein Programm zum Scannen Ihres R/3-Systems zugesandt.
- Sie scannen das System, das gecheckt werden soll (geringer Aufwand, mit sehr wenig Zugriffsrechten möglich).
- Die gescannten Daten brennen Sie auf CD.
- Am vereinbarten Termin spielt unser Berater bei Ihnen diese Daten auf den mitgebrachten Präsentationsrechner und führt den Sicherheits-Check anhand dieser Daten durch (Dauer ca. 3 Stunden).
- Nach der Präsentation werden die Daten vom Präsentationsrechner rückstandslos wieder gelöscht.

Wenn Sie Fragen haben oder gleich einen Termin vereinbaren möchten:

Tel.: 040/69 69 85-18, Sebastian Schreiber / Silke Bertrang

Mail: sales@ibs-schreiber-gmbh.de

Dieses Angebot gilt auch für die anderen Prüf-Produkte aus unserem Hause:

NTaudit
Check**Aud** for Hard- and Software
Check**Aud** for Windows 2000

Informationen zu unseren Produkten sowie unsere aktuelle Referenzliste finden Sie unter:

www. Check**Aud.de**

ANMELDUNG

KOSTENLOSER SICHERHEITS-CHECK

FON: 040/69 69 85-18 • FAX: 040/69 69 85-31 • email: sales@ibs-schreiber-gmbh.de

Name / Vorname _____ PLZ / Ort _____

Firma / Abteilung _____ Telefon / Fax _____

Straße _____ eMail _____

Terminvorschlag (KW) _____ Datum / Unterschrift _____

ibs schreiber gmbh
international business software
SAP Software Partner

ibs schreiber gmbh • Friedrich-Ebert-Damm 145 • 22047 Hamburg
www.CheckAud.de • www.ibs-schreiber-gmbh.de

Jahresfachkonferenz „2. Hamburger Revisions-Tagung“

Corporate Governance, Internationale Rechnungslegung und Unternehmensanalyse im Zentrum aktueller Entwicklungen

1. Tag

Begrüßung durch die Veranstalter IWSt und IBS
Prof. Dr. Carl-Christian Freidank und Dipl.-Ing. Ottokar R. Schreiber

Grußwort
Senator Gunnar Uldall

Zum Umsetzungsstand des Berichts der Regierungskommission “Corporate Governance”
Prof. Dr. Ulrich Seibert
Bundesministerium der Justiz

Diskussion

Kaffeepause

Zum Stand und zur Entwicklung der Rechnungslegung in Deutschland
Prof. Dr. Eberhard Scheffler
Rechtsanwälte Lovells Boesebeck

Diskussion

gemeinsames Mittagessen
(Spiegelsaal)

Wiedergewinnung von Vertrauen in die Arbeit des Wirtschaftsprüfers
Dr. Adalbert Wahl
Vorsitzender des Beirates der Wirtschaftsprüferkammer

Diskussion

Kaffeepause

Qualitätssteigerung der Finanzberichterstattung durch Einführung einer Enforcement-Institution?
Prof. Dr. Klaus Stolberg
KPMG Deutsche Treuhand-Gesellschaft AG

Diskussion

anschließend Sektempfang!

2. Tag
(An diesem Tag können Sie an einem Programm Ihrer Wahl teilnehmen)

Rückblick und Ausblick auf das Tagungsthema
Prof. Dr. Carl-Christian Freidank

Einflüsse der Internationalen Rechnungslegung auf die Bilanzanalyse
Prof. Dr. Laurenz Lachnit
Carl-von-Ossietzky-Universität Oldenburg

Diskussion

Kaffeepause

Früherkennung von Unternehmenskrisen anhand von Abschlusskennzahlen
Prof. Dr. Dr. h.c.
Jörg Baetge
Westfälische Wilhelm-Universität Münster

Diskussion

gemeinsames Mittagessen
(Spiegelsaal)

In- und externes Rating vor dem Hintergrund von Basel II
Prof. Dr. Stephan Paul
Ruhr-Universität Bochum

Diskussion

Kaffeepause

Vorbereitung des Mittelstandes auf Basel II
Dr. Karsten Paetzmann
Angermann & Partner, Hamburg

Diskussion

Schlusswort und Verabschiedung
Prof. Dr. Carl-Christian Freidank

Raum Europa

Prüfung des Risikomanagementsystems durch die Interne Revision
Dipl.-Betriebwirt
Frank Braun
Versicherungskammer Bayern

Kaffeepause

gemeinsames Mittagessen

Raum Hamburg

Zukunftsorientierte Analyse mittelständischer Unternehmen
Dipl.-Wirt.-Ing., Dipl.-Kfm.
Thorsten Holland, Hamburg
Angermann & Partner

Kaffeepause

gemeinsames Mittagessen

Raum Europa

Prüfungssoftware für SAP R/3®
Thomas Tiede
ibs schreiber gmbh, Hamburg

Kaffeepause

Raum Hamburg

Controlling-Software für den Mittelstand
Dipl.-Kfm. Peter Sinn
CP Corporate Plannung AG, Hamburg

www.ibs-hamburg.com

ANMELDUNG zur 2. Hamburger Revisions-Tagung

22.05. - 23.05.2003 in Hamburg

FON: +49 40 69 69 85-15 • FAX: +49 69 69 85-31 • E-Mail: seminare@ibs-hamburg.com

Name / Vorname: _____ Telefon/Fax : _____

Firma / Abteilung: _____ E-Mail: _____

Straße : _____ Ort/Datum: _____

PLZ/Ort : _____ Unterschrift: _____

Ort: Hotel Elysée, Hamburg

Ja, ich nehme an folgenden Tagen teil:

- ❑ **an beiden Tagen (22. - 23.05.2003)**
- ❑ **nur am 22.05.2003**
- ❑ **nur am 23.05.2003**

Teilnahmegebühr/Person 2 Tage: € 1.200,– zzgl. MwSt.
Teilnahmegebühr/Person 1 Tag: € 700,– zzgl. MwSt.

(Hochschulangehörige erhalten 50 % Ermäßigung!)

Preis für Studenten: € 150 zzgl. MwSt. (Nur begrenzte Anzahl möglich!)

BEIDE TAGE SIND GETRENNT BUCHBAR

inkl. Abendveranstaltung, Fachkonferenzunterlagen, Mittagessen und Pausengetränke

Sonstiges: Stornieren ist bis zum **24.04.2003** möglich. Danach ist die Veranstaltungsgebühr in voller Höhe zu zahlen. Ersatzteilnehmer können benannt werden.

IBS behält sich das Recht vor, inhaltliche und personelle Änderungen im Programm vorzunehmen, wenn die Gründe hierfür nicht vom Veranstalter zu vertreten sind.

- ❑ Ja, ich nehme am Hamburger Abend teil.
- ❑ Ja, ich nehme am Hamburger Abend teil und bringe meine/n Partner/in mit.
- ❑ Nein, ich nehme nicht am Hamburger Abend teil.

