Ottokar R. Schreiber
Herausgeber

Liebe Leserinnen und Leser,

haben Sie ´s gewusst? Die Ergebnisse unseres „Millionär"-Spiels können Sie auf Seite 44 mit Ihren Lösungen vergleichen. Die Hauptgewinner - vielleicht gehören Sie dazu? - werden wir in ReVision IV/01 vorstellen.
SAP R/3 ist nach wie vor der „Dauerbrenner" der Wissensvermittlung im IT-Umfeld. Die kaum mehr zählbaren Seminare und Konferenzen - i. d. R. ausgerichtet von reinen Konferenz-Vermarktern ohne eigenes Fachwissen und ohne eigene Ressourcen - belegen dies. Und immer wieder dasselbe Thema, an dem sich diese traktieren: Das SAP R/3-Berechtigungskonzept. „... man gut, dass SAP gerade dieses vertrackte Berechtigungskonzept eingefallen ist". Eine ganze Dienstleistungsindustrie ernährt sich davon; dabei kommt es häufig gar nicht darauf an, ob die Vortragenden selbst verstehen, wovon sie genau reden. Holt diese ans System! Dort sollen sie ihre Kenntnisse nachweisen! Im Beitrag „Ausgesuchte Berechtigungsobjekte" (dieser wird in ReVision IV/01 fortgesetzt) und mit der Vorstellung von SAPaudit v2.0 wird diesem - teilweise bewusst aufgebauschten - Problemfeld „SAP R/3-Berechtigungskonzeption" die „Extravaganz" genommen, es wird für die Revision in die „Normalität" gerückt. Es ist erstaunlich, wie viele Scharlatane in Form selbsternannter SAP-Experten auf diesem Gebiet „abzocken", wie viele ahnungslose Revisoren auf diese reinfallen, ohne dies zu merken.
Immer aktuell - und diesmal vorgetragen von einem Programmierer selbst - ist das Thema „Software-Projekte unter Revisionsaspekten", insbesondere unter Wirtschaftlichkeitsaspekten. In den nächsten Ausgaben von ReVision werden - dieses Thema fortsetzend - weitere vertiefende betrachtungen folgen.
In ReVision II/01 wurde das Revisions-Organisations- und Verwaltungsprogramm REDIS in einem Anwenderbeitrag vorgestellt. Die vorliegende Ausgabe stellt das Konkurrenzprodukt AUDITmaster vor. Fordern Sie Testversionen ab, bilden Sie sich selbst ein Urteil!
Viele praktische Anregungen für Ihre Revisionsarbeit wünscht Ihnen wie immer

Ihr

Ottokar R. Schreiber

Verlagshinweis:
Nächste Ausgabe der

ReVision

Oktober 2001

Redaktions-/Einsendeschluss für diese Ausgabe: 10.09.2001

Termine 2001

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

IBS-Jahresfachkonferenz
„Baurevision"
13.09.- 14.09.2001 in Berlin

IBS-Jahresfachkonferenz
„IT-Revision"
24.09.- 25.09.2001 in München
s. Seite 52

IBS-Jahresfachkonferenz
„Prüfen von SAP R/3"
15.10.- 16.10.2001 in Berlin
s. Seite 54

IBS-Strategieseminar
„SAP R/3"
17.10.2001 in Berlin
s. Seite 54

IBS-Jahresfachkonferenz
„Datenschutz im Wandel der Zeit"
05.11.- 06.11.2001 in Berlin

Kongress 2001
„ISO/IEC 17799"
12.11.- 13.11.2001 in Hamburg
s. Seite 56

Zentrale Buchung über:
Tel.: 040-69698519
Fax: 040-69698531
www.ibs-Hamburg.com

Inhaltsverzeichnis

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
Tel. 040 / 69 69 85 -11 Fax 040 / 69 69 85 -31
eMail: revision@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 -11. Design-Erstellung auf Wunsch auch durch unsere Medienabteilung möglich.

Anzeigenleitung: Angela Lindemann,
Telefon 040 / 69 69 85 -11
eMail: anzeigen@osv-hamburg.de

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

DTP-Produktion
Grafik/Illustration: Angelika Tiede, OSV Hamburg
Layout/Satz: Anja Frederichs, OSV Hamburg

Druck: Druckerei Zollenspieker Kollektiv GmbH
Zollenspieker Hauptdeich 54
21037 Hamburg

Printed in Germany.
Gedruckt auf chlorfrei gebleichtem Papier

Auditierung der Sicherheit von IT-Systemen: eine Aufgabe der internen Revision

Von Prof. Dr. Reinhard Voßbein,
Geschäftsführer, UIMCert, Wuppertal

Die interne Revision muss zunehmend mehr in neue Aufgaben hineinwachsen. Diese lassen sich oft aus dem Vordringen der Informationstechnologie in den Unternehmensalltag ableiten. Aus der Vielzahl dieser Gebiete, die durch Digitale Signaturen, Datenschutzauditierung und IT-Sicherheit repräsentiert werden, soll im Folgenden das letztgenannte Gebiet wegen seiner herausragenden Bedeutung für die praktische Revisionsarbeit dargestellt werden.

1. Aufgaben der Revision im Wandel: Warum IT-Sicherheitsrevision?

Die Aufgaben der internen Revision haben sich in den letzten Jahren deutlich gewandelt. Während früher reaktive Kontrollen die Regel bei der Revisionsarbeit waren, sind heute proaktive Aufgaben im Sinne einer Mitgestaltung von Entwicklungen normal. Offen ist hierbei häufig noch die Frage, inwieweit die Revision bei der Mitgestaltung Beratungsaufgaben übernehmen soll. Dies wird in vielen Fällen deswegen abgelehnt, weil durch die Beratung eine Präjudizierung zukünftiger Revisionsaufgaben und Revisionsergebnisse entstehen könnte. Auch die Entwicklung der Informationstechnologie hat zu einem Wandel im Aufgabenspektrum geführt. Hierbei ist zu beachten, dass die eigentliche DV-Revision mehr der internen Revision angenähert wird, da durch den Fortfall unternehmenseigener Anwendungs-/Programmierabteilungen eine stärkere Konzentration auf die reinen Revisionsaufgaben erfolgen konnte.

Revisionsaufgaben im Bereich der IT-Sicherheit sind schon seit langem Bestandteile des üblichen Arbeitsgebietes der internen Revision. Allerdings hat sie sich bisher meist mit punktuellen Revisionsvorhaben befasst, während die im Folgenden diskutierten Ansätze sich auf das Sicherheitsmanagement kompletter Systeme beziehen. Dieses neue Arbeitsgebiet wurde deswegen zur sinnvollen Revisionsaufgabe, weil die Entwicklung von Standards der Revision die notwendigen Vorgaben und Messkriterien gibt, um effizient prüfen zu können.

Sicherheit ist heute in den meisten Unternehmen keine Chefsache: In nur weniger als 20% der Unternehmen ist das Topmanagement aktiv in strategische Fragen der IT-Sicherheit eingebunden. Diese Feststellung wird durch die KES-Studie 2000 belegt. Das Engagement scheint zwar besser zu werden, ist aber immer noch zu gering. Dies bedeutet, dass die interne Revision ihren Auftrag zur Prüfung der Sicherheit von IT-Systemen in zu geringem Umfang von der Unternehmensleitung erhält.

Andererseits: Wenn Vorstände und Geschäftsführer nicht die Sorgfalt des ordentlichen Kaufmanns beachten, sind sie gem. HGB und GmbHG bei Schäden hierfür zur Verantwortung zu ziehen (§ 43 GmbHG, § 93 AktG). Dies ist inzwischen durch verschiedene Gerichtsurteile bestätigt worden. Auch die gelegentlich vertretene Auffassung, der Vorstand/die Geschäftsführung könne sich hiergegen versichern, erscheint fragwürdig. Wenn nachweislich grobe Fahrlässigkeit vorliegt, dürfte sich selbst eine Absicherung durch Versicherung als problematisch erweisen.

Deutlich schärfer fordert das KonTraG das Engagement der Führung. Hier wird der Vorstand verpflichtet, ein Risikomanagement zu betreiben. Die Informationsverarbeitung ist einer der zwar modernen, aber geradezu „klassischen“ Risikobereiche. Hier eine Risikobehandlung ohne Berücksichtigung der IT-Sicherheit vornehmen zu wollen, ist absurd. Da jedoch in den meisten Unternehmen, in denen Risikostrategieteams zur Behandlung der KonTraG-

Problematik aufgestellt wurden, die interne Revision Mitglied dieses Teams ist, ist sie prädestiniert zur ganzheitlichen Revision der IT-Sicherheit in Form des Sicherheitsmanagements.

2. Auditierung der IT-Sicherheit: gesetzliche, interne und externe Gründe

IT-Sicherheit kommt nicht von selbst: Sie ist das Ergebnis ernsthafter Bemühungen und Arbeit. Diese Erfahrung machen alle Unternehmen, die sich fundiert und ernsthaft mit der IT-Sicherheit beschäftigen. Die Erfahrung lehrt aber auch, dass die in den Unternehmen vorhandenen Möglichkeiten, sichere Systeme zu gestalten, häufig nur unzureichend genutzt werden: Der Schlendrian des betrieblichen Alltags und die Auffassung, dass ja bisher auch nichts Ernsthaftes passiert sei, scheinen demjenigen Recht zu geben, der IT-Sicherheit für vernachlässigungswürdig hält. Wenn allerdings der K-Fall auftritt, kommt die Frage nach dem Schuldigen und danach, warum keine Risiko- und Bedrohungspolitik entwickelt wurde und weshalb nicht alle Möglichkeiten der Vorbeugung, insbesondere solche, deren Einsatz nur geringe Kosten verursacht, ernsthaft genutzt wurden. Dass es nicht so weit kommt, ist eine der wesentlichen vorbeugenden Aufgaben der internen Revision. Die interne Revision hat durch Prüfungshandlungen Schwachstellen und Fehler im Sicherheitssystem zu erkennen, aus denen sich Risiken für das Unternehmen ergeben können. Sie prüft nach der Implementierung des Risikomanagementsystems die Funktionsfähigkeit des Systems in angemessenen Zeitabständen durch Systemprüfung und Stichprobenprüfung.

Die interne Revision kann durch Auditierung der Sicherheit der Systeme, Schwachstellenberichte und Aufstellen von Schwachstellenbeseitigungsprogrammen entscheidend dazu beitragen, dass IT-Systeme sicherer werden, der K-Fall unwahrscheinlicher wird und dass die Qualität der IT-Sicherheit nach außen und innen kommuniziert werden kann, zum Marketingargument werden kann. Wenn diese Schritte gegangen wurden, ist der letzte Schritt zur Zertifizierung der IT-Sicherheit vergleichsweise klein. Zertifizierung ist kein Selbstzweck: Befassung mit der IT-Sicherheit zahlt sich aus durch die Verbesserung des IT-Sicherheitsniveaus und die damit verbundenen Nutzeffekte. Zertifizierung ist machbar: Gute Vorbereitung durch die interne Revision ist eine wesentliche Vorbedingung für den Erfolg.

Falls auf der Topebene die Einsicht in die Notwendigkeit nicht ausreichend ausgeprägt ist, gibt es eine Vielzahl von gesetzlichen und gesetzesnahen Gründen, die der Revision die Berechtigung und Verpflichtung zur Prüfung geben. Dies sind - ohne Anspruch auf Vollständigkeit - solche traditioneller Art und andere, die auf dem Vordringen der Informationstechnologie beruhen.

1. Hierbei gehören die Forderungen der Handels- und Steuergesetze zum Traditionsbestand.
2. Das KonTraG will
   - risikobehaftete Geschäfte
   - Unrichtigkeiten der Rechnungslegung
   - Verstöße gegen gesetzliche Vorschriften,

   die sich auf die Vermögens-, Finanz- und Ertragslage wesentlich auswirken, offen legen mit der Zielsetzung, sie durch geeignete Maßnahmen beseitigen zu lassen.
3. Das Datenschutzgesetz BDSG fordert sichere Systeme, speziell zum Schutz personenbezogener Daten.
4. Die IT-Sicherheitsanforderungen der Telekommunikationsgesetze gelten für das Gros der Unternehmen, vor allem aber dann, wenn sie e-business betreiben.

Ergänzt werden die gesetzlich fundierten Rechtfertigungsgründe für Prüfvorhaben durch weitere interne und externe Auslöser. Die Tabelle 1 gibt eine Übersicht.

Die genaue Betrachtung der aufgeführten Auslöser zeigt, dass sie sich nicht oder nicht wesentlich von denen tradierter Revisionsgebiete unterscheiden. Als Prüfungsgegenstand sei jedoch in allen Fällen die IT-Sicherheit genannt.

Spezifisch lassen sich die in den einzelnen IT-Sicherheitsgebieten entstehenden und bestehenden Risiken nach den Kategorien

- Verfügbarkeit der IT-Systeme,
- Integrität (Richtigkeit/Fehlerfreiheit) der Daten und Programme sowie
- Vertraulichkeit, vor allem der Daten, aber auch der Programme

charakterisieren.