Auf Wunsch nehmen wir gerne nachstehende Hotelreservierung für Sie vor:

Hotelreservierung von: _____ bis: _____

❑ Raucher ❑ Nichtraucher

Zimmer:	❑ Einzelzimmer ohne Frühstück	€ 132,00
	❑ Doppelzimmer ohne Frühstück	€ 152,00
Frühstück:	❑ Elysée Frühstücksbuffet	€ 14,00
	❑ Boulevard Frühstück	€ 7,00
	❑ kein Frühstück	

Unterschrift: _____ **Ort / Datum:** _____

➲ www.ibs-hamburg.com

Jahresfachkonferenz „IT-Revision“

1. Tag

Begrüßung durch den Veranstalter *IBS*
MARIE-LUISE WAGENER, ***IBS*** **-** Geschäftsleitung

Eröffnung der Fachkonferenz durch den Vorsitzenden
OTTOKAR R. SCHREIBER, ***IBS***

eCommerce - Elektronischer Geschäftsverkehr unter dem Aspekt der Revision
- Rechtswirksamkeit der elektronischen Kommunikation
- Elektronische Form und elektronische Signaturen
- Beweisqualität elektronischer Dokumente
- Ordnungsmäßigkeit der Archivierung

DR. JUR. IVO GEIS

Kaffeepause

eCommerce unter Revisionsaspekten
- Ausgangssituation
- Aktuelle Gefährdung und Bedrohungsszenarien
- Sicherheitsanforderungen
- Technische Lösungskonzepte und -modelle
- Lessons Learned und Ausblick

DIPL.-KFM., DIPL.-WIRTSCH.-INF. KARL-HEINZ REIS

Mittagessen

Digitale Signaturen als Basismechanismus im eCommerce
- Benutzer- und Rollenverwaltung
- Sicheres Systemmanagement
- Abbildung von Vertrauensbeziehungen
- Sicherheit auf Anwendungsebene

DR. GERHARD SCHABHÜSER, BSI

Kaffeepause

GoB und eCommerce
- Welche Anforderungen ergeben sich für die IT aus den GoB?
- Welche besonderen Risiken sind bei eCommerce zu beachten?
- Wie sehen Maßnahmen zur Risikoreduzierung aus?
- Was enthalten die neuen Prüfungsstandards des IDW?

DR. JÜRGEN PEEMÖLLER

2. Tag

Risikomonitoring mit Unternehmensdaten - Proaktives datengesteuertes ökonomisches Risikomanagement
- Unternehmensdaten als Indikatoren für den Störfall
- Risikomonitoring als Bestandteil der Business Intelligence
- Verfahren der Anomaliensuche für Controlling und vor der Betriebsprüfung
- Risikomonitoring unter Low-Cost und High-Performance
- Potentiale des Risikomonitorings
- Continious Auditing / IKS / MIS / GDPdU / Basel II
- Implementierung eines Risikoberichtswesens
- Das Information Warehouse

DIPL.-INF. HOLGER KLINDTWORTH, SUSAT & PARTNER

Kaffeepause

Archivierung nicht codierter und codierter Daten unter dem Blickwinkel von Ordnungsmäßigkeit, Sicherheit und Wirtschaftlichkeit
- Externe und interne Anforderungen
- Archivierungsobjekte und -fristen
- Archivierungsverfahren und -technologien
- Besonderheiten der Archivierung im SAP R/3®-System
- Neue Anforderungen im Bereich der Archivierung codierter Daten (GDPdU)

DR. GERD WÄHNER, REVIDATA UNTERNEHMENSBERATUNG AG

Mittagessen

TCPA / Palladium (Trusted Computing Platform Alliance) NGSBC - next generation secure computing base - Wer schützt wen?
- Klärung der Begrifflichkeiten
- Erläuterung der Systematik
- Gegenüberstellung: Pro und Contra
- Fallbeispiel aus der möglichen Anwendungspraxis
- Fazit mit Empfehlungen für Revision und Administration

ARNE MARCUS STROHMANN, IBS SCHREIBER GMBH

Diskussion und Verabschiedung

ANMELDUNG zur Jahresfachkonferenz IT-Revision

05.06. - 06.06.2003 in Hamburg

FON: +49 40 69 69 85-15 • FAX: +49 69 69 85-31 • E-Mail: seminare@ibs-hamburg.com

Name / Vorname: _____ Telefon/Fax : _____

Firma / Abteilung: _____ E-Mail: _____

Straße : _____ Ort/Datum: _____

PLZ/Ort : _____ Unterschrift: _____

Ort: Hotel Elysée, Hamburg

Teilnahmegebühr/Person (2 Tage):
€ 1.200,– zzgl. MwSt.

inkl. Abendveranstaltung, Fachkonferenzunterlagen, Mittagessen und Pausengetränke

Sonstiges: Stornieren ist bis zum **08.05.2003** möglich. Danach ist die Veranstaltungsgebühr in voller Höhe zu zahlen. Ersatzteilnehmer können benannt werden.

IBS behält sich das Recht vor, inhaltliche und personelle Änderungen im Programm vorzunehmen, wenn die Gründe hierfür nicht vom Veranstalter zu vertreten sind.

❑ Ja, ich nehme am Hamburger Abend teil.

❑ Ja, ich nehme am Hamburger Abend teil und bringe meine/n Partner/in mit.

❑ Nein, ich nehme nicht am Hamburger Abend teil.

Auf Wunsch nehmen wir gerne nachstehende Hotelreservierung für Sie vor:

Hotelreservierung von: _____ bis: _____

❑ Raucher ❑ Nichtraucher

Zimmer:	❑ Einzelzimmer ohne Frühstück	€ 132,00
	❑ Doppelzimmer ohne Frühstück	€ 152,00
Frühstück:	❑ Elysée Frühstücksbuffet	€ 14,00
	❑ Boulevard Frühstück	€ 7,00
	❑ kein Frühstück	

Unterschrift: _____ **Ort / Datum:** _____

➲ www.ibs-hamburg.com

Jahresfachkonferenz

„SAP R/3® - Security Auditing“

1. Tag

Begrüßung durch den Veranstalter *CCC : IBS*
MARIE-LUISE WAGENER, Geschäftsleitung, Hamburg

Eröffnung der Fachkonferenz durch den Vorsitzenden
UWE BERND STRIEBECK, KPMG, ESSEN

Datenschutzaudit - Techniken und Vorgehensweisen
- Prüfungsvorbereitung
- Voraussetzungen der Prüfbarkeit
- Change and Transporting System: Die Veränderung am System
- Fragen an die Berechtigungen
- Spezielle Prüfungen der Verzeichnisse

THOMAS BARTHEL, CARO GMBH UND FORBIT E.V., HAMBURG

Kaffeepause

Moderne Personalwirtschaftsysteme und Auswirkungen auf die Revision
- Vom Integrierten System zu Systemlandschaften mit Zugriffen über Intra-/Internet
- Mitarbeiter und Manager als zusätzliche Benutzer im Personalverfahren
- Workflow-Szenarien und Auswirkungen auf die Berechtigungen
- Anforderungsprofil Revisor für eine Auditierung dieser Verfahrenslandschaften
- Konsequenzen für die Arbeit der Revisoren
- Möglichkeiten zur Vereinfachung der Berechtigungsverwaltung in diesen komplexen Systemen

GERALD BORCHERT, SBS, HAMBURG

Mittagessen

SAP aus Betriebsrats- / Personalratssicht
- Einführung und Erweiterung von SAP R/3® aus Sicht des BR/PR
- Beteiligung des BR/PR in betrieblichen SAP®-Projekten
- Anwenderbeteiligung
- Umgang mit personenbezogenen Daten in SAP®
- Kontrolle/Audit/Revision des betrieblichen SAP®-Systems

TORSTEN SCHULZ, TBS, OBERHAUSEN

Kaffeepause

Das SAP R/3® Berechtigungskonzept der Bayer AG
- Organisatorisches und technisches Umfeld
- Rahmenbedingungen für die Berechtigungsentwicklung
- Aufgaben der Benutzer- und Berechtigungsadministration
- Rollen und Verantwortlichkeiten im Support Prozess
- Exkurs: Toolvorführung der Bayer Account Management Datenbank
- Ausblick

JOHANNES KUMPF, BAYER AG, LEVERKUSEN

gemeinsames Abendprogramm

2. Tag

Das Audit Framework Projekt der SAP AG
- Zielsetzung des Audit Frameworks (Systemübergreifende und -unabhängige Abbildung von Prüfungsabläufen)
- Struktur und Inhalt des Audit Frameworks
- Technische Umsetzung auf den verschiedenen Plattformen am Beispiel von SAP R/3®
- Einbindung des Audit Frameworks in ein ganzheitliches Sicherheitskonzept

THOMAS TIEDE, IBS SCHREIBER GMBH, HAMBURG

Kaffeepause

Digitale (Betriebs-)Prüfung in SAP®
- Neue methodische Ansätze für die elektronische Revision
- Leistungsmerkmale des Audit Information System (AIS) der SAP®
- Optimales Datenhandling für die externe Weiterverarbeitung
- Vorgehensstrategien für eine Betriebsprüfung mit SAP

PETER SCHIWEK, SAP AG, WALLDORF

Mittagessen

Archivierungskonzepte und -anforderungen unter SAP R/3®
- Übersicht über Archivierungsformen
- Archive Link Schnittstelle von SAP R/3®
- Möglichkeiten und Grenzen von Archive Link
- Das Records Management - Aktenverwaltung mit SAP R/3®
- Der Document Finder - Integration fremder Archive in SAP R/3®
- Datenzugriff der Finanzbehörden (GDPdU)

KARL-HEINZ REIS, DEUTSCHE BÖRSE AG, FRANKFURT/M.

Diskussion und Verabschiedung

ANMELDUNG zur Jahresfachkonferenz

SAP R/3® - Security Auditing

08.09. - 09.09.2003 in Hamburg

FON: +49 40 - 69 69 85-15 • FAX: +49 - 40 69 69 85-31
E-Mail: seminare@ibs-hamburg.com

Name: _____ PLZ/Ort : _____

Vorname: _____ Telefon/Fax : _____

Firma: _____ E-Mail: _____

Abteilung: _____ Ort/Datum: _____

Straße : _____ Unterschrift: _____

Ort: Hotel Elysée, Hamburg

Teilnahmegebühr/Person (2 Tage):
€ 1.200,– zzgl. MwSt.

inkl. Abendveranstaltung, Fachkonferenzunterlagen, Mittagessen und Pausengetränke

Sonstiges: Stornieren ist bis zum **08.08.2003** möglich. Danach ist die Veranstaltungsgebühr in voller Höhe zu zahlen. Ersatzteilnehmer können benannt werden.

Das ***IBS*** behält sich das Recht vor, inhaltliche und personelle Änderungen im Programm vorzunehmen, wenn die Gründe hierfür nicht vom Veranstalter zu vertreten sind.

❑ Ja, ich nehme am Hamburger Abend teil.

❑ Ja, ich nehme am Hamburger Abend teil und bringe meine/n Partner/in mit.

❑ Nein, ich nehme nicht am Hamburger Abend teil.

Auf Wunsch nehmen wir gerne nachstehende Hotelreservierung für Sie vor:

Hotelreservierung von: _____ bis: _____

❑ Raucher ❑ Nichtraucher

Zimmer:	❑ Einzelzimmer ohne Frühstück	€ 132,00
	❑ Doppelzimmer ohne Frühstück	€ 152,00
Frühstück:	❑ Elysée Frühstücksbuffet	€ 14,00
	❑ Boulevard Frühstück	€ 7,00
	❑ kein Frühstück	

Unterschrift: _____ **Ort / Datum:** _____

IBS *Prüfen mit Konzept*

EXCEL für Revisoren

Inhalte u.a.:

- Handling von Tabellen, Blättern und Mappen
- Einlesen von Prüfdaten
- Selektionen/Stichprobennahmen
- Schichten von Datenbeständen (ABC-Analyse)
- Funktionen zur Aufbereitung und Analyse von Daten

Die Referenten:

Marie-Luise Wagener,
CCC : IBS, Hamburg
Dipl.-Ing. Gerald Schrott,
CCC : IBS, Hamburg

Termin und Ort:

05. - 07. Mai 2003,
Montag 09:30-17:00 Uhr,
Dienstag 09:00 - 17:00 Uhr
Mittwoch 09:00 - ca. 15:30
im *IBS*-Schulungscenter,
Hamburg, Friedrich-Ebert-Damm 145.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Frau Ute Meyer
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -15
schriftl.: IBS, Friedrich-Ebert-Damm 145,
22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: seminare@ibs-hamburg.com
Die Seminarnummer ist **CDXR**.

IBS *Prüfen mit Konzept*

Einführung in die IT-Revision: GoDV

Inhalte u.a.:

- Einführung
- GoDV Grundsätze ordnungsmäßiger Datenverarbeitung
- GoBS Grundsätze ordnungsmäßiger DV-gestützter Buchführung
- FAMA- und FAIT-Verlautbarungen des IDW
- DV-gestützte Datenprüfung
- GDPdU Grundsätze für die Datenprüfung digitaler Unterlagen

Der Referent:

Dipl.-Ing. Ottokar R. Schreiber,
CCC : IBS, Hamburg

Termin und Ort:

08. - 09. Mai 2003,
Donnerstag 09:30-17:00 Uhr,
Freitag 09:00-ca. 15:30 Uhr
im *IBS*-Schulungscenter,
Hamburg, Friedrich-Ebert-Damm 145.

Anmeldung und Auskünfte:

Bitte melden Sie sich bei
Frau Ute Meyer
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -15
schriftl.: IBS, Friedrich-Ebert-Damm 145,
22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: sales@ibs-hamburg.com
Die Seminarnummer ist **DSDV**.

IBS *Prüfen mit Konzept*

Einführung in die Interne Revision

Inhalte u.a.:

- Einführung
- Grundsätze der Internen Revision (IR)
- Prüfungsdurchführung
- Risikomanagement unter Revisionsaspekten
- Organisation und Verwaltung der Revision

Der Referent:

Dipl.-Ing. Ottokar R. Schreiber,
CCC : IBS, Hamburg

Termin und Ort:

12. - 13. Mai 2003,
Montag 09:30-17:00 Uhr,
Dienstag 09:00-ca. 15:30 Uhr
im *IBS*-Schulungscenter,
Hamburg, Friedrich-Ebert-Damm 145.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Ute Meyer
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -15
schriftl.: IBS, Friedrich-Ebert-Damm 145,
22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: seminare@ibs-hamburg.com
Die Seminarnummer ist **GMIR.**

IBS *Prüfen mit Konzept*

Prüfmittel und Tools in LANs und im Internet für die IT-Revision

Inhalte u.a.:

- Tools
- Werkzeuge
- Erstellen eines Scripts zum Erfassen bestimmter Dateitypen auf lokalen Systemen
- Zusammentragen und Auswerten von Informationen

Der Referent:

Dipl.-Ing. Michael Foth, Siemens AG
Marcus Rasokat, ibs schreiber gmbh

Termin und Ort:

15. - 16. Mai 2003,
Donnerstag 09:30-17:00 Uhr,
Freitag 09:00-17:00 Uhr
im *IBS*-Schulungscenter,
Hamburg, Friedrich-Ebert-Damm 145.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Ute Meyer
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -15
schriftl.: IBS, Friedrich-Ebert-Damm 145,
22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: seminare@ibs-hamburg.com
Die Seminarnummer ist **GMPR**.