Gelegentlich werden noch andere - wie zum Beispiel das Risiko der Verbindlichkeit - mit einbe-

zogen, obwohl Verbindlichkeit im Regelfall unter Integrität rubriziert werden kann.

Auslöser für Prüfaufträge und -vorhaben
Externe Gründe
Prüfung durch übergeordnete Instanzen/Muttergesellschaft
Forderung von Kooperations-/Geschäftspartnern
Forderung von Kunden bei Outsourcingunternehmen
Bewertung der Sicherheit als Qualitätskriterium
Interne Gründe
Prüfungsauftrag der Unternehmensleitung
Kenntnis von Schwächen in der Organisation
Technische Neuerung/Berufung von neuen Mitarbeitern
Interne Zielsetzung für externe Fragen (z. B.: Vermarktung des Unternehmens über IT-Sicherheit)

Tabelle 1: Auslöser für Prüfaufträge und -vorhaben

3. Vorgang der Auditierung

Es ist für den vorliegenden Zweck der Auditierung des Sicherheitsmanagements eines IT-Systems durchaus sinnvoll, zwischen Checkup und Audit zu unterscheiden. Hierbei ist der Checkup die Feststellung des Ist-Zustandes durch unterschiedliche Erhebungsverfahren wie Dokumentenanalyse und interviewgeführte Erhebungen, das Audit die Verifizierung oder Falsifizierung der durch den Checkup gewonnenen Ergebnisse. Die in der Tabellen 2 enthaltene Phase 4 beinhaltet eine Bewertung der Feststellungen, die entweder von der internen Revision für eine qualifizierte Berichterstattung genutzt werden kann oder als Grundlage für eine Zertifizierung durch eine dritte, neutrale Institution dient.

Die Aufgaben der Revision ergeben sich aus der Zwecksetzung des Audits. Falls seine Ergebnisse der Verbesserung der IT-Sicherheit dienen sollen, ohne dass eine Zertifizierungsvorbereitung notwendigerweise beabsichtigt ist, geht der so erzeugte Revisionsbericht in die „interne Pipeline“ und führt im Regelfall zu einem Projekt, das den oben genannten Zwecken der Schwachstellenbeseitigung und Systemverbesserung dient und zu einem späteren Zeipunkt durch ein Nachaudit ergänzt wird.

4. Ziele eines IT-Sicherheitsaudits und der nachfolgenden Schritte/Phasen

Ziel eines IT-Sicherheitsaudits ist die Verbesserung der Qualität der Sicherheit des IT-Systems, da auf seiner Basis Schwachstellenbeseitigungsprogramme aufgesetzt werden sollen.

Zur Erreichung dieser Zielsetzung sollte ein IT-Sicherheitsaudit, insbesondere wenn es als Basis für ein IT-Sicherheitszertifikat dienen soll, folgende Merkmale erfüllen:

1. Das IT-Sicherheitsaudit muss von einem definierten Zielniveau ausgehen.
2. Es liefert die Grundlage für Prüfkriterien. Dies können auch interne Sollvorgaben sein.
3. Es liefert und belegt K.o.-Kriterien für Nichtbestehen der Prüfung.
4. Die Feststellungen müssen verifizierbar/falsifizierbar sein.
5. Es liefert eine objektiv-vergleichbare institutionsübergreifende Prüfbasis.
6. Es ist in der Lage, in einer Organisation bestehende Schwachstellen aufzudecken, um Ansätze zur Verbesserung zu geben.
7. Es gestattet eine Gewichtung der Feststellungen.
8. Es stellt klare, vergleichbare Prüfergebnisse zur Verfügung.
9. Das IT-Sicherheitsaudit ist als Grundlage für eine Zertifizierung geeignet.
10. Es ist möglich, einen zeitlichen Zustandsvergleich über mehrere Jahre vorzunehmen.

Phasenschema
• Phase 1: Dokumentenanalyse
• Phase 2: Interviewgeführte Analyse
• Phase 3: Verifizierung und Falsifizierung
• Phase 4: Entscheidung über Auditierungsergebnisse
• Dokumentenanalyse als Grundlage
• Prüfverfahren analog zu ISO-Verfahrensweisen
• Regelungsvorschriften als organisatorische Realität
• Bedeutung der Kontrolle der Regelungen
• in der täglichen Arbeit
• für den Auditierungsprozess
• Prüfung der Sinnhaftigkeit/Qualität von Regelungen

Tabelle 2: Phasenschema

11. Das Auditsystem ist skalierbar, d. h. es ist für Großunternehmen in Teilbereichen einsetzbar und kann zu einer Gesamtbeurteilung vereinigt werden.
12. Es kann nicht als Alibifunktion missbraucht werden, ermöglicht aber eine Verwendung als Marketing-/Qualitätskriterium.
13. Zur Erreichung/Beibehaltung einer testierten Ordnungsmäßigkeitsbescheinigung muss das IT-Sicherheitsaudit in periodischen Abständen wiederholt werden.

Ein solcher Auditierungsprozess schließt eine Zertifizierung als Möglichkeit ein, obwohl dies nicht zwangsläufig ist. Der Nutzen in Bezug auf die Innenwirkung - verursacht durch die Auditierung - besteht in der intensiven Beschäftigung mit dem IT-Sicherheitssystem durch die Revision, eigene Mitarbeiter und gegebenenfalls Dritte. Weitere Nutzen liegen in der Erhöhung der IT-Sicherheit des Gesamtsystems oder wesentlicher Teile sowie der Möglichkeit, sich auf besonders sicherheitssensitive Teile des Gesamtsystems zu konzentrieren. Meist ergibt sich darüber hinaus eine Erhöhung des Imagewertes in Sachen IT-Sicherheit bei Mitarbeitern: Sie entwickeln Sicherheitsbewusstsein und werden in ihrem Sicherheitsverhalten positiv beeinflusst.

Kostenlenkungseffekte im Sinne von Kosteneinsatzoptimierung sollten sich als Ergebnis von IT-Sicherheitsprojekten dergestalt ergeben, dass Investitionen in IT-Sicherheit gelenkt und nach generell akzeptierten Zielsetzungen erfolgen.

Eine Außenwirkung wird sich in der Regel erst dann ergeben, wenn die Qualität des IT-Sicherheitssystems durch ein Zertifikat bestätigt wird. Dieses ist damit der Erhalt eines publicity-wirksamen Zeugnisses über die Sicherheitsqualität und ist damit in der Lage, die Erhöhung des Imagewertes in Sachen IT-Sicherheit bei externen Bezugsgruppen zu liefern.

Erlös- und Gewinnzuwächse durch Vertrauenserhöhung bei umsatzrelevanten Bezugsgruppen sollen als Möglichkeit nicht ausgeschlossen werden, insbesondere dann, wenn die Geschäftsverbindung wesentlich durch Sicherheitsdenken auf dem IT-Sektor beeinflusst wird bzw. werden kann.

5. IT-Sicherheitsauditierungs- und zertifizierungsstandards

Es gibt im Prinzip mehrere Standards, die als Grundlage für Auditierungsvorhaben eingesetzt werden können; nach dem derzeitigen Stand aber nur einen, der Auditierungs- und Zertifizierungsgrundlage ist. Es handelt sich hier um:

- die Common Criteria (CC)
- das Grundschutzhandbuch
- den British Standard BS 7799, jetzt ISO/IEC 17799-1

Die Common Criteria (CC) sind ein international anerkannter Standard für die Beurteilung der Sicherheit von IT-Systemen. Sie haben 1997 die sog. IT-Sec abgelöst und beinhalten eine Anzahl von Bewertungskriterien, die als Vorgaben für Prüfprozesse eingesetzt werden können. Ihr Nachteil ist die geringe Operationalität und damit begrenzte Brauchbarkeit für Nichtfachleute, zu denen in diesem Sinne die Revisoren im Regelfall auch zählen.

Auf der Basis des Grundschutzhandbuches, das an sich schon jetzt in der Hand des Fachmannes eine vorzügliche Prüfungsgrundlage bildet, wird im Verlauf der nächsten Monate eine Auditierungsvorlage entwickelt, die dann nach Fertigstellung in einer gewissen Konkurrenz zum nachstehend beschriebenen British Standard BS 7799/ISO/IEC 17799-1 stehen dürfte. Sie unterscheidet sich jedoch von diesem durch die folgenden Punkte:

- Die technische Ausrichtung ist stärker.
- Behandlung von K.o.-Kriterien für das Nichtbestehen der Prüfung werden anders gehandhabt.
- Eine internationale Geltung ist zur Zeit noch nicht vorgesehen.
- Der Gütesiegel-/Zertifikatserteilungsprozess ist anders ausgelegt: Es wird mehrere Stufen der IT-Sicherheitsqualität geben.

Inhalt des ISO/ IEC 17799-1 (Überarbeiteter Auszug)

1 Zielsetzung des ISO/ IEC 17799-1

2 Vorgehensweise

3 Sicherheitspolitik des Unternehmens

4 Organisation der Sicherheit

4.1 Infrastruktur der Informationssicherheit

4.2 Sicherheit bei dem Zugang durch Fremdunternehmen

5 Beurteilung und Kontrolle der Werte

6 Personelle Sicherheit

6.1 Personenorientierte Fragen

6.2 Benutzerschulung

7 Physische und umgebungsbezogene Sicherheit

7.1 Sicherheitszonen und Geräte

7.2 Allgemeine Maßnahmen

8 Management der Kommunikation und des Betriebs

8.1 Betriebsverfahren und -verantwortlichkeiten

8.2 Systemplanung und -abnahme

8.3 Schutz vor bösartiger Software

8.4 Netzwerkmanagement

8.5 Umgang mit und Sicherheit von Datenträgern

8.6 Austausch von Informationen und Software

9 Zugangskontrolle

9.1 Geschäftsanforderungen an die Zugangskontrolle

9.2 Verwaltung der Zugriffsrechte der Benutzer

9.3 Netzzugriffskontrolle

9.4 Kontrolle des Betriebssystemzugriffs

9.5 Zugriffskontrolle für Anwendungen

9.6 Mobile Computing und Telearbeit

10 Systementwicklung und -wartung

10.1 Sicherheitsanforderungen an Systeme

10.2 Sicherheit in Anwendungssystemen

10.3 Kryptographische Maßnahmen

10.4 Sicherheit bei Entwicklungs- und Supportprozessen

11 Management des kontinuierlichen Geschäftsbetriebs

12 Einhaltung von Verpflichtungen

12.1 Einhaltung gesetzlicher Verpflichtungen

12.2 Überprüfungen der Einhaltung technischer Normen

Tabelle 3: Inhalt des ISO/IEC 17799-1 (Überarbeiteter Auszug)

- Die zeitliche Verfügbarkeit ist noch unklar.
- Die Aussagenqualität ist durch die o. a. Abstufung weniger deutlich.

Die einzige zur Zeit bestehende normierte Prüfungsgrundlage ist der BS 7799/ISO IEC 17799-1. Sie wurde von einem britischen Standardisierungsgremium entwickelt und ist seit dem vergangenen Jahr eine ISO-Norm. Sie ist damit international gültig und deshalb für multinationale Unternehmen von beachtlichem Wert. Sie beansprucht für sich, eine Prüfnorm für das Sicherheitsmanagement von IT-Systemen zu sein und distanziert sich damit von stärker technisch ausgerichteten Normungsansätzen wie dem Grundschutzhandbuch oder den CC. Die Logik ihrer Struktur ist nicht immer voll überzeugend, aber sie soll - wie alle Normen - einem ständigen Be- und Überarbeitungsprozess unterworfen werden. Ihr Aufbau geht aus der Tabelle 3 hervor.

Mit ca. 120 übergeordneten Kriterien und ca. 600 einzelnen Checkpunkten ist der British Standard BS 7799/ISO/IEC 17799-1 bei der genannten und gewollten Beschränkung auf das Sicherheitsmanagement eine ausgefeilte und wertvolle Prüfunterlage. Sie kann jedem Revisor die erforderliche Basis für Revisionsvorhaben geben, wobei aber ein gewisses Maß an Fachkenntnis für das Verständnis der Prüfunterlage, die Durchführung der Prüfung und die Interpretation der Prüfergebnisse notwendig ist.

6. Technische Hilfen und computergestützte Tools zur Unterstützung der Auditierungsarbeit des Revisors

Auch bei Prüfvorhaben der internen Revision wird zunehmend mehr mit unterstützenden Mitteln gearbeitet. Es lassen sich für das Gebiet der IT-Sicherheitsauditierung zwei Gruppen von effizienten Hilfen unterscheiden:

- Prüflisten/Checklisten
- Computergestützte Tools

Checklisten gibt es wohl schon seit langem. Eine der bekanntesten auf dem Sektor der Prüfung von IT-Systemen befindet sich im „Handbuch der EDV-Revision“ (Schuppenhauer) und ist außerhalb des Handbuches als eigenständige DIN A4-Prüfliste erhältlich. Auf dem Sektor der IT-Sicherheitsaudits lassen sich auf der Basis des o. a. Grundschutzhandbuches Prüflisten entwickeln, was jedoch eine gewisse Eigenleistung erfordert.