IBS *Prüfen mit Konzept*

Workshop zur Berechtigungsprüfung des Basismoduls von SAP R/3®

Inhalte u.a.:

- Spezifikation der Berechtigungskonzeption für die Basis
- Berechtigungsvergabe
- Prüfung und Dokumentation
- Auswertungsmäglichkeiten mit SAP R/3® Standardreports und Tabellen

Der Referent:

Thomas Tiede, ibs schreiber gmbh

Termin und Ort:

19. - 20. Mai 2003,
Montag 09:30-17:00 Uhr,
Dienstag 09:00-ca. 15:30 Uhr
im *IBS*-Schulungscenter,
Hamburg, Friedrich-Ebert-Damm 145.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Ute Meyer
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -15
schriftl.: IBS, Friedrich-Ebert-Damm 145,
22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: seminare@ibs-hamburg.com
Die Seminarnummer ist **R3SB**.

IBS *Prüfen mit Konzept*

Workshop zur Berechtigungsprüfung des Moduls HR von SAP R/3®

Inhalte u.a.:

- Spezifikation der Berechtigungskonzeption für die Personalwirtschaft - HR
- Strukturelle Berechtigungen
- Prüfung und Dokumentation
- Erstellung eines Prüfleitfadens zur Prüfung der Berechtigungskonzeption der Personalwirtschaft

Der Referent:

Gerald Borchert,
Siemens Business Services

Termin und Ort:

26. - 27. Mai 2003,
Montag 09:30-17:00 Uhr,
Dienstag 09:00- ca. 15:30 Uhr
im *IBS*-Schulungscenter,
Hamburg, Friedrich-Ebert-Damm 145.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Ute Meyer
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -15
schriftl.: IBS, Friedrich-Ebert-Damm 145,
22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: seminare@ibs-hamburg.com
Die Seminarnummer ist **R3HB**.

IBS *Prüfen mit Konzept*

Workshop zur Berechtigungsprüfung des Moduls FI von SAP R/3®

Inhalte u.a.:

- Spezifikation der Berechtigungskonzeption für die Finanzbuchhaltung
- Berechtigungsvergabe
- Prüfung und Dokumentation
- Abbildung der Prüfungstätigkeit
- Auswertungsmöglichkeiten mit SAP R/3® Standardreports und Tabellen

Der Referent:

Marie-Luise Wagener,
CCC : IBS, Hamburg

Termin und Ort:

26. - 27. Mai 2003
Montag 09:30-17:00 Uhr,
Dienstag 09:00-ca. 15:30 Uhr
im *IBS*-Schulungscenter,
Hamburg, Friedrich-Ebert-Damm 145.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Ute Meyer
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -15
schriftl.: IBS, Friedrich-Ebert-Damm 145,
22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: seminare@ibs-hamburg.com
Die Seminarnummer ist **R3FB**.

IBS *Prüfen mit Konzept*

Einführung in die IT-Revision: IT und IT-Netzwerke

Inhalte u.a.:

- Einführung
- Prüfungsarten
- Einführung in die IT-Netzwerk-Technik
- Risikopotential von IT- und vernetzten IT-Systemen
- Das Grundschutzhandbuch des BSI (GSH)
- Prüffelder und Prüfobjekte

Der Referent:

Dipl.-Ing. Ottokar R. Schreiber,
CCC : IBS, Hamburg

Termin und Ort:

26. - 27. Mai 2003
Montag 09:30-17:00 Uhr,
Dienstag 09:00- ca. 15:30 Uhr,
im *IBS*-Schulungscenter,
Hamburg, Friedrich-Ebert-Damm 145.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Frau Ute Meyer
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -15
schriftl.: IBS, Friedrich-Ebert-Damm 145,
22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: seminare@ibs-hamburg.com
Die Seminarnummer ist **DSIT**.

IBS *Prüfen mit Konzept*

Prüfen von Firewall-Konzepten

Inhalte u.a.:

- Grundlagen der Sicherheit
- Sicherheitselemente
- Einbindung von Sicherheit in Netzwerke
- Sicherheitskonzepte
- Internetprotokoll IP
- Firewall-Architekturen
- Angriffstest und Revisionen

Der Referent:

Dipl.-Ing. Michael Foth, Siemens AG

Termin und Ort:

02. - 06. Juni 2003
Montag 09:30-17:00 Uhr,
Dienstag 09:00-15:30 Uhr,
im *IBS*-Schulungscenter,
Hamburg, Friedrich-Ebert-Damm 145.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Ute Meyer
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -15
schriftl.: IBS, Friedrich-Ebert-Damm 145,
22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: seminare@ibs-hamburg.com
Die Seminarnummer ist **DSFW**.

IBS *Prüfen mit Konzept*

Systemprüfung von SAP R/3®

Inhalte u.a.:

- Basissicherheit
- Benutzerverwaltung
- Protokollierungskomponenten
- Verbuchungsprinzip
- Tabellensteuerung

Der Referent:

Thomas Tiede,
ibs schreiber gmbh

Termin und Ort:

04. - 06. Juni 2003
Mittwoch 09:30-17:00 Uhr,
Donnerstag 09:00-17:00 Uhr,
Freitag 09:00-ca. 15:30 Uhr
im *IBS*-Schulungscenter,
Hamburg, Friedrich-Ebert-Damm 145.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Ute Meyer
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -15
schriftl.: IBS, Friedrich-Ebert-Damm 145,
22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: seminare@ibs-hamburg.com
Die Seminarnummer ist **R3SY**.

IBS *Prüfen mit Konzept*

eCommerce unter Prüfaspekten

Inhalte u.a.:

- Rechtliche Grundlagen
- Haftung, Gewährleistung
- Datenschutz als Vorraussetzung für eine hohe Akzeptanz
- GoB bei eCommerce
- eCommerce im Business-to-Business-Geschäft
- eCommerce im Business-to-Customer-Geschäft

Die Referenten:

Dr. rer. pol. Jürgen Peemöller, Hamburg
Dr. jur. Ivo Geis, Hamburg

Termin und Ort:

12. - 13. Juni 2003
Donnerstag 09:30-17:00 Uhr,
Freitag 09:00-ca. 15:30 Uhr
im *IBS*-Schulungscenter,
Hamburg, Friedrich-Ebert-Damm 145.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Ute Meyer
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -15
schriftl.: IBS, Friedrich-Ebert-Damm 145,
22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: seminare@ibs-hamburg.com
Die Seminarnummer ist **DSTM.**

IBS *Prüfen mit Konzept*

Baurevision Grundlagen + Praxis, mit Spezialproblematiken

Inhalte u.a.:

- Grundlagen Bau
- Grundlagen IT
- Praxis
- Verfahrensabläufe
- Kalkulation von Baupreisen

Der Referent:

Dipl.-Ing. Jürgen Habenicht,
RevCon, Hannover

Termin und Ort:

12. - 13. Juni 2003
Donnerstag 09:30-17:00 Uhr,
Freitag 09:00-ca. 15:30 Uhr
im *IBS*-Schulungscenter,
Hamburg, Friedrich-Ebert-Damm 145.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Ute Meyer
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -15
schriftl.: IBS, Friedrich-Ebert-Damm 145,
22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: seminare@ibs-hamburg.com
Die Seminarnummer ist **BWGL**.

dib **Unternehmenspolitik**
Deutsches Institut für Betriebswirtschaft e.V.

Zukunftswerkstatt

Inhalte u.a.:

- Neue Medien
- Managementsysteme
- Wirtschaftliche Entwicklung
- Bündelung bereits vorhandener Ressourcen
- Nutzenanalyse der vorhandenen Ressourcen
- Personalentwicklung durch Ideenmanagement
- 1:1 - Beispiele aus der Praxis
- Sie erstellen Ihre Erfolgsstrategie

Die Referenten:

Bernhard Ott, Werk Salzgitter
Thomas Uihlein, Fraport AG

Termin und Ort:

05. - 06. Mai 2003
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **030501**.

dib **Unternehmenspolitik**
Deutsches Institut für Betriebswirtschaft e.V.

Betriebsvereinbarungen zum Ideenmanagement

Inhalte u.a.:

- Der rechtliche Aspekt
- Das Ideenmanagement aus rechtlicher Sicht
- BVW und Betriebsverfassung
- Durchführung des BVW
- Auswirkungen von aktuellen Gesetzesänderungen
- Konsequenzen von aktuellen Gesetzesänderungen

Der Referent:

Dipl.-Ing. Hans Rüdiger Munzke,
Ingenieurbüro IdeenNetz

Termin und Ort:

08. Mai 2003
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **030502**

dib **Unternehmenspolitik**
Deutsches Institut für Betriebswirtschaft e.V.

Wachstumsfaktor Strukturierte Kreativität

Inhalte u.a.:

- Strukturierte Kreativität
- Wachstumsspirale des Ideen-Management nach Blumenschein und Ehlers
- Umgang mit Kreativitätsvampiren und Ideenkillern

Der Referent

Annette Blumenschein, ATB
Ingrid Ute Ehlers, PRODUKT * KONZEPT

Termin und Ort:

12. - 13. Mai 2003
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **030504**.

dib **Unternehmenspolitik**
Deutsches Institut für Betriebswirtschaft e.V.

Projektmanagement

Inhalte u.a.:

- Was versteht man unter einem Projekt?
- Welche Vielfalt an Projekten gibt es in der Praxis?
- Welchen Nutzen bietet die Projektarbeit?
- Wer ist an einem Projekt beteiligt?
- Welche Formen der Projektorganisation bieten sich an?
- Wo liegen die Potenziale und Grenzen?
- Welche EDV-Unterstützung ist denkbar?

Die Referenten:

Dr. Klaus Reiter, Deutsche Gesellschaft für Technische Zusammanarbeit

Termin und Ort:

12. - 13. Mai 2003,
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Teilnehmer:

Datenschutzbeauftragte, Mitarbeiter der Revision und der Personalabteilung

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **030534**.

dib **Unternehmenspolitik**
Deutsches Institut für Betriebswirtschaft e.V.

Mitarbeiterzeitschriften

Inhalte u.a.:

- Zielsetzung
- Inhalte
- Gestaltung
- Beispiele
- Ausdrucksformen
- Mithilfe
- Organisation
- Analyse

Die Referenten:

Dr. Perry Reisewitz,
Compass Communications
Dipl.-Volksw. Friedhelm Wolf,
Konzerndatenschutz, Dresdner Bank AG,
Frankfurt am Main

Termin und Ort:

15. - 16. Mai 2003,
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **030520**

dib **Unternehmenspolitik**
Deutsches Institut für Betriebswirtschaft e.V.

Beschwerdebriefe kundenorientiert beantworten

Inhalte u.a.:

- Durch Kunden-Orientierung Reklamationen als Chance begreifen.
- Anlässe und Absichten bei Beschwerden kennen und einbeziehen.
- Den Aufbau des modernen Briefes geschickt zum Beschwerde-Management nutzen
- Zufriedenheit herstellen durch gutes Deutsch und freundlichen Stil
- Transfer des Gelernten an eigenen Beispielen und vielen Übungsaufgaben

Der Referent:

Peter Schughart,
Werkstatt für moderne Sprache

Termin und Ort:

02. - 03. Juni 2003
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **030628**.

dib **Unternehmenspolitik**
Deutsches Institut für Betriebswirtschaft e.V.

Einstellungsgespräche systematisch und erfolgreich führen

Inhalte u.a.:

- Bedeutung und Prüfung des Anforderungsprofils
- evtl. Lücken im Lebenslauf
- Vorbereitungen
- Fragenkatalog
- Informationen vom Bewerber
- Eigenes Verhalten
- Signale des Bewerbers
- Einstellungsentscheidungen

Der Referent

Wolfgang Hildebrandt,
Hildebrandt ABC GmbH

Termin und Ort:

15. - 16. Mai 2003
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **030524**

dib **Unternehmenspolitik**
Deutsches Institut für Betriebswirtschaft e.V.

Geringfügig entlohnte und kurzfristige Beschäftigungen Besondere Beitragsberechnung bei Entgelten von € 400,01 - € 800,00

Inhalte u.a.:

- Neuregelung der geringfügig entlohnten Beschäftigungen
- Neuregelung der kurzfristigen Beschäftigung
- Beiträge
- Verzicht auf die Rentenversicherung
- Geändertes Meldeverfahren nach DEÜV
- ISteuern

Der Referent

Lothar Wiegelmann, AOK Hessen

Termin und Ort:

16. Mai 2003
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **030531.**

dib **Unternehmenspolitik**
Deutsches Institut für Betriebswirtschaft e.V.

Sozialversicherung in der Praxis

Inhalte u.a.:

- Versicherungspflicht
- Versicherungsfreiheit
- Mitgliedschaft
- Meldewesen
- Kassenzuständigkeit/Wahlrechte
- Beiträge
- Altersteilzeit

Der Referent

Lothar Wiegelmann, AOK Hessen

Termin und Ort:

26. - 27. Mai 2003
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **030538**.

dib **Unternehmenspolitik**
Deutsches Institut für Betriebswirtschaft e.V.

Die Bekämpfung der Geldwäsche und Terrorismusfinanzierung im Kreditinstitut

Inhalte u.a.:

- Probleme und Entwiklungen bei der Umsetzung des GwG
- Nationale und Internationale Zusammenhänge
- Ansätze für effektives Monitoring und Research

Der Referent

Wolfgang Gabriel, SEB AG

Termin und Ort:

15. Mai 2003, im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Teilnehmer:

Mitarbeiter mit Basiskenntnissen von Kredit- bzw. Finanzdienstleistungen aus den Bereichen Rechnungswesen und Innenrevision.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee.
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **030537**.

dib **Unternehmenspolitik**
Deutsches Institut für Betriebswirtschaft e.V.