Die Papierversion des British Standard BS 7799/ISO/IEC 17799-1 kommt einer Prüfliste sehr nahe. Die UIMC Wuppertal hat auf der Basis des British Standard BS 7799/ISO/IEC 17799-1 eine Prüfliste entwickelt, die den Standard exakt abbildet und damit sowohl für interne Audits als auch für die Vorbereitung auf eine Zertifizierung gem. British Standard BS 7799/ISO/IEC 17799-1 geeignet ist. Die Papierversion ist auch zur besseren und bequemeren Nutzung auf einer CD als Liste vorhanden und erspart so den lästigen Umgang mit Papierstapeln.

Von einem computergestützten Tool ist jedoch ein größerer Komfort zu erwarten. Die UIMC hat ein Prüftool entwickelt, das den Vorgang der Ist-Aufnahme effizient unterstützt und gleichzeitig einen Rohbericht auf Basis der Ist-Aufnahme erstellt. Dieser Rohbericht kann in verschiedenen Varianten ausgedruckt werden, wie z. B. als Positivbericht, Schwachstellenreport oder in einer Sonderversion als quantitativer Managementreport.

Nähere Auskünfte hierzu sind im *web* unter uimc.de erhältlich.

<

Termine 2001

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

IIR-Kongress
20.09.- 21.09.2001 in Magdeburg

Kongress 2001
„ISO/IEC 17799“
12.11.- 13.11.2001 in Hamburg
s. Seite 56

25. DAFTA
Interressengerechter Datenschutz
22.11.- 23.11.2001 in Köln

Software-Projekte unter Revisionsaspekten

Von Christoph Alt
Geschäftsführer, ibs schreiber gmbh, Hamburg

Das Prüfen von Softwareentwicklungen und -abteilungen ist ein Thema, an das sich Prüfer und Revisoren nur ungern wagen. Auf der einen Seite ist das Prüfen hier aus zwei Gründen überaus notwendig:

- *Softwareentwicklung ist immer kostenintensiv.*
- *Softwareentwicklung ist immer risikobehaftet.*

Zum Anderen ergeben sich Hemmnisse wie

- *Softwareentwicklung ist immer im Fluss, d. h. es ist schwierig, zu einem bestimmten Zeitpunkt einen Schnitt zu machen.*
- *Softwareentwickler sind immer im Stress und mit hochwichtigen Dingen beschäftigt, so dass man sie nicht unterbrechen mag.*
- *Softwareentwickler nehmen unter Umständen die Revision nicht ernst.*

Dieser Artikel soll einen Einstieg in die Problematik der Prüfung von Softwareentwicklungen und -abteilungen darstellen. Es wird nicht der Anspruch der Vollständigkeit erhoben. Einzelne Themen aus diesem Bereich werden, in loser Folge, in späteren Ausgaben dieser Zeitschrift, detaillierter besprochen werden.

Auch für die Prüfung von Softwareentwicklungen und -abteilungen gelten wie für jedes Prüfobjekt die revisionsspezifischen Kriterien, gegen die zu prüfen ist:

- Ordnungsmäßigkeit
- Sicherheit
- Wirtschaftlichkeit

Die Ordnungsmäßigkeit einer Softwareentwicklung

Softwareentwicklungen erstrecken sich oftmals über mehrere Jahre, insbesondere wenn man die Zeiten der Produktions- und Wartungs-Phase hinzurechnet, da hier ja ebenfalls Aufwand entsteht. Aus dieser langen Laufzeit ergeben sich besondere Anforderungen hinsichtlich der Dokumentation der Projekte: Es müssen nicht nur die Struktur des Projektes und seine Realisierung dokumentiert werden, sondern auch Fehlerkorrekturen mit Beurteilungen der Kosten, Reichweite und Ausmaß der behobenen Fehler sowie ausführliche und aussagekräftige Dokumentationen sämtlicher Interfaces, Module und Systeme.

Diese Dokumentationen müssen hinsichtlich der Lesbarkeit und Nachvollziehbarkeit so beschaffen sein, das neue Programmierer eine möglichst kurze Einarbeitungszeit benötigen. Auf Grund der mehrjährig zu veranschlagenden Laufzeit ist der Wechsel von Programmierern und Programmiererinnen ein Gesichtspunkt eminenter Relevanz. Einarbeitungs- und Wartungsfreundlichkeit müssen aus diesem Grunde bereits bei der Entwurfsphase Einfluss nehmen. Es ist hinlänglich bekannt, das Kosten einer Fehlerkorrektur sich zwischen Entwurfsphase und Wartungsphase verhundertfachen.

Die Notwendigkeit der Nachvollziehbarkeit trifft nicht nur auf die Dokumentation als solches zu, sondern auch auf die Programmierung, also den Quellcode. Jeder Programmierer entwickelt im Laufe der Jahre einen eigenen Stil. Damit dieser Stil sich nicht unvereinbar von den Programmierstilen der anderen Programmierer unterscheidet, müssen diesbezüglich Richtlinien geschaffen werden. Diese Richtlinien sind am Besten in einer Arbeitsvorlage oder einem Handbuch zusammenzufassen. Die Prüfung der Existenz dieser Richtlinien und des Nachweises der Einhaltung ist Aufgabe der Prüfung/Revision.

Genauso wie sich die Programmierstile der einzelnen Programmierer unterscheiden, unterscheiden sich die einzelnen Programmierer auch hinsichtlich ihrer Qualifikation, Erfahrung, Vorlieben und Abneigungen. Letztere Eigenschaften sollten bei

- Gibt es eine dedizierte und dezidierte schriftliche Zielvorgabe für das Softwareprojekt?
- Welche Kostenschätzung liegt dem Projekt zu Grunde?
- Gibt es eine Kosten-Nutzen-Analyse?
- Gibt es eine Untersuchung über evtl. vorhandene gleichwertige Software?
- Wer hat das Projekt gefordert, wer genehmigt?
- Wodurch hat sich der Projektleiter qualifiziert? Wie ist das Projektteam zusammengestellt?
- Sind Konventionen festgelegt worden: z. B. einheitliche Architektur? z. B. genormte Benutzerschnittstellen?
- Gibt es weitere präventive Maßnahmen, um das Projekt von einzelnen Programmierern unabhängig zu halten (Fluktuationsgefahr)?
- Gibt es ein Regelwerk zur Sicherung der Entwicklung?
- Wie ist gewährleistet, dass das Programm möglichst frühzeitig in die produktive Nutzung überführt wird?
- Gibt es schriftliche Vereinbarungen zur Erstellung einer zeitnahen Dokumentation?
- Gibt es eine Zeittafel für die Entwicklung mit Kontrollpunkten?

Tabelle 1: Ex ante-Fragen der Revision

der Fragestellung des optimalen Personaleinsatzes keinen geringen Stellenwert einnehmen, da es sich bei der Programmierung immerhin um eine Tätigkeit mit kreativen Anforderungen handelt. Somit kann es auch für die entstehenden Kosten relevant werden, wer welche Aufgabe zugeordnet bekommt. Dies bezieht sich nicht nur auf die professionellen Programmierer, sondern auch auf Entwicklungen, die an der (hoffentlich) geordneten Programmierung vorbeigehen. Moderne Softwarepakete wie zum Beispiel Microsoft Office enthalten Programmierschnittstellen wie *Visual Basic for Applications* (VBA) von der Firma Microsoft. Mit einer derart offenen Programmierschnittstelle kann jeder Benutzer, auch mit geringer Vorbildung, eigene Makros oder Applikations-Bestandteile erstellen. Wird die Erstellung eigener Programme innerhalb einer Unternehmung erlaubt, so stellt die ein immenses Risiko dar, da diese Programme weder einer ordnungsgemäßen Entwicklung folgen noch dokumentiert werden und auch nicht an einem Test- bzw. Freigabeverfahren teilnehmen.

Test- und Freigabeverfahren bilden den Abschluss einer ordnungsgemäßen Softwareentwicklung. In diesen Test- und Freigabeverfahren müssen nicht nur die Module/Bestandteile/Objekte/Systeme eines Projektes geprüft werden, sondern auch dokumentiert werden, unter welchen Voraussetzungen, Laufzeiten, Wertebereichen und Randbedingungen. Zum Einen entwickeln Programmierer naturgemäß während der Entwicklung eine gewisse Art der „Betriebsblindheit“, d. h. da sie unterbewusst genau wissen, wie der aktuelle Bestandteil funktioniert, prüfen sie schnell mit Werten, die dem erwarteten Verhalten entsprechen. Zum Anderen prüfen Software-Tester hingegen am Besten, wenn sie das Projekt gar nicht kennen, da sie dann auch „Verhalten“ produzieren, an das die Programmierer bei der Entwicklung gar nicht gedacht haben. Das bedeutet allerdings auch, dass die Software-Tester in diesem Fall nicht den Wertebereich mit dem erwarteten Verhalten kennen und auch nicht die Randbereiche der Werte, in denen ein Fehlerauftreten wahrscheinlicher ist. Somit muss nach dem Testverfahren auch geprüft werden, ob in dem Testverfahren alle Möglichkeiten für ein Fehlverhalten abgedeckt wurden.

Die Etablierung einer ordnungsgemäßen Softwareentwicklung erfordert somit eine klare Strukturierung von Aufgabenbereichen und Kompetenzen sowie durchgängige Dokumentations-, Test- und Freigabeverfahren. Damit diese Strukturierung für jedermann nachvollziehbar ist, ist die Struktur der Softwareentwicklung in einem oder mehreren Organigramm(en) darzustellen. Diese

Organigramme erleichtern die Prüfbarkeit und vermitteln Transparenz.

Die Sicherheit einer Softwareentwicklung

Einer Softwareentwicklung drohen vielerlei Gefahren. Zum Einen bestehen für die Daten, aus denen die Softwareentwicklung besteht, Risiken, zum Anderen stellen die Programmierer ein Risiko dar.

Die Datensicherungsmaßnahmen im Entwicklungsumfeld sind noch relevanter und kritischer zu bewerten als in den üblichen Datenschutz-Bereichen. Die Daten der Entwicklung müssen zumindest tageweise gesichert werden und in Teilbereichen bedarfsabhängig zusätzlich bei größeren Versionsunterschieden. Selbst der Verlust nur eines Entwicklungstages kann immense Kosten nach sich ziehen, da nicht nur Änderungen und Erweiterungen des verlorenen Tages nachvollzogen werden müssen, sondern auch sichergestellt sein muss, dass die Datensicherung den Ausgangszustand wiederspiegelt. Die aus dem Verlust resultierende Unsicherheit hat zusätzlich psychologische Konsequenzen auf die betroffenen Programmierer. Dieser Verlust pflanzt sich wie die Schockwelle einer Naturkatastrophe durch die Gemüter der Abteilung fort.

Bei der Datensicherung darf der einzelne Mitarbeiter nicht vernachlässigt werden. Dem Programmierer ist bezüglich der persönlichen Datensicherung eine besondere Disziplin aufzuerlegen, wenn das Projektmanagement nicht über ein zentralisiertes Datenbankverwaltungssystem geregelt wird, welches automatisch die Integrität der Daten gewährleistet. Insbesondere Berufsanfängern mangelt es an Bewusstsein hinsichtlich der Notwendigkeit der Datensicherung.

Diese oftmals unzureichende Sensibilität kann auch auf anderen Gebieten bestehen: Geheimhaltung, Datenschutz und Neugierde. Das bei der Softwareentwicklung realisierte Gedankengut ist Eigentum der Unternehmung, die ja schließlich sowohl die Kosten als auch das Risiko trägt. Somit sind die Programmierer dahingehend so schulen, dass das Wissen, das während der Softwareentwicklung erlangt wird, der Unternehmung gehört und nicht für andere Zwecke verwendet werden darf. Zwar kann niemand von einem Programmierer verlangen, dass er einen eleganten Algorithmus vergisst und sich niemals daran erinnert, aber man kann und sollte Programmierer vertraglich dazu verpflichten, beim Verlassen der Unternehmung für eine bestimmte Zeit nicht auf dem gleichen Arbeitsgebiet tätig zu werden oder gar zu einer Konkurrenzunternehmung zu wechseln. Die hieraus für den Programmierer eventuell entstehenden Nachteile sollten ihm, selbstverständlich, entsprechend „versüßt“ werden. Dass der Programmierer während der Softwareentwicklung beim Umgang mit zur Verfügung gestellten Daten die Anforderungen des Datenschutzes einhält, ist zwar ziemlich wahrscheinlich (Programmierer interessiert zumeist das Verhalten der Software, nicht, womit diese agiert), muss aber dennoch sichergestellt werden.

Eine immense und tiefsitzende Neugierde ist fast allen Programmierern gemein. Diese Eigenschaft ist notwendige Voraussetzung für einen wachen Geist und Motivation. Diese Vorteile ziehen natürlich auch Risiken nach sich. Softwareentwicklungen sollten immer getrennt von produktiven Systemen sein, nach Möglichkeit in eigenen, separaten, Netzwerksystemen arbeiten und eigene Testumgebungen zur Verfügung haben. Wenn dies nicht möglich ist, sollte der Zugriff auf produktive Systeme auf wenige Mitarbeiter beschränkt werden. Die Abkapselung der Softwareentwicklung erleichtert auch die Etablierung eines ordnungsgemäßen Berechtigungskonzeptes, damit sichergestellt werden kann, dass nur berechtigte Mitarbeiter Zugriff auf die Projekte erhalten.