US GAAP und IAS im Vergleich mit den deutschen GoB

US-amerikanische und internationale Rechnungslegung

Inhalte u.a.:

- Grundlagen der Rechnungslegung nach US GAAP und IAS
- Aufbau der IAS und US GAAP Jahresabschlüsse
- Praktische Erfahrungen zum Übergang auf US GAAP oder IAS
- Aktuelle Entwicklungen in US GAAP und in der IAS-Rechnungslegung

Die Referenten:

Dirk Gallowsky, StB, Senior Manager
Carsten Heuer, WP, StB, Senior Manager

Termin und Ort:

14. - 15. Mai 2003,
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **030526** .

dib **Unternehmenspolitik**
Deutsches Institut für Betriebswirtschaft e.V.

Datenzugriff - Neue Prüfungsmethoden der Finanzverwaltung

Inhalte u.a.:

- Rechtsgrundlagen
- Datenzugriff der Finanzverwaltung
- Prüfsoftware IDEA
- Digitales Archiv
- Elektronische Rechnung
- Ordnungsmäßigkeit von DV-Buchführungen
- Sanktionen bei Verletzung von Buchführungs- und Mitwirkungspflichten

Der Referent:

Oberamtsrat Dipl.-Finanzw.
Reinhold Siebert, Bad Hersfeld

Termin und Ort:

21. Februar 2003
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **030528**

Herausgegeben von der AWV -
Arbeitsgemeinschaft für wirtschaftliche Verwaltung

Aufbewahrungspflichten und -fristen nach Handels- und Steuerrecht

Schriftgut - Mikrofilm - Optische Archivierung - EDI - EDV-Dokumentation

Erich Schmidt Verlag
176 Seiten; ISBN 3 503 07022 2; € 24,80

Diese Veröffentlichung gibt als Entscheidungshilfe für die Praxis Antworten auf die Fragen, wer nach dem Handels- und Steuerrecht aufbewahrungspflichtig ist, was aufzubewahren ist, in welcher Form aufbewahrt werden darf, wie lange aufbewahrt werden muss und wo aufzubewahren ist.

Das Buch bietet Buchführungspflichtigen Sicherheit, die gesetzlichen Anforderungen nach dem Handelsgesetzbuch und der Abgabenordnung zu beachten. Den Prüfern (Interne Revision, Wirtschaftsprüfer, Abschlussprüfer, Betriebsprüfer) hilft der Ratgeber bei ihren Prüfungen, gesetzeskonforme Aufbewahrungsanforderungen zu stellen.

Ein für die Praxis besonders wichtiger Schwerpunkt der Neuauflage sind die Konsequenzen des Rechts auf Datenzugriff und auf Prüfbarkeit digitaler Unterlagen nach der Änderung des § 147 AO. Den erhöhten Anforderungen muss sich der Steuerpflichtige mit einem strategischen Archivierungskonzept stellen.

In der Praxis sehr bewährt haben sich außerdem die in der Schrift enthaltenen umfassenden tabellarischen Verzeichnisse mit einer alphabetisch geordneten Aufzählung von Unterlagen/Aufzeichnungen, zu denen jeweils die gesetzliche Aufbewahrungsfrist und die zulässige(n) Aufbewahrungsform(en) angegeben sind.

Prof. Dr. Rolf Hoffmann unter Mitarbeit von Ingo Hoffmann

Prüfungs-Handbuch

Praxisorientierter Leitfaden einer umfassenden unternehmerischen Überwachungs- und Revisionskonzeption

Erich Schmidt Verlag
352 Seiten; ISBN 3 503 06662 4; € 78,00

Aufgrund der Erhebungen des Instituts für Interne Revision e. V. verwenden Revisionsabteilungen zunehmend Manuals als Orientierungs- und Arbeitshilfe. Dabei steigt der Grad der schriftlichen Dokumentation in sämtlichen Wirtschaftsbereichen mit zunehmender Betriebsgröße, Komplexität und transnationaler Betätigung.

Mangels einer überzeugenden Konzeption und sicherlich auch wegen nicht ausreichender personeller Ressourcen und erforderlicher Zeit, die einen wesentlichen Kostenfaktor darstellt, verfügen zahlreiche Gesellschaften nicht über diese den Prüfungs- und Verwaltungsaufwand minimierende Organisationshilfe. Keine Interne Revision, unabhängig von der Betriebs- und Abteilungsgröße, sollte auf die Vorteile eines Prüfungs-Handbuchs verzichten.

In der Prüfungsliteratur fehlen geschlossene Abhandlungen über praxisorientierte Revisions-Manuals. Die 4. Auflage dieses bestens eingeführten Standardwerkes schließt diese Lücke. Damit haben Unternehmen die Möglichkeit, mit einem Minimum an Aufwand ein auf ihre Gegebenheiten abgestimmtes Handbuch zu erstellen, zu erweitern oder zu aktualisieren.

Raimund Weyand

Insolvenzdelikte

Unternehmenszusammenbruch und Strafrecht
6., überarbeitete und erweiterte Auflage 2003

Erich Schmidt Verlag
238 Seiten; ISBN 3 503 06346 3; € 34,00

Die Zahl der Unternehmenszusammenbrüche steigt seit Jahren stetig an und hat erneut einen Höhepunkt erreicht. Im Umfeld der zahlreichen Insolvenzen kommt es vermehrt zu Straftaten, die umfangreiche und meist zeitaufwendige Ermittlungsverfahren nach sich ziehen. Die Änderungen der InsO zum 1. Dezember 2001 haben zudem zu einem enormen Anstieg der Insolvenzen privater Schuldner geführt. Von der Zunahme betroffen ist auch eine Vielzahl von Einzelunternehmen und Freiberuflern.

Die 6. Auflage dieses bestens eingeführten Standardwerks gibt auf sämtliche Fragen unter Berücksichtigung der aktuellen Tendenzen in Literatur und Rechtsprechung umfassende praxisorientierte Antworten. Zahlreiche Übersichten und Schaubilder erschließen die relevanten Problemfelder. Der Autor beschäftigt sich außerdem ausführlich mit den Konsequenzen der zum 1.1.1999 in Kraft getretenen Reform des Insolvenzrechts für die Strafverfolgung.Weiterführende Hinweise auf abweichende Auffassungen der juristi-

schen Fachliteratur finden sich stets in den Anmerkungen. Es wurden unter anderem die Ausführungen zur Entwicklung des Insolvenzstrafrechts, zur Verbraucherinsolvenz, zur Gläubigerbegünstigung und zur strafrechtlichen Verantwortlichkeit der Ange-hörigen rechts- und steuerberatender Berufe überarbeitet. Bei dieser Neuauflage wurde die Rechtsprechung und Literatur bis September 2002 umfassend berükksichtigt.

Hrsg. Prof. Dr. Martin Richter

Theorie und Praxis der Wirtschaftsprüfung III

Entwicklungstendenzen - Corporate Governance - E-Commerce

Erich Schmidt Verlag
256 Seiten; ISBN 3 503 05988 1; € 49,00

Das dritte Symposium zur „Theorie und Praxis der Wirtschaftsprüfung" beschäftigte sich mit dem Rahmenthema „ Wandel der Prüfungspraxis unter dem Einfluss dynamischer Entwicklungen in Wirtschaft und Gesellschaft". Das Buch enthält neben den Langfassungen der gehaltenen Vorträge zusätzlich einen forschungsmethodischen Beitrag.