Die Wirtschaftlichkeit einer Softwareentwicklung

Die Frage der Wirtschaftlichkeit ist der größte und schwierigste Teil einer Revision einer Softwareentwicklung. Eine vollständige oder zu mindest größtenteils abdeckende Behandlung dieser Frage würde hier den verfügbaren Rahmen sprengen (Übersicht: über Methoden zur Aufwand/Nutzen-Abschätzung, s. Tabelle 2). Aus diesem Grunde führe ich in diesem Beitrag eine Liste von Fragen auf, die in die Revision der Wirtschaftlichkeit Einzug halten sollten:

Kosten einer Softwareentwicklung

Wie viel Personal mit welchen Kosten pro Monat sind wie viele Monate involviert?

- Elementare Verfahren
  - Analogie-/Relationenverfahren
  - Gewichtungsverfahren
  - Prozentsatzverfahren
  - Methode der parametrischen Schätzgleichung
  - Multiplikatorverfahren
- Kombinierte Verfahren
  - Function-Point-Methode (IBM)
  - COCOMO "Constructive-Cost-Model" (TRW-Boehm)
  - INVAS (Integriertes Verfahren zur Aufwandschätzung - Uni Köln/Siemens AG)
  - Component Analysis Methode

Tabelle 2:
Methoden zur Aufwand/Nutzen-Abschätzung

Es zählt außer den Programmierern auch das Personal für Projektmanagement, Schulungen, Test- und Freigabeverfahren, Support, Vertrieb, etc.

Außer den üblichen Betriebskosten sind auch Abonnements von Software und Zeitschriften, Mitgliedschaften in Entwickler-Kreisen, Computer-Updates und -Wartung, Lizenzkosten für Entwicklungssysteme, Betriebssysteme, Netzwerksysteme und Testsysteme zu nennen.

Für Datensicherungen entstehen Kosten aus den Materialien, der notwendigen Arbeitszeit der betroffenen Sicherungsfachkräfte und der Rechnerleistung.

Welche Folgekosten entstehen durch das (zu verkaufende) Produkt? Folgekosten wie etwa durch Werbematerial, Handbücher, Internet-Auftritt, Wartung und Support, Helpdesk, Verpackung und Porto, Schulungen und Präsentationen sind nicht zu vernachlässigen.

Nutzen einer Softwareentwicklung

Der Nutzen muss unterschiedlich betrachtet werden, je nachdem, ob die Software verkauft oder im eigenen Hause eingesetzt wird. Bei beabsichtigtem Verkauf der Software ist eine Marktanalyse hinsichtlich der Akzeptanz, der zu erwartenden Verkaufszahlen, der Marktaufteilung unter den Konkurrenzprodukten und eine Analyse des Break-Even-Punktes vor der Projektfreigabe notwendig.

Bei Nutzung im eigenen Haus entfallen zwar Marketing und Vertriebskosten, aber andere Kosten sind gleichermaßen zu bewerten: Schulung, Hotline und Support, Dokumentation/Handbücher/Arbeitsanleitungen.

Abschließende Anmerkungen

Die oben dargestellten Gedanken zur Revision von Softwareprojekten sind rein theoretisch. Häufig lassen sich diese wünschenswerten Anforderungen nicht realisieren. Dennoch erscheint es mir sinnvoller, sich Gedanken über diese Thematik zu machen, als davor zurückzuschrecken und die Augen zu verschließen.

In meinem Artikel habe ich an vielen Stellen die Existenz von weiblichen Programmierern, den Programmiererinnen, unterschlagen. Dies diente lediglich der Vereinfachung der Schreibweise.

Fazit

Die Revision von Softwareprojekten ist ein riesiges, nahezu unüberschaubares Gebiet, das weit gefächert komplexe Anforderungen mit sich bringt. Ein definitiver Ansatzpunkt ist auf jeden Fall die Frage: Gibt es eine Dokumentation? Denn die Existenz einer Kokumentation ist zweifelsfrei ein K.o.-Kriterium.

<

Crash-Kurs in ReVision
Migration von NT nach Windows 2000

Teil III: Planung der ADS

Von Markus Rasokat,
Supportleiter, ibs schreiber gmbh, Hamburg

Der dritte und letzte Teil der Migrationsreihe befasst sich mit den Active Directory Services, kurz ADS. Hierbei soll besonders auf die Problematik der Planung bei einem bestehenden NT4-Umfeld eingegangen werden.

Was ist ADS?

ADS ist ein Verzeichnisdienst, also ein Netzwerkdienst, der alle Informationen zu Netzwerkressourcen speichern und Benutzern zugänglich machen kann. Der Verzeichnisdienst gewährleistet das einheitliche Zugreifen, Suchen, Benennen, Beschreiben, Sichern und Verwalten der Ressourcen und deren Informationen. ADS ist, wie auch das Domänenkonzept, ein virtuelles Konstrukt, das auf bestehende physikalische Gegebenheiten gesetzt wird. Wer einmal das Vergnügen hatte, mit Novell-Netware zu arbeiten, wird viele Parallelen zwischen der NDS und ADS entdecken. So wird in der ADS ebenfalls angestrebt, die gesamte Unternehmensstruktur hierarchisch abzubilden. Dies geschieht mit zwei Arten von Objekten, den Containerobjekten und den Blattobjekten. Containerobjekte können weitere Containerobjekte enthalten sowie Blattobjekte. Blattobjekte hingegen sind sogenannte Endobjekte, also Objekte, die für sich selbst stehen und keine weiteren Objekte enthalten können. Dieser Strukturaufbau ermöglicht es, alle Objekte der ADS in hierarchischer Form darzustellen und zu verwalten. Die ADS ist an den X.500-Standard angelehnt und hat gegenüber der NT4-Version eine domänenunabhängige, eindeutige Benutzererkennung.

LDAP

Das Lightweight Directory Access Protocol ist ein Verzeichnisdienstprotokoll zur Abfrage und Aktualisierung der Daten von ADS. Jedes Objekt in der ADS hat einen eindeutigen Namen und wird durch einen LDAP Namenspfad angesprochen. Ein LDAP Namenspfad besteht aus zwei Komponenten:

- Definierte Namen (Distinguished Names, kurz DNs)
- Relative definierte Namen (Relative Distinguished Names, kurz RDNs)

Jedes Objekt in der ADS besitzt einen definierten Namen. Der DN gibt die Domäne an, in der sich das Objekt befindet, sowie den vollständigen Pfad des Objektes.

DC (Domain Component)
= Komponente des DNS Namens der Domäne
OU (Organizational Unit)
= Eine Organisationseinheit bzw. Container
CN (Common Name)
= Jedes Objekt, das nicht DC oder OU ist

Beispiel:
CN=MMeier
OU=Vertrieb
DC=au
DC=ibs
DC=de

Der RDN von LDAP ist der Teil des LDAP Namens, der das Objekt in seinem Container eindeutig identifiziert. In dem vorangegangenen Beispiel wäre das MMeier. Dadurch, dass der Benutzer durch diesen Kontext authentifiziert wird, ist der eigentliche Benutzername (User Principal Name) mmeier@vertrieb.au.ibs.de

Logische Struktur

Die logische Struktur von der ADS ist flexibel und umfasst folgende Komponenten (Bild 1):

- Gesamtstrukturen
  (z. B.: DE)
- Strukturen
  (z. B.: REVCON, IBS)
- Domänen
  (z. B.: ASIA, AU)
- Organisationseinheiten (OUs)
  (z. B.: VERTRIEB)

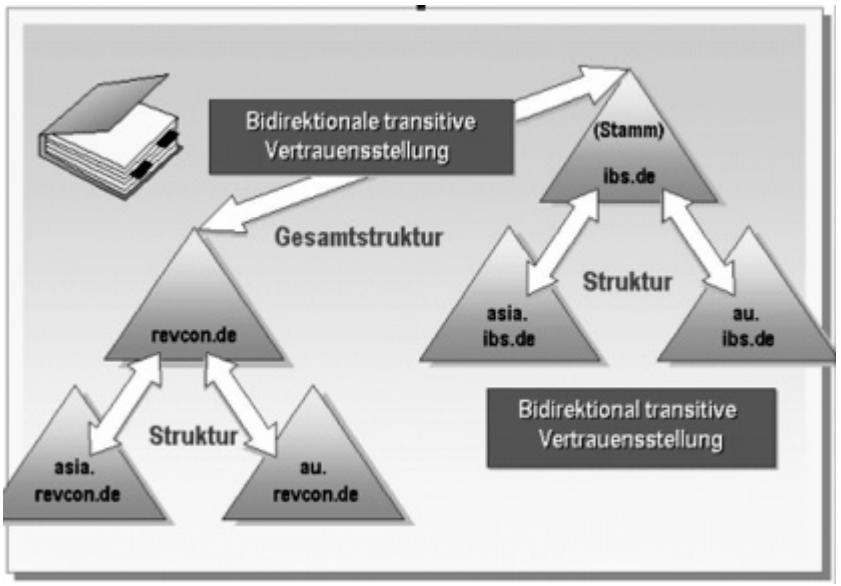

Bild 1: Strukturen und Gesamtstruktur mit bidirektionalen Vertrauensstellungen

Die Gesamtstruktur stellt das gesamte Unternehmen dar. Sie entsteht mit dem Einrichten des ersten Windows 2000-Domänencontrollers. Auf ihm ist auch der „globale Katalog“ eingerichtet. In dem „globalen Katalog“ wird eine Teilmenge der Attributinformationen zu allen Objekten in der Gesamtstruktur abgebildet. Das ermöglicht zum einen die Anmeldung der Benutzer an einem beliebigen physikalischen Punkt der Gesamtstruktur. Zum anderen wird das Auffinden von Verzeichnisinformationen in der Gesamtstruktur ermöglicht, wobei die Position der Daten bei der Suche irrelevant ist. In unserem Beispiel nehmen wir „de“ als Namen der Gesamtstruktur.

Strukturen sind der Gesamtstruktur untergeordnet. Normalerweise werden über die Strukturen Länder abgebildet. In unserem Beispiel nehmen wir „ibs“ und „revcon“ als Strukturnamen.

Die Domänen unter Windows 2000 stellen nach wie vor eine Sicherheitsgrenze dar. D. h. dass Administratoren und Benutzer nur in den Domänen agieren können, in denen diese mit Rechten eingerichtet wurden. Gegenüber der Windows NT4 Domäne kann 2000 nicht nur 40.000, sondern mehrere Millionen Objekte innerhalb einer Domäne verwalten. Die ADS kann in zwei Domänenmodi eingerichtet werden. Für eine Migration gibt es den „gemischten Modus“. Wird ein reines Windows 2000-Netzwerk eingerichtet, arbeiten die Domänen im „einheitlichen Modus“. Es kann vom „gemischten Modus“ auf den „einheitlichen Modus“ konvertiert werden. Eine Konvertierung vom „einheitlichen“ in den „gemischten Modus“ ist nicht möglich. Solange Windows 2000 im „gemischten Modus“ arbeitet, sind fast alle Vorteile, die Windows 2000 mit sich bringt, nicht nutzbar. U. a. ist die Anzahl der Objekte innerhalb der Domänen nach wie vor auf 40.000 begrenzt, es können keine Universellen Gruppen eingerichtet werden, und transitive Vertrauensstellungen sind nicht möglich. Microsoft empfiehlt auf Grund des neuen Leistungspotenzials der Windows 2000-Domänen, die Domänenanzahl so gering wie möglich zu halten. Im Gegensatz zu NT4-Domänen ist unter W2000 ein domänenübergreifender, transitiver Zugriff möglich. Das heißt, dass Benutzer aus Domäne A über eine vertraute Domäne B auf Ressourcen in Domäne C zugreifen können. In unserem Beispiel nehmen wir als Domänennamen ASIA, REVCON.

Standorte stellen eine Kombination aus einem oder mehreren IP-Subnetzen dar, die über eine Hochgeschwindigkeitsverbindung miteinander kommunizieren. Ein Standort ist im Gegensatz zur Domäne, die auf die logische Struktur aufsetzt, auf die physische Struktur aufgesetzt. Standorte werden in erster Linie zum Organisieren des Replikationsverkehrs eingerichtet. Die Planung des Replikations- und Anmeldeverkehrs ist besonders wichtig, da sie den Verbindungen der Domänencontroller untereinander angepasst sein muss, um eine optimale Nutzung der physikalischen Netzwerkgegebenheiten gewährleisten zu können.

Da die logische Struktur der ADS getrennt von der physischen Struktur arbeitet, können sowohl Standorte mehrere Domänen enthalten als auch Domänen mehrere Standorte. Da diese Flexibilität sehr schnell zur Intransparenz führen kann, ist auch hier eine genaue Dokumentation unabdingbar.

Generell wird spätestens an dieser Stelle klar, warum für die Migration von NT4 nach 2000 sowohl die physikalische als auch die logische Dokumentation des NT4 Ist-Zustandes absolute Voraussetzung ist (Siehe ReVision I/2001). Vor allem die Geschwindigkeitsangaben der einzelnen Netzwerkverbindungen sind für die Planung der Standorte und der Replikationsabläufe essenziell. Nur mit Hilfe der Dokumentation kann folglich auch erst die ADS geplant werden. Weiterhin ist es wichtig zu wissen, dass bei Windows 2000 zwar zwischen PDC und BDC nicht mehr unterschieden wird, Domänencontroller aber nicht gleich Domänencontroller ist. So muss es DCs geben, die innerhalb einer Gesamtstruktur und innerhalb der Domänen besondere Aufgaben übernehmen. Zunächst muss hier sicherlich der DC Erwähnung finden, der als erstes eingerichtet wird. Er verwaltet den schon erwähnten globalen Katalog. Des weiteren gibt es noch DCs, die im „Einzelmasterbetrieb“ arbeiten. Es gibt verschiedene Einzelmaster-Betriebsfunktionen in einer ADS-Domäne oder Gesamtstruktur, die einzelnen DCs zugewiesen werden müssen. Diese Funktionen dürfen jeweils nicht gleichzeitig auf mehreren DCs ausgeführt werden und müssen daher jeweils auf einzelnen DCs eingerichtet werden. Es gibt insgesamt fünf Einzelmaster-Betriebsfunktionen:

1. Schema-Master
2. Domain Naming Master
3. RID-Master
4. PDC-Emulator
5. Infrastrukturmaster

Zwei der Einzelmaster-Betriebsfunktionen müssen auf DCs der Gesamtstruktur eingerichtet sein:

1. Schema-Master
   (Steuert Änderungen und Aktualisierungen im Schema)
2. Domain Naming Master
   (kurz DNS, steuert Hinzufügen und Entfernen von Domänen)

Die anderen drei Einzelmaster-Betriebsfunktionen müssen jeweils auf den DCs innerhalb von Domänen eingerichtet sein:

1. RID-Master
   (Steuert die Zuweisung von SIDs und RIDs)
2. PDC-Emulator
   (Verwaltet Änderungen v. Clients u. Servern, die nicht W2000 sind)
3. Infrastrukturmaster
   (Verwaltet, Aktualisiert Gruppenmitgliedschaften in Domänen)

Alle Einzelmaster-Betriebsfunktionen können jeweils auf einem DC eingerichtet werden oder aber auf verschiedene DCs verteilt werden. Die Entscheidung, ob eine verteilte oder zentrale Installation der Einzelmaster-Betriebsfunktionen auf einem einzelnen DC besser ist, hängt von der Größe, also von der Anzahl der Benutzer, Gruppen und Ressourcen, der Domäne ab. Durch Aufgabenverteilung der Einzelmaster-Betriebsfunktionen kann die Performance der jeweiligen Domäne bzw. der Gesamtstruktur erhöht werden.

Organisationseinheiten (engl. Organizational Unit, kurz OU) sind eine weitere Neuerung. Eine OU unter Windows 2000 stellt eine Teileinheit einer Domäne dar. Innerhalb der ADS wird sie als Containerobjekt dargestellt und ermöglicht eine genaue Delegierung von Aufgaben (sowohl auf Benutzer- als auch Administrationsebene) innerhalb einer Domäne. OUs können weitere OUs enthalten, wodurch eine detaillierte Abbildung der Abteilungen und Unterabteilungen des Unternehmens generiert werden kann. In unserem Beispiel heißen die ersten OUs der österreichischen Domäne AU: VERTRIEB und LAGER. (Bild 2)

Die Flexibilität der ADS ermöglicht eine freie Gestaltung der Firmendarstellung in hierarchischer Form. Alle Container-Elemente lassen sich ver-

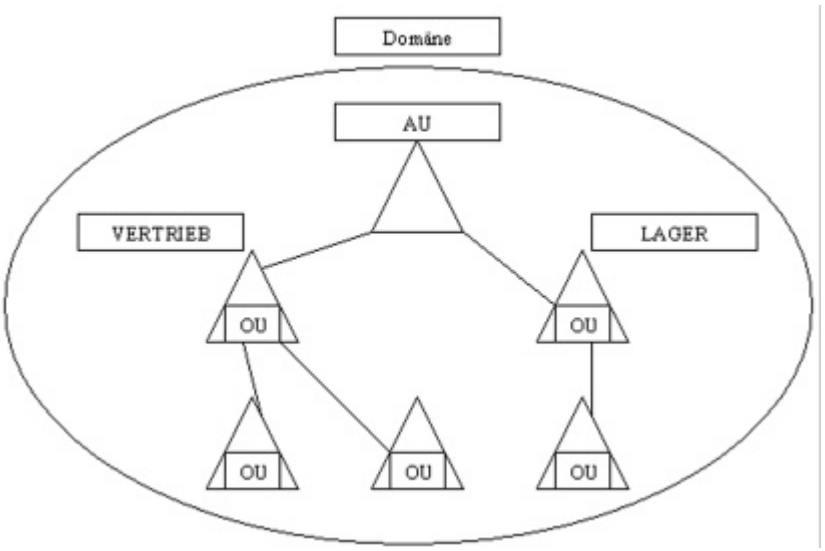

Bild 2: Struktur von Organisationseinheiten innerhalb einer Domäne

schachteln, wodurch die Abbildung des Unternehmens, bei entsprechender Planung, übersichtlich gestaltet werden kann. Die hohe Flexibilität bedeutet aber auch, dass bei fehlender oder mangelhafter Planung der Überblick (Transparenz) innerhalb der ADS schnell verloren gehen kann. Insbesondere bei der Vergabe von Domänen in Verbindung mit der Definition von Standorten ist eine exakte Planung Voraussetzung, um hohe Transparenz mit optimaler Performance zu realisieren.

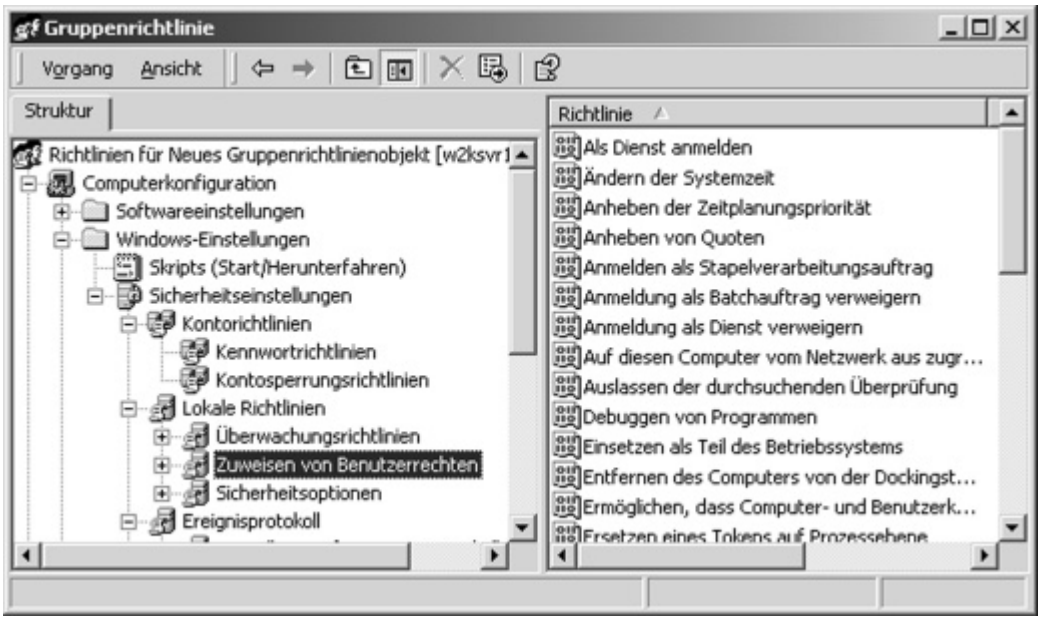

Bild 3: Sicherheitseinstellungen können über Gruppenrichtlinien skaliert werden

Sicherheit unter Windows 2000

Ein besonderes Augenmerk aus Sicht der Revision gilt natürlich den Sicherheitseinstellungen, die unter Windows 2000 möglich sind. Windows 2000 bietet eine äußerst exakte Skalierbarkeit für jeden einzelnen Bereich der ADS bezüglich der Sicherheit. Für jedes Containerelement lassen sich über Gruppenrichtlinien explizite Einstellungen vornehmen, die an alle darin befindlichen Objekte, also weitere Container und Blattobjekte, vererbt werden (Bild 3). Die Richtlinien teilen sich in drei Kategorien mit jeweils mehreren Unterkategorien auf:

- Kontorichtlinien
  - Kennwortrichtlinien
  - Kontosperrungsrichtlinien
- Lokale Richtlinien
  - Überwachungsrichtlinien
  - Zuweisen von Benutzerrechten
  - Sicherheitsoptionen
- Einstellungen für Ereignisprotokolle
  - Einstellungen für Ereignisprotokolle

Die Unterkategorien bieten eine Vielzahl an Sicherheitspunkten, die einzeln deklariert und aktiviert werden können. Der Clou: Jede Richtlinie lässt sich über eine Datenbank mit einer Vorgabe mittels eines Konfigurations- und Analysetools prüfen. Für die Revision stellt dies eine einmalige Chance dar, vor der Migration mit der Administration eine Vorgabe zu definieren, die später bei einer Prüfung gegengeprüft werden kann. Aber auch die Administration kann sich die Arbeit bei der Einrichtung von Sicherheitsrichtlinien erheblich erleichtern, denn alle Richtlinien lassen sich sowohl exportieren als auch importieren. Microsoft hat sogar einige fertige Sicherheitsvorlagen in binärer Form mitgeliefert, die sich nach Belieben importieren und untersuchen lassen. Doch sei an dieser Stelle zur Vorsicht und wieder ein Mal zur guten Planung geraten. Denn einige der vorgefertigten Sicherheitskonfigurationen sind **sehr(!)** restriktiv und würden den Arbeitsfluss in einigen Unternehmungen/ Abteilungen erheblich gefährden. So ist in einer der Sicherheitsvorlagen u. a. die Vorgabe zu finden, dass ein Benutzer ein Passwort von 8 Zeichen Länge in Verbindung mit einer Komplexitätsanforderung (Groß-/Kleinschreibung, Sonderzeichen und Zahl) vorweisen muss. Da solche Restriktionen die Benutzer dazu anregen würden,mit sogenannten „Passwortzetteln“ durch die Abteilungen zu marschieren, sind diese für die meisten Unternehmen als sinnlos oder gar gefährlich einzustufen.

Gruppen unter Windows 2000

Wie schon erwähnt sind die wichtigsten Funktionen von Windows 2000 nur im „einheitlichen Modus“ zu finden. Zu den signifikanten funktionellen Einschränkungen gehört die Verwaltung der Gruppen. Windows 2000 fährt mit 3 bzw. 4 Gruppen auf. Da ist zunächst die Domänenlokale. Sie hat die gleiche

Funktion wie die lokale Gruppe unter NT4. Sie kann also, wenn auf einem DC eingerichtet, nur innerhalb der lokalen Domäne eingesetzt werden, oder, wenn auf einem Member-Server eingerichtet, nur auf diesem einen Server verwendet werden. Die nächste Gruppe wäre die Globale. Sie kann domänenübergreifend eingesetzt werden und kann, was neu ist, andere globale Gruppen enthalten. Eine Verschachtelung mit globalen Gruppen ist also möglich. Die letzte Gruppe ist die Universelle. Sie wird nicht wie die anderen in den Domänen verwaltet, sondern über den globalen Katalog. Universelle Gruppen sollten möglichst statisch eingerichtet werden, da auf Grund ihrer Verwaltung im globalen Katalog bei jeder Änderung ein erheblicher Replikationsaufwand entsteht. Der Vorteil der universellen Gruppe liegt darin, dass sie in der gesamten Struktur eingesetzt werden kann. Es wäre also endlich möglich, eine unternehmensweite Gruppe der Revision einzurichten, die in der gesamten Struktur „Leserechte“ erhalten könnte. Auf diese Weise lässt sich der Verwaltungsaufwand natürlich erheblich verringern. Doch sei wieder zur genauen Planung ermahnt, denn auch Microsoft hat erkannt, dass der Replikationsverkehr mit jeder universellen Gruppe steigt und daher dazu angeraten, die Anzahl der universellen Gruppen so klein wie möglich zu halten bzw., wie schon erwähnt, so statisch wie möglich. Leider fällt genau die universelle Gruppe und die Möglichkeit der Verschachtelung im „gemischten Modus“ weg. In Bild 4 sind die Verschachtelungsmöglichkeiten unter Windows 2000 zu sehen.