In den Beiträgen werden die Fragen erörtert, wie sich die klassische Abschlussprüfung durch eine kapitalmarktorientierte Unternehmensberichterstattung ändert, welche Anforderungen an die Ordnungsmäßigkeit und Sicherheit der Informationssysteme im E-Business zu stellen sind, welche Konsequenzen das Outsourcing von Dienstleistungen für die interne und externe Revision hat, wie sich die Aufgaben der Rechnungshöfe unter dem Einfluss der Haushaltsreform, insbesondere aus der Ablösung der Kameralistik durch die doppische (kaufmännische) Buchhaltung verändern und welche Eigentumsstrukturen in Wirtschaftsprüfungsgesellschaften aus ökonomischer Sicht optimal sind.

Mit dem Symposium wurde zugleich Prof. em. Dr. Dr. h.c. Klaus von Wysocki geehrt. Der in dieser Veröffentlichung abgedruckte Beitrag „Prüfung als wissenschaftliche Untersuchungsprozesse" würdigt die wissenschaftliche und berufspraktische Bedeutung des messtheoretischen Ansatzes von Klaus von Wysocki. Gleichzeitig beinhaltet der Beitrag Ansatzpunkte für ein neues Selbstverständnis von Prüfern und für die Verbesserung ihres Images.

Univ.-Prof.. Dr. Dr. h.c.. Wolfgang Lück

Zusammenarbeit von Interner Revision und Abschlussprüfer

Vergangenheit, Gegenwart , Zukunft

Erich Schmidt Verlag
176 Seiten; ISBN 3 503 07059 1; € 36,80

Die Zusammenarbeit von Interner Revision und Abschlussprüfer ist ein altes, aber immer wieder aktuelles Thema. Die Aufgabengebiete der Internen Revision und des Abschlussprüfers überschneiden sich teilweise. Eine Zusammenarbeit der beiden Überwachungsorgane ist allein schon aus wirtschaftlichen Gründen notwendig.

In dieser Veröffentlichung werden zentrale Entwicklungslinien der Zusammenarbeit von Interner Revision und Abschlussprüfer in Vergangenheit, Gegenwart und Zukunft aufgezeigt. Die dargestellten Anforderungen an die Interne Revision und an die Abschlussprüfung müssen aus Sicht beider Prüfungseinrichtungen auf qualitativ höchstem Niveau gegeben sein, damit eine effiziente Zusammenarbeit beider Überwachungsorgane möglich ist. Die geforderte Internationalisierung der Zusammenarbeit ist als notwendige Reaktion beider Prüfungseinrichtungen auf zukünftige Herausforderungen zu verstehen. Sie ist als Bestandteil von Grundsätzen interner und externer Überwachung national und international eine unabdingbare Voraussetzung.

Der Autor entwickelt in diesem Buch für alle Fachleute, die im Bereich der Unternehmensüberwachung tätig sind oder sich damit beschäftigen, Richtlinien für eine erfolgreiche Zusammenarbeit von Interner Revision und Abschlussprüfer. Das Werk gibt darüber hinaus dem Management und den anderen Corporate Governance-Partner wertvolle Einsichten in die Unternehmensüberwachung.

Univ.-Prof. Dr. Dr. h.c. Wolfgang Lück

Betriebswirtschaft

Erich Schmidt Verlag
176 Seiten; ISBN 3 503 05736 6; € 49,80

Dieses Werk vermittelt die für den Wirtschaftsprüfer/-Kandidaten besonders relevanten Teilgebiete der Betriebswirtschaftslehre gem. § 5 PrüfO WP (Prüfungsordnung für Wirtschaftsprüfer). Die Beiträge

dieses Ausbildungswerkes wurden von namhaften Spezialisten verschiedener Universitäten geschrieben. Das Werk präsentiert in präziser und übersichtlicher Form die jeweils wesentlichen Stoffinhalte aus den Bereichen Unternehmensführung, Kosten- und Erlösrechnung, Finanzierung und Investition einschließlich Unternehmensbewertung. Damit ist die Loseblattsammlung zugleich ein wichtiges Nachschlagewerk für Praktiker und Studierende der Wirtschaftswissenschaften, die sich mit den Grundlagen der Betriebswirtschaft vertraut machen müssen.

Sam DiPiazza Jr. und Robert G. Eccles

Vertrauen durch Transparenz. Die Zukunft der Unternehmensberichterstattung

Wiley-VCH Verlag
232 Seiten; ISBN 3-527-50050-2; € 34,90

Bilanzskandale wie Enron oder Worldcom haben zu einer Vertrauenskrise auf den Kapitalmärkten geführt. Doch auch systematische Mängel der traditionellen Unternehmensberichterstattung beziehungsweise Corporate Reporting Supply Chain führen zu einem Vertrauensverlust bei den Anlegern. Wie ein Corporate Reporting mit mehr Transparenz und aussagekräftigeren Kennzahlen aussehen muss, zeigen die Autoren in ihrem Drei-Stufen-Modell für eine Reform der globalen Rechnungslegungsstandards.

Hrsg. Hans-Dietrich Koch

Der betriebliche Datenschutzbeauftragte

Datakontext-Fachverlag GmbH
472 Seiten; ISBN 3-89577-208-9; € 49,00

Die übersichtliche und verständliche Abhandlung dieser komplizierten Materie, die in Verbindung mit vielfältigen Arbeitshilfen und Materialien eine bis ins Detail führende Ausarbeitung des Themas darstellt, wurde in der 5. Auflage vor dem Hintergrund der Novellierung des BDSG vollständig überarbeitet und erweitert.

Langjährig tätige betriebliche Datenschutzbeauftragte beschreiben bewährte Vorgehensweisen zur praxisnahen Umsetzung der gesetzlichen Erfordernisse für die betriebliche Datenverarbeitung in ein unternehmensbezogenes Datenschutz- und Sicherheitsmanagement.

Das Werk richtet sich sowohl an neu bestellte Datenschutzbeauftragte als auch an „mitten im Berufsleben" stehende Datenschutzpraktiker. Beispielhaft und überschaubar werden eine praxisbezogene Zusammenfassung gesetzlicher und betriebsorganisatorischer Erfordernisse sowie bewährte Vorgehensweisen zur Realisierung des Datenschutzes an die Hand gegeben. Einschlägige technische und organisatorische Maßnahmen zur Abwendung von Gefährdungen der Datenverarbeitung, die in ihrer Summe den Datenschutz in verantwortlichen Stellen ausmachen, sind durchgängig und verständlich - „von der Praxis für die Praxis" - abgehandelt.

Nicht die Kommentierung des Bundesdatenschutzgesetzes, sondern die praxisnahe Ergänzung vorhandener Literatur, ist charakteristisch für das gelungene Werk. Die Fülle von Verweisen auf einschlägige Literatur und Kommentierungen ermöglichen es dem Leser, auf vertiefende Lektüre zu den Themen zurückzugreifen.

Dieses Fachbuch wurde ursprünglich für betriebliche Datenschutzbeauftragte entwickelt. Da die Aufgabenstellung der Datenschutzbeauftragten in nicht öffentlichen und öffentlichen Stellen vielfach dekkungsgleich ist, eignet sich dieses Werk sowohl für privatwirtschaftliche wie auch für öffentliche Stellen.