Auch hier wird schnell klar, dass das Berechtigungskonzept der Gruppen und deren Mitglieder zur Aufrechterhaltung der Transparenz genau geplant sein will. Für die Revision bedeutet dies, dass *ex ante* Vorgaben gemacht werden müssen, die sowohl die Verschachtelungstiefe unternehmensweit festlegen als auch den Dokumentationsumfang festlegen. Gerade die Flexibilität der Gruppenmitgliedschaften kann ohne entsprechende Vorgaben zur Unprüfbarkeit führen. In kleinen und mittelständischen Unter-

Universal	**Global**	**Lokale Domäne**
Domänen im einheitlichen Modus können Konten, globale Gruppen und universelle Gruppen aus einer beliebigen Domäne als Mitglieder haben.	Domänen im einheitlichen Modus können Konten und globale Gruppen aus derselben Domäne als Mitglieder haben.	Domänen im einheitlichen Modus können Konten, globale Gruppen und universelle Gruppen aus einer beliebigen Domäne sowie Gruppen der lokalen Domäne aus derselben Domäne als Mitglieder haben.
In Domänen im einheitlichen Modus können keine Sicherheitsgruppen mit dem Bereich "Universal" erstellt werden.	Domänen im einheitlichen Modus können Konten aus derselben Domäne als Mitglieder haben.	Domänen im einheitlichen Modus können Konten und globale Gruppen aus beliebigen Domänen als Mitglieder haben.
Gruppen können in anderen Gruppen aufgenommen werden (sofern die Domäne im einheitlichen Modus ausgeführt wird), und ihnen können in jeder beliebigen Domäne Berechtigungen zugeordnet werden.	Gruppen können in andere Gruppen aufgenommen werden, und ihnen können in jeder beliebigen Domäne Berechtigungen zugeordnet werden.	Gruppen können in andere Gruppen der lokalen Domäne aufgenommen werden, und ihnen können nur Berechtigungen in derselben Domäne zugeordnet werden.
Kann nicht in einen anderen Gruppenbereich konvertiert werden.	Kann in den Gruppenbereich "Universal" konvertiert werden, solange keine Mitgliedschaft in einer anderen Gruppe mit dem Bereich "Global" besteht.	Kann in den Gruppenbereich "Universal" konvertiert werden, solange keine andere Gruppe mit dem Bereich "Lokale Domäne" Mitglied ist.

Bild 4: Gruppen und deren Verschachtelungsmöglichkeiten im einheitlichen Modus

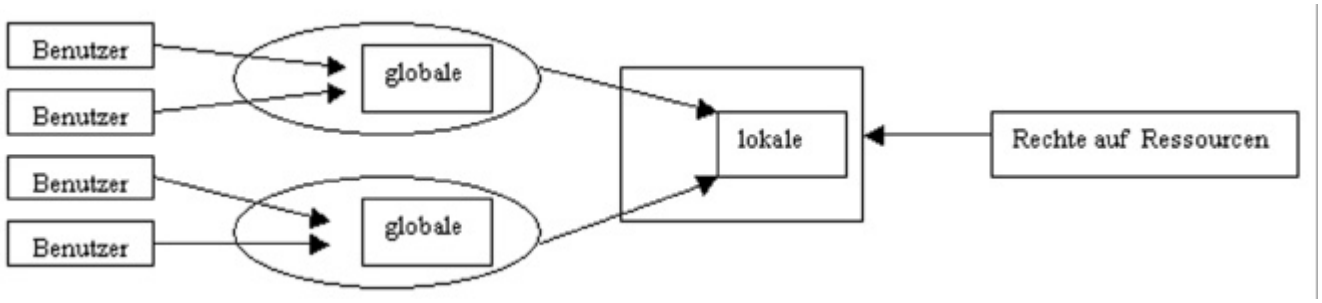

Bild 5: Gruppenstruktur für kleine und mittelständische Unternehmen

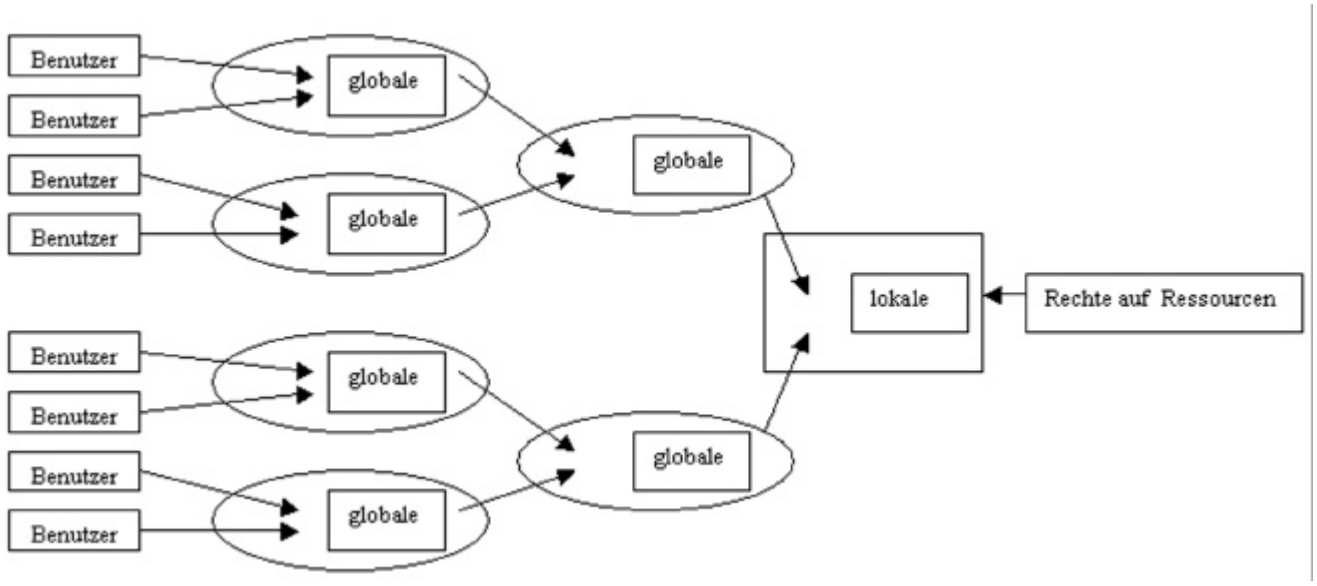

Bild 6: Gruppenstruktur für Großunternehmen

nehmen empfiehlt es sich, die von NT4 her bekannte Vorgabe zu übernehmen (Bild 5): Benutzer werden in globalen Gruppen zusammengefasst, globale Gruppen werden zu lokalen Gruppen zusammengefasst, lokale Gruppen bekommen Rechte. Großunternehmen können die von Microsoft empfohlene Strategie übernehmen (Bild 6): Benutzer werden zu globalen Gruppen zusammengefasst, die globalen Gruppen in weitere globale Gruppen verschachtelt, zusammengefasst, und in letzter Instanz werden die globalen Gruppen zu lokalen Gruppen zusammengefasst, welche dann die Rechte erhalten.

Resümee

Die Migration von Windows NT 4 nach Windows 2000 stellt sowohl die Administration als auch die Revision vor eine große Aufgabe. Zum Einen müssen der logische und physikalische Ist-Zustand des NT4 Netzes genau erfasst und dokumentiert werden, zum Anderen ist eine Überprüfung der Kompatibilität und eine genaue Planung der Windows 2000-Umgebung und der ADS ein unbedingtes Muss für die Migration. Insbesondere die Vorgaben, die erstellt werden müssen, um eine „Sicherheit von Anfang an“ zu gewährleisten, sind essenziell. Nur so kann vermieden werden, dass der bisher entstandene „Netzwerkmüll“, also Benutzer-/Gruppenleichen etc., mit in die neue Umgebung übernommen werden. Hat die Migration erst einmal begonnen, so ist diese möglichst schnell abzuschließen, da der volle Funktionsumfang von Windows 2000 nur im „einheitlichen Modus“ erreicht wird. Der auf den ersten Blick absurde Gedanke, statt über eine Migration mit einer Neueinrichtung auf Windows 2000 umzustellen, rückt, wenn man den Aufwand der Migration genau betrachtet, in ein neues Licht. Welche der beiden Umstellungsvarianten die bessere ist, bleibt offen. Tatsache ist, dass nach der Umstellung mit Windows 2000 eine sehr leistungsstarke Betriebssystemumgebung zur Verfügung steht, die bei richtiger Planung durch die gegebene Prüfbarkeit der Revision und durch die damit implizit gegebene Administrierbarkeit auch der Administration erhebliche Vorteile bringt.

<

Ausgesuchte Berechtigungsobjekte des SAP R/3-Systems als Prüfungsansatz für die IV-Revision

Teil I: Eine Übersicht

Von Dipl.-Betriebswirt Christoph Wildensee,
Stadtwerke Hannover AG und Mitglied im Prüfungsteam der RevCon GmbH, Hannover

Das SAP R/3 - System ist so umfangreich und vielschichtig wie kaum ein anderes DV-System mit dem Anspruch eines ganzheitlichen Charakters. Prüfungen in diesem Umfeld durchzuführen ist nicht ganz unproblematisch. Erschwerend wirkt sich zum einen die große Anzahl von Verwaltungsobjekten wie Transaktionen, Profilen/Sammelprofilen, Rollen/Aktivitätsgruppen und Berechtigungsobjekten aus, zum anderen aber besonders auch die Semantik dieser Objekte, die sich in den Einzelausprägungen der einzustellenden Objektkriterien widerspiegeln. Weiterhin bedeutsam ist die Möglichkeit der Mehrfachverschachtelung von Profilen/ Sammelprofilen über mehrere Iterationsstufen, die Berechtigungszuweisungen verschleiern kann.

Einführung

Bisher ist es für den Revisor nicht immer eindeutig, welche Systemumgebungsparameter und Berechtigungsobjekte für ihn relevant sind. Die Betrachtung unterscheidet sich natürlich durch den Prüfansatz, d. h. prüft er als IV-Revisor im überwiegenden Bereich der Basis oder z. B. als kaufmännischer Revisor im Bereich Finanzwesen/Controlling/Kostenrechnung. Eine umfassende Übersicht über vorhandene relevante Berechtigungsobjekte und deren Ausprägungen ist bisher nicht vorhanden, so dass jeder Prüfer doch eher auf sich gestellt ist.

Dieser Artikel soll eine Übersicht über einige der wichtigsten Berechtigungsobjekte geben, die für die Prüfung der SAP-Basis und in einem späteren Schritt des Bereiches FI/CO relevant sind. Weiterhin sollen auch kurz die Problemstellungen dargelegt werden, die mit der Prüfung dieser Objekte verbunden sind. Umfassend ist natürlich auch diese Übersicht nicht, sie kann aber Hinweise für zukünftige Prüfungen geben.

SAP R/3 - Betrachtungsebene

Bevor das Berechtigungsumfeld von SAP R/3 geprüft wird, sollte dem Revisor bewusst sein, was eine Prüfung in diesem Umfeld bedeutet. Die SAP R/3-Berechtigungsvergabe ist das Zusammenspiel von Transaktionen (Berechtigungsobjekt S_TCODE [Feld TCD]) und Berechtigungsobjekten, zusammengefasst in Profilen/Sammelprofilen und diese wiederum in aufgabenorientierten Rollen/Aktivitätsgruppen.

Basis einer sinnvollen Berechtigungskonzeption ist somit in erster Linie das Berechtigungsobjekt, welches Profilen/Sammelprofilen zugewiesen wird. Ausschlaggebend ist die jeweilige Einzelausprägung der Kriteriensteuerung des Berechtigungsobjektes, welches somit über den Zugriff zu SAP-Ressourcen entscheidet.

Über die zielführende Definition von Aktivitätsgruppen/Rollen und Profilen/Sammelprofilen lässt sich streiten, so dass dies unternehmensspezifisch zu klären und nicht Thema dieses Artikels ist. Streiten kann man sich jedoch nicht über die Wirkung und notwendige restriktive Vergabe von Rechten auf einzelne kritische Berechtigungsobjekte der SAP-Module, so dass hier eine Auswahl kritischer Berechtigungsobjekte dargestellt werden soll, die für Revisoren von besonderer Bedeutung sind.

Besonderheiten beim Prüfungsvorgehen

Zur Prüfung des SAP R/3-Umfeldes stehen mehrere Instrumentarien zur Verfügung. Zum Einen die SAP-

eigenen Mittel wie z. B. das Audit Information System (AIS; Transaktion SECR; releaseabhängig), welches in strukturierter Form die vorhandenen Auswertungsreports zur Verfügung stellt, natürlich das Reporting selbst, um notwendige ABAP's direkt aufzurufen (z. B. RSUSR002 o. Ä.) und die Systemverwalterfunktionen (z. B. Werkzeuge - Administration - Benutzerpflege - Berechtigung/Profile/Benutzer [...]Transaktionen SU0x).

Zum Anderen kann z. B. auch SAPaudit als externes Prüfungswerkzeug zum Einsatz kommen, das vielfältige Auswertungsmöglichkeiten zur Verfügung stellt, die SAP direkt nicht bietet. (www.sapaudit.de)

Zu Beginn einer Prüfung sollten die Analyse und Dokumentation des zu untersuchenden Systems stehen. Dieses erfolgt u. a. mit dem Report RSPARAM, der insbesondere in den Parametern login/...., DIR_...., rdisp/...., rec/client und auth/.... geprüft werden sollte.

Bei der weiteren Vorgehensweise und der Nutzung der Instrumentarien ist in jedem Fall der Grundsatz der restriktiven Vergabe von Rechten zu beachten. Auch wenn dem Benutzer in R/3 zur Nutzung einer Berechtigung nicht jede Ausprägung zugedacht wurde (Transaktion + Berechtigungsobjekt + Einzelausprägung), sollten die Zuweisungen der Berechtigungsobjekte und Einzelausprägungen nicht freigiebig erfolgen.

Ausgesuchte Berechtigungsobjekte

Die nachfolgenden Berechtigungsobjekte stehen hier als Auszug kritischer Objekte. Die Darstellung ist so zu lesen, dass links das Berechtigungsobjekt mit Beschreibung steht, rechts daneben die Steuerungsobjekte (Felder) und z. T. die Referenztabelle, die die Ausprägung des Steuerungsfeldes definiert (kursiv dargestellt; einsehbar mit der Transaktion SE16), daneben als kritisch zu untersuchende Ausprägungen mit kurzer Bemerkung.

Natürlich ist auch die Kombination von Berechtigungsobjekten mit entsprechenden Einzelausprägungen wichtig, wie dies in der Tabelle vereinzelt angedeutet ist.

Die Suche nach Berechtigungsobjekten kann über „Werkzeuge - Administration - Benutzerpflege - Berechtigung - Info - Objektliste m. Doku“ erfolgen. Hier sind die Objekte ausführlich dokumentiert.

Basisberechtigungsobjekt

Berecht.obj.		**Feld 1** *Prüftabelle*	**Feld 2** *Prüftabelle*	**Feld 3** *Prüftabelle*	**Feld 4** *Prüftabelle*	**Feld 5** *Prüftabelle*
	Kritische Berechtigung	Krit. Feldwert	Krit. Feldwert	Krit. Feldwert	Krit. Feldwert	Krit. Feldwert
S_GUI GUI-Aktivitäten		**ACTVT** *TACT/TACTZ*				
	Download von Reports und Tabellen	61				
S_DEVELOP Entwicklerberechtigungen Zur Anwendungsentwicklung ist zusätzlich ein Entwicklerschlüssel (Tabelle DEVACCESS) notwendig		**ACTVT** *TACT/TACTZ*	**DEVCLASS** *TDEVC*	**OBJNAME**	**OBJTYPE** *EUOBJ*	**P_GROUP** *TPGP*
	Anlegen	01	Z*	Z* oder Y*	DYNP, FUGR, PROG, LDBA, TRAN, DEVC, DOMA, STRU, TAB*, VIEW, SQLT, SUSO, *	
	Ändern	02				
	Aktivieren/ Generieren	07				
	Ausführen	16				
	Generalberecht.	*	*	*		*
	Die hier zu Grunde liegenden Objekte sind sehr vielfältig, so z. B. Dynpros, Funktionsbausteingruppen, Programme, Entwicklungsklassen, logische Datenbanken, Menüs, Transaktionen, Domänen/Strukturen/ Tabellen, Views, Clustertabellen, Sperrobjekte usw.					

S_RFC RFC-Zugriffs-berechtigung		**ACTVT** *TACT/TACTZ*	**RFC_NAME**	**RFC_TYPE**		
	Ausführen eines Zugriffs	16	*	FUGR		
S_TABU_CLI Änderung mandanten-unabhängiger Tabellen in Kombination		**CLIIDMAINT**				
	Zugriff auf mandatenunab-hängige Tab.	'X'				'X' sollte nur bei wenigen Usern vorkom-men wie Admin
S_TABU_DIS Tabellenpflege S_TABU_CLI -> 'X' sollte mit S_TABU_DIS -> 02 nur bei Basis-Admin liegen, mit 03 bei Show-Usern (Revi, bDSB, ggf. BR)		**ACTVT** *TACT/TACTZ*	**DICBERCLS** *s. TDDAT*			
	Ändern von Tabellen der Basis	02	S*			
	Ändern von Tabellen Personal	02	P*, T5*			
	Generalberecht.	*	*			
S_PATH Filezugriff aus ABAP		**ACTVT** *TACT/TACTZ*	**FS_BRGRU** *s. SPTH / SPTHB*			
	Pflegeberecht.	02				
	Generalberecht.	*	*			Sollte bei keinem üblichen Nutzer zu finden sein.
S_BDC_MONI Batch-Input-Berechtigung		**BDCAKTI**	**BDCGROUPID**			
	Mappe einer best. Gruppe (u. Protokoll) ...		z. B. Gruppe RF* = Finanzbereich			
	...für Hinter-grundverarbei-tung übergeben	ABTC				
	...analysieren	ANAL				
	...im Dialog abspielen	AONL				
	...löschen	DELE				
	...freigeben	FREE				
	...sperren/ entsperren	LOCK				
	...reorganisieren	REOG				
	Generalberecht.	*				

S_BTCH_JOB		**JOBACTION**	**JOBGROUP**			
Batch-Job-Steuerung	autom. Freigabe eigener Jobs	RELE				
Die Job-Steuerung ist als kritisch anzusehen, Beschränkung auf den aktuellen Mandanten.	Anz. alle Spoolaufträge	SP01				
	Anz. aller Verarbeitungs.-protokolle	PROT				
	Anz. fremde Job-Def. und Details	SHOW				
	Löschen von Jobs (auch fremde)	DELE				
in Kombination	Anz. fremder Spool-Aufträge	LIST				
	Generalberecht.	*	*			
S_BTCH_ NAM		**BTCUNAME**				
Angabe des Batch-Benut-zernamens für Berechtigungs-prüfung	Generalberecht.	*	Stellt die Berechtigung zur Verfügung, unter der ein Job abläuft. Diese Kombination kommt insb. in Fachbereichen mit umfangreichen Batch-Input-Aktivitäten vor wie Finanz- und Pers.bereich.			
S_BTCH_ ADM		**BTCADMIN**				
Batch-Administrator/ Job-Super-User	Generalberecht. Admin-Berecht.	* Y (= Yes)	Ausführen aller Operationen auf alle Jobs mandantenübergreifend, auch externe Programme in Job-Steps ausführen Nur für besondere Funktionsträger innerhalb der Fachbereiche sinnvoll -> Batch-Admin, Modul-Admin, System-Admin			
S_CTS_ADMI		**CTS_ADM FCT**				
Administration des Change & Transport Systems	Änderung der Systemänder-barkeit	SYSC	Diese Berechti-gung sollte ausschließlich in der Hand der Basis-Admin. liegen.			
	Pflege der Steuertabellen (auch TCODE SE03 Work BenchOrgan.)	TABL				
	Auslösen von Importen (Transp.Mngm System)	IMPT				
	Initialisierung des WBO nach Systemkopie (TCODE SE06)	INIT				
	Generalberecht.	*				
S_C_FUNCT		**ACTVT** *TACT/TACTZ*	**CFUNCNAME**	**PROGRAM**		restriktive Vergabe; nur für Basis-Admin
direkter Aufruf von C-Kernel-Funktionen aus ABAP	Ausführen	16				
	Audit Konf.			RSAUCONF		
	Generalberecht.	*	*	*		

S_CLNT_IMP Dateiimport bei Mandanten-kopie		**ACTVT** *TACT/TACTZ*				
	Generalberecht. Importieren	* 60				
S_DATASET Berechtigung zum Dateizu-griff auf Betriebssystem-ebene; auch Berechtigung zur Benutzung von BS-Kommandos als Dateifilter		**ACTVT** *TACT/TACTZ*	**FILENAME**	**PROGRAM**		
	Schreibender Zugriff	34	auf alle Dateien auf BS-Ebene = *	z. B. Finanzber. RF* und ZF*	sollte auf einige wenige bekannte Programme beschränkt werden. -> z. B. RSWATCH0	
	Schreibender Zugriff mit Filter	A7				
S_ENQUE Anzeigen und Löschen von Sperreinträgen BObjekt für Administration.		**S_ENQ_ACT**				
	Anz. fremder Sperrobjekte	DPFC				
	Lösch. fremder Sperrobjekte	DLFU				
	Generalberecht. auch fremd. Mandant	* oder ALL				
S_LOG_COM Logische Betriebssystem-kommandos		**COMMAND** *SXPGCOSTAB/ SXPGCOTABE*	**HOST**	**OPSYSTEM**		
	Generalberecht.	* siehe auch Transaktion SM69	* z. B. Win NT SY-OPSYS	* SY-HOST		Nur für System-Admin !
S_NUMBER Nummernkreis-pflege; Berechtigung zur Verwaltung der Nummern-kreise -> Belege, Kred./ Deb./Sachk. etc.		**ACTVT** *TACT/TACTZ*	**NROBJ** *TNRO/TNRGT*			Hierüber kann "hart" in das Systemver-halten einge-griffen werden. Zu beachten: Gesetzl. Rahmenbedin-gungen. Administra-tionsobjekt.
	Hinzufügen/ Ändern eines Objektes	01/02				
	Nummerkreis-stand eines Obj. ändern	11				
	Nummerstände eines Objektes initialisieren	13				
	Nummernkreis-objekt pflegen	17				
	Generalberecht.	*	*			
S_OLE_CALL OLE-Aufruf aus ABAP		**ACTVT** *TACT/TACTZ*	**OLE_APPL**	**PROGRAM**		
	Ausführen	16				Für Admin.
	Generalberecht.	*	*	*		

S_ADMI_FCD		**S_ADMI_FCD**				
Systemberechtigungen	Netzwerkadministration, z. B. Verwaltung von RFC-Verbindungen	NADM				restriktive Vergabe; nur für Basis-Admin
	Prozessadministration, z. B. Verwaltung der Benutzer-Modi mit TA SM04	PADM				
	Sperren / Entsperren von Transaktionen	TLCK				
	Verbuchungsadministration mit TA SM13	UADM				
	Anlegen neuer Mandanten (nur in Kombi. mit S_TABU_DIS und S_TABU_CLI)	T000				
	Mandantenübergreifende Spooladministration, u. a. Einsehen Druckaufträge in allen Mandanten	SPAD + SPAM + SP01				
	Einsehen aller Druckaufträge des eigenen Mandanten (nur in Kombi. mit S_SPO_ACT)	SP01				
	Löschen alter AuditLogs	AUDA				
	Ausführen von UNIX-Befehlen	UNIX				
	Daten löschen ohne Archivierung	RSET				
S_USER_OBJ		**ACTVT**	**OBJECT**			
Ausschalten von Berechtigungsobjekten		*TACT/TACTZ*	*TOBJ*			
	Aus/Anschalten von BO	02				
	Aktivieren der Änderungen	07				

S_USER_GRP Verwaltung von Benutzern		**ACTVT** *TACT/TACTZ*	**CLASS** *USGRP*			
	Anlegen von Benutzern	01				
	Ändern von Benutzer inkl. Profilzuordnung	02 + 22				
	Löschen von Benutzern	06				
	Kennwörter vergeben und Sperren/ Entsperren	05				
	Benutzer SAP* löschen	06	SUPER			
S_USER_AGR Verwaltung von Aktivitätsgruppen		**ACTVT** *TACT/TACTZ*	**ACT_GROUP** *AGR_DEFINE/ AGR_AGRS*			
	Anlegen neuer AGs	01				
	Ändern von AGs mit Profilgenerierung	02 + 64				
	Benutzer zu AG zuordnen	22				
	ASs löschen	06				
S_USER_PRO Verwaltung der Profile		**ACTVT** *TACT/TACTZ*	**PROFILE** *USR10*			
	Anlegen neuer Profile	01				
	Ändern von Profilen	02				
	Löschen von Profilen	06				
	Aktivieren von Profilen	07				
S_USER_AUT Verwaltung der Berechtigungen		**ACTVT** *TACT/TACTZ*	**AUTH** *USR12*	**OBJECT** *TOBJ*		
	Anlegen neuer Berechtg.	01				
	Ändern von Berechtg.	02				
	Löschen von Berechtg.	06				
	Aktivieren von Berechtg.	07				

S_RZL_ADM Rechenzentrum leitstand		**ACTVT** *TACT/TACTZ*				restriktive Vergabe; nur für Basis-Admin
	Systemparameter pflegen, logische BS-Kommandos pflegen	01				
S_SCD0 Änderungsbelege verwalten		**ACTVT** *TACT/TACTZ*				restriktive Vergabe; nur für Basis-Admins
	Änderungebelege löschen (ist im Prod.-System nicht zulässig!)	06				
	Änderungebelegobjekte verwalten	12				
S_TABU_RFC RFC-Datenexport für Mandantenkopien und Vergleiche		**ACTVT** *TACT/TACTZ*				restriktive Vergabe; nur für Basis-Admins
	Berechtigung zum Vergleich und Datentransfer	03				
S_SPO_DEV Druckerberechtigungen		**SPODEVICE** *SH_PRIN*				
	Drucken auf allen Druckern	*				
S_SPO_ACT Zugriff auf Spool-Aufträge, die geschützt sind durch Berecht.zeich.-folgen (fremde Aufträge)		**SPOACTION**	**SPOAUTH**			
	Anz. Inhalt v. geschütztem Auftrag	DISP	Eingrenzung auf Gebiet, z. B. FI* o. Ä. Spool-Admin nicht zu freigiebig für übliche Nutzer			
	Ändern von Attributen eines gesch. Auftrags	ATTR				
	Ändern eines Berecht.wertes eines gesch. Auftrags	AUTH				
	gesch. Auftrag ausgeben 1.Mal	PRNT				
	gesch. Auftrag ausgeben mehrmals	REPR				
	manuelles Löschen	DELE				
	Ändern des Eigentümers	USER				

S_TRANSPRT		**ACTVT**	**TTYPE**			
Berechtigung zur Nutzung der Workb., Customizing und des TransportOrg.		*TACT/TACTZ*				
	Hinzufügen/ Erzeugen/ Ändern	01/02	DLOG	lok. Änd.auftr.		
	Sperren/Lösch.	05/06	DTRA	transport.bare Änder.auftr.		
	Freigeben	43	CUST	Custom.auftr.		
	Quellmandant eines Auftrags ändern	50	TRAN	Transporte v. Kopien		
	Import	60	CLCP	Mandanten-transporte		
	Freig. fremd. Aufträge	75				
	Generalberecht.	*				

Fazit und weiteres Vorgehen

Das SAP R/3-Berechtigungsumfeld ist ein umfangreiches und für den Revisor ergiebiges Gebiet, das - aufgeteilt in unterschiedliche Prüfungsschwerpunkte - mehrmals jährlich einer Prüfung unterzogen werden sollte. Die zuständigen Fachbereiche (SAP-Basis, Finanzbereich etc.) müssen jedoch auch angehalten werden, regelmäßig mit den eigenen Prüfungsschwerpunkten Reviews durchzuführen, um im Eigeninteresse Transparenz über die zugrundeliegenden Berechtigungen zu erhalten.