Das Werk präsentiert sich als praktisches Handbuch für den Datenschutz bei datenverarbeitenden Stellen. In den bisherigen Auflagen hat es sich als „Klassiker" in der Praxis bewährt.

Heiko Haaz

Tätigkeitsfeld Datenschutzbeauftragter

2. überarbeitete Auflage 2003

Datakontext-Fachverlag GmbH
384 Seiten; ISBN 3-89577-207-0; € 46,00

Das gesamte Aufgabengebiet des Datenschutzbeauftragten hat sich aufgrund der Veränderungen der Systemstrukturen, Systemumgebungen, der Sicherheitsansprüche in Unternehmen sowie aufgrund des neuen Bundesdatenschutzgesetzes (BDSG 2001) stark gewandelt.

Infolge dieser Entwicklungen müssen Datenschutzbeauftragte nicht nur ihre Fachkompetenz und ihr Wissen ständig auf dem neuesten Stand halten, son-

dern auch einen vergrößerten Wirkungsbereich durch zuwachsende Kompetenzen bewältigen.

Diese Entwicklungstendenzen greift Haaz in seinem Werk, das nunmehr in zweiter überarbeiteter Auflage vorliegt, auf und legt den Schwerpunkt auf die Darstellung des Tätigkeitsfelds eines Datenschutzbeauftragten mit seinen Aufgaben und Anforderungen, die der Gesetzgeber selber übrigens nicht näher definiert hat.

Anhand von zwei Praxisbeispielen eines Datenschutzbeauftragten im Gesundheitswesen wird anschaulich die allgemeine Umsetzung der vorgestellten Theorie aufgezeigt, was für Verantwortliche dieser Branche besonders interessant ist.

In einem gesonderten Kapitel geht Haaz auf die wichtigsten, aktuellen Tendenzen in der Datenverarbeitung ein, die entscheidende Auswirkungen für die Arbeit der Datenschutzbeauftragten haben.

Auch der Beziehungszusammenhang zwischen Datenschutz und EDV-Revision wird in einem eigenen Kapitel behandelt, da diese Tätigkeitsfelder häufig in Personalunion ausgeübt werden.

Maßgebliche Gesetzestexte im Anhang, runden die Arbeitshilfe für die tägliche Datenschutzpraxis ab.

Helmut und Ute Mocker

E-Nutzen

eBusiness und eKommunikation auf dem Prüfstand der betrieblichen Praxis - 1. Auflage 2003

Datakontext-Fachverlag GmbH
230 Seiten; ISBN 3-89577-265-8; € 41,00

Wir stehen heute vor der zweiten Welle des Einsatzes von Internettechnologien in Wirtschaft und Verwaltung. Dieses Buch zeigt den effektiven Nutzen, den professionelle Anwender aus eBusiness und eKommunikation ziehen können.

Themenleitpunkte:

- Situationsanalyse
- Web-Based HR
- eKommunikation
- eMarketing
- eProcurement
- eLogistik
- Mediales Design
- Sicherheit
- Datenschutz

Praxisbeispiele und Checklisten sowie ein ausführliches Stichwortregister helfen dem Leser, schnell zu einer passenden Lösung zu kommen.

Die Autoren haben sich bereits mit ihrem Erstlingswerk „Intranet - Internet im betrieblichen Einsatz", was mittlerweile in der dritten Auflage vorliegt, sowie den Folgeerscheinungen „E-Commerce im betrieblichen Einsatz" und „E-Communication" einen Namen gemacht.

Autoren:

Helmut und Ute Mocker sind nach langjähriger Tätigkeit in der Industrie, im Bildungsbereich und bei einem Forschungsprojekt der Universität Mannheim seit 1987 Besitzer der Firma MOCCOM EDV-Beratung in Mannheim. Sie arbeiten im Bereich der Organisations-, Trainings- und Bildungsberatung mit den Schwerpunkten Einführung und Einsatz von Intemettechnologien in Industrie- und Dienstleistungsbetrieben und entwickeln WEB-Anwendungen von Projektmanagement bis zur WWW-Präsenz.

Security Service Providing

Da der Stellenwert der IT-Sicherheit in der Praxis ständig wächst, stehen die Verantwortlichen oft vor einem großem Problem: l. Wo sind entsprechend gut ausgebildete Fachkräfte? 2. Spezialisten sind teuer!

Als wirtschaftlich effektive Alternative bietet sich das Outsourcing der Gestaltung, Administration, Überwachung und Fortschreibung der Security-Problematik an. Mit dem Security Service Providing hat sich seit einiger Zeit eine spezielle Form des Outsourcing herausgebildet; der Markt ist kaum überschaubar, weil neben größeren Anbietern zahlreiche Kleinstfirmen bis hin zu Einzelpersonen solche Dienstleistungen anbieten. Die aktuelle Ausgabe 4-5/2002 der Fachzeischrift IT-SICHERHEIT gibt deshalb u. a. eine Übersicht, wer welche Dienstleistungen auf ausgewählten Bereichen anbietet.

Datakontext-Fachverlag:

02234/96610-0

fachverlag@datakontext.com

Abo-Bestellung für ReVision

Ein Abo von ReVision beinhaltet folgende Verlags-Dienstleistungen:

- Zusendung vertiefender Hinweise und Unterlagen zu Beiträgen auf Anfrage
- Zugriffsfreigabe auf umfassende Informationen unter: **www.revision-hamburg.de**
- Zusendung Jahres-CD mit allen jeweils erschienenen ReVisions-Beiträgen und Zusatzinformationen, abrufbar, selektierbar über mitgelieferten Browser

Jahresabonnement gilt für 4 Folgeausgaben ab Abo-Bestellung und verlängert sich jeweils um ein Jahr (d. h. um zusätzlich 4 Ausgabefolgen), wenn nicht gekündigt wird. Kündigung ist mit Ablauf des jeweiligen Jahresabo-Termins einen Monat vorher möglich.

ReVision erscheint quartalsweise (Januar/April/Juli/Oktober)

Kosten für ein Jahresabonnement: € 47,- (incl. 7% MwSt).

Abo-Bestellschein für die ReVision

FON: 040 / 69 69 85 - 14 • FAX: 040 / 69 69 85 - 31 • eMail: sales@osv-hamburg.de

Hiermit bestelle ich ReVision im Jahresabonnement zum nächstmöglichen Zeitpunkt. Ein Jahresabonnement (4 Ausgaben) kostet € 47,- incl. 7% MwSt. Die Abo-Gebühren zahle ich

☐ nach Rechnungsstellung durch den Verlag spätestens mit der ersten Abo-Ausgabe.
☐ per Bankeinzug. Bitte belasten Sie fällige Beträge:

meine Konto-Nr.: _____ Bankleitzahl: _____

Bank: _____ Kontoinhaber: _____

Falls ich nicht spätestens 1 Monat vor dem Beginn meines Jahresabonnements kündige, verlängert sich das Jahresabonnement automatisch jeweils um ein weiteres Jahr.

Name: _____ Vorname: _____

Abteilung: _____ Telefon/Fax: _____

Firma: _____ eMail: _____

Straße: _____ PLZ/Ort: _____

Ort/Datum: _____ Unterschrift: _____