Im Zuge der Vor- und Nachbereitung von Berechtigungsprüfungen ist bei der Vielzahl von Prüfobjekten in SAP R/3 eine Dokumentation wie hier vorliegend sinnvoll. Als Ergebnis sollten vorhandene Profile um die entsprechenden Berechtigungsobjekte und Einzelausprägungen - insbesondere mit Generalfunktionalität - korrigiert werden, besonders auch die der Basis- und Modul-Administration.

Die Fortsetzung dieses Artikels wird sich auf gleiche Weise mit den Berechtigungsobjekten der Module FI und CO beschäftigen. Gerade auch in diesen Bereichen werden oftmals umfangreiche Berechtigungen zur Debitoren-, Kreditoren-, Sach- und Anlagenverwaltung vergeben, aus denen nicht unerhebliches Gefahrenpotenzial resultiert. (Tabelle 2)

01	Hinzufügen/Erzeugen	23	Pflegen	64	Generieren
02	Ändern	24	Archivieren	65	Reorganisieren
03	Anzeigen	27	Summensätze anzeigen	66	Aktualisieren
04	Drucken	28	Einzelposten anzeigen	70	Verwalten, Administrieren
05	Sperren	29	Gespeicherte Daten anzeigen	71	Auswerten
06	Löschen	33	Lesen	85	Stornieren
07	Aktivieren/Generieren	41	Löschen auf Datenbank	91	Reaktivieren
08	Änderungsbelege anzeigen	42	Umsetzen auf Datenbank	A1	Rückstellen
10	Buchen	40	Anlegen auf Datenbank	A2	Auszahlen
16	Ausführen	60	Importieren	A3	Status ändern
21	Transportieren	61	Exportieren	A5	Berichte anzeigen
22	Eintragen, Aufnehmen, Zuordnen	63	Aktivieren	A6	Lesen mit Filter

Tabelle 2: Auszug aus der Aktivitätenliste

Ausgesuchte Literatur:

Thomas Tiede	SAP R/3 Ordnungsmäßigkeit und Prüfung des SAP-Systems, 2000
Uwe Bernd-Striebeck/ Thomas Glauch u. a.	SAP R/3 Sicherheit und Prüfung, 1998
Paul Wenzel	Betriebswirtschaftliche Anwendungen des integrierten Systems SAP R/3, 1995
Horst Keller/ Sascha Krüger	ABAP Objects, 2001
Rüdiger Kretschmer/ Wolfgang Weiss	SAP R/3 - Entwicklung mit ABAP/4, 1999

Mein besonderer Dank gilt Thomas Tiede, Fa. *ibs schreiber gmbh*, Hamburg, Technischer Geschäftsführer und Leiter Qualitätsmanagement und Prüfungswesen, für die freundliche Unterstützung.

<

Liebe Leserin, lieber Leser!

Die Fortsetzung in ReVision IV/2001 hat das Thema:

Ausgesuchte Berechtigungsobjekte des SAP R/3-Systems als Prüfungsansatz für die IV-Revision Teil II: FI und CO

SAPaudit 2.0: Prüfung von SAP R/3 auf Knopfdruck?

Von Thomas Tiede
Geschäftsführer, ibs schreiber gmbh, Hamburg

Mit SAPaudit in der Version 2.0 wurde eine neue Dimension der Prüfungsmöglichkeiten für SAP R/3 geschaffen - weit über die R/3-eigenen Möglichkeiten (manuell oder mit dem AIS) hinaus. Prüfungen von Zugriffsberechtigungen, Systemsicherheit und modulbezogenem Customizing, die mit R/3 selbst mühsam und zeitraubend sind, lassen sich automatisieren und sind durch die mit SAPaudit 2.0 gegebenen Möglichkeiten in einem Bruchteil der Zeit durchführbar.
In diesem Artikel werden einige wesentliche Features von SAPaudit 2.0 aufgezeigt. Eine Darstellung des gesamten Programmumfanges ist im Rahmen dieses Artikels nicht möglich.

Einführung

Wer kennt sie nicht, die altbekannten Probleme bei jeder R/3-Prüfung:

Sie sollen die Systemsicherheit feststellen:

- Welche Systemparameter gibt es dafür, wie müssen sie eingestellt sein, welche Auswirkung haben sie (und was sind eigentlich „Systemparameter“)?
- Welche Tabellen sind sicherheitsrelevant, was darf in den Tabellen stehen und was nicht, was muss in den Tabellen stehen, welche Auswirkungen haben welche Einträge?

Sie sollen kritische Berechtigungen überprüfen:

- Ein Administrator kann Ihnen viele Vorgänge im R/3-System aufzählen, die hochkritisch und sicherheitsrelevant sind. Ein Entwickler kann Ihnen noch viel mehr hochkritische und sicherheitsrelevante Vorgänge aufzählen. Und ein Modulbetreuer kann Sie mit den kritischen Vorgängen in seinem Modul praktisch erschlagen. Und Sie sollen das gesamte Wissen auch parat haben, um die Berechtigungen auf die Vorgänge zu prüfen?
- Und wenn jemand Ihnen sagt: Die Berechtigung *Anlegen neuer Mandanten* ist im Produktivsystem eine der kritischsten Berechtigungen. Warum ist sie es? Ist sie es in jedem System - oder nur bei Ihnen? Wie wird dieser Vorgang denn von R/3 geschützt? Welche Berechtigungsobjekte mit welchen Feldwerten benötigt man für diesen Vorgang (und was ist überhaupt ein Berechtigungsobjekt)?
- Schlimmer wird es in den Anwendungsmodulen: Wer darf denn nun die Kontonummer Ihrer Kreditoren ändern? Welche Berechtigung ist dafür notwendig? Werden diese Felder über ein eigenes, optionales Berechtigungsobjekt (F_LFA1_AEN) bei Ihnen geschützt? Ist dies richtig konfiguriert (Tabellen T055/T055G)? Oder gibt es gar ein Vier-Augen-Prinzip für diesen Vorgang (Tabelle T055F/T055G)? Und was muss überhaupt in diesen Tabellen stehen, damit das alles richtig funktioniert und nicht umgangen werden kann?

Wahrscheinlich werden Sie diese Fragen kennen oder vielleicht doch nicht, weil Ihnen (wie den meisten internen und externen Prüfern) das Hintergrundwissen um einzelne Vorgänge in R/3 fehlt, um überhaupt diese Fragen stellen zu können? Und trotzdem sind Sie der Verantwortliche für die Prüfung und Bestätigung der Ordnungsmäßigkeit Ihres R/3-Berechtigungskonzeptes. In R/3 selbst stoßen Sie bereits bei den obigen Fragen an die Grenzen. Ohne sehr großes Hintergrundwissen werden Sie mit der Beantwortung Ihrer Fragen nicht weiterkommen, abgesehen davon, dass ohne umfassendes Wissen auch die einfachsten Fragestellungen zum Berechtigungskonzept von R/3 (und auch vom AIS) nicht beantwortet werden können. Und sollte Ihnen jemand etwas anderes erzählen: Lassen Sie es sich vom Betreffenden live am System mit konkre-

ten Fragestellungen zeigen, dann werden Sie es selber feststellen!

Bereits mit der SAPaudit-Version 1.1 wurden diese Fragen weit gehend beantwortet. Mit der SAPaudit-Version 2.0 wurden gänzlich neue Elemente implementiert, die nicht nur die Vorgänge überhaupt prüfbar machen, sondern strukturiert aufzeigen, was, warum und wie es zu prüfen ist.

Unter dem Punkt *Einführung in den technischen Teil* werden die wesentlichen neuen Features von SAPaudit 2.0 in Stichpunkten dargestellt. Im Punkt *Technische Beschreibung der Neuerungen* wird einzeln, mit Beispielen, auf diese Features eingegangen.

Einführung in den technischen Teil

Die maßgeblichen Neuerungen in SAPaudit 2.0:

- Implementierung eines Analysebaumes, in dem sowohl die Funktionalität von SAPaudit integriert ist als auch die einzelnen Punkte, die bei Prüfungen durchzuführen sind.
- Zu jedem Punkt im Analysebaum sind Texte hinterlegt, welche den zu prüfenden Vorgang beschreiben, Checklisten, Tabellen (soweit notwendig), Parameter, Standardberichte und kritische Berechtigungen (es sind bereits ca. 540 kritische Berechtigungen vordefiniert).
- Über den Analysebaum können die Prüfungen automatisiert werden, sind also „auf Knopfdruck“ durchführbar.
- Für kritische Berechtigungen können Vorgaben (z. B. berechtigte/unberechtigte Benutzer) hinterlegt werden, um kritische Vorgänge oder die Umsetzung von Vier-Augen-Prinzipien automatisiert überprüfen zu können. Außerdem kann selektiert werden, welche Benutzer ausgewertet werden sollen (z. B. keine Auswertung der SAP_ALL-Benutzer, nur Dialog-Benutzer, nur die nicht gesperrten, ...)
- Als Ergebnis der kritischen Berechtigungen werden nicht nur die Benutzer mitsamt der Herkunft der Rechte angezeigt, sondern auch die Profile und Aktivitätsgruppen, in denen das betreffende Recht vorhanden ist.
- Vom Analysebaum können beliebige Kopien erstellt werden, die völlig individuell an die Unternehmung und an eigene Bedürfnisse angepasst werden können. So können eigene kritische Berechtigungen implementiert werden, eigene Checklisten oder jegliche Texte eingebunden werden und völlig neue Strukturen erstellt werden.

Technische Beschreibung der Neuerungen

Der Analysebaum

Das Kernstück von SAPaudit 2.0 bildet der Analysebaum. In diesen Analysebaum, den jeder sehr leicht und komfortabel an die eigenen Bedürfnisse anpassen kann, ist alles integriert, was für eine Prüfung erforderlich ist. Er ist so konzipiert, dass er, geordnet nach einzelnen Prüfungsschritten, von oben nach unten „abgearbeitet“ werden kann. Folgendes Beispiel soll den Aufbau verdeutlichen:

Es soll eine Systemprüfung durchgeführt werden, in der die systemseitige Sicherheit des R/3-Systems überprüft wird. Im Analysebaum befindet sich hierzu ein Eintrag „System“. Unterhalb dieses Punktes ist als erstes eine Checkliste hinterlegt, anhand derer der Aufbau des Systems überprüft werden kann (Bild 1). Danach folgt ein Punkt „Systeminformationen“, welcher ein Fenster aufruft, in dem u. a. angezeigt wird, um welches R/3-Release es sich handelt, welche Datenbank und welches Betriebssystem eingesetzt wird.

Zur Prüfung der Systemsicherheit gehört als besonders relevanter Punkt auch die Anmeldesicherheit. Dies ist ein Unterpunkt vom Eintrag „System“ (siehe Bild 1). Zur Prüfung dieses Punktes ist hier folgendes hinterlegt:

- Die Anforderungen zur Absicherung der Anmeldesicherheit von R/3 (Text)
- Die Beschreibung der von R/3 genutzten Anmeldeparameter (Text)
- Eine Checkliste zur Anmeldesicherheit (Text)
- Die Kennwortkonventionen von R/3 (Text)
- Die eigen definierten verbotenen Kennwörter (Tabelle)
- Die Berechtigungen, die im Zuge der Anmeldesicherheit zu überprüfen sind:
  - Wer darf die Anmeldeparameter ändern? (Kritische Berechtigung)
  - Wer darf verbotene Kennwörter einpflegen? (Kritische Berechtigung)
  - Wer darf Kennwörter für Benutzer vergeben? (Kritische Berechtigung)
- Die Einstellungen der Anmeldeparameter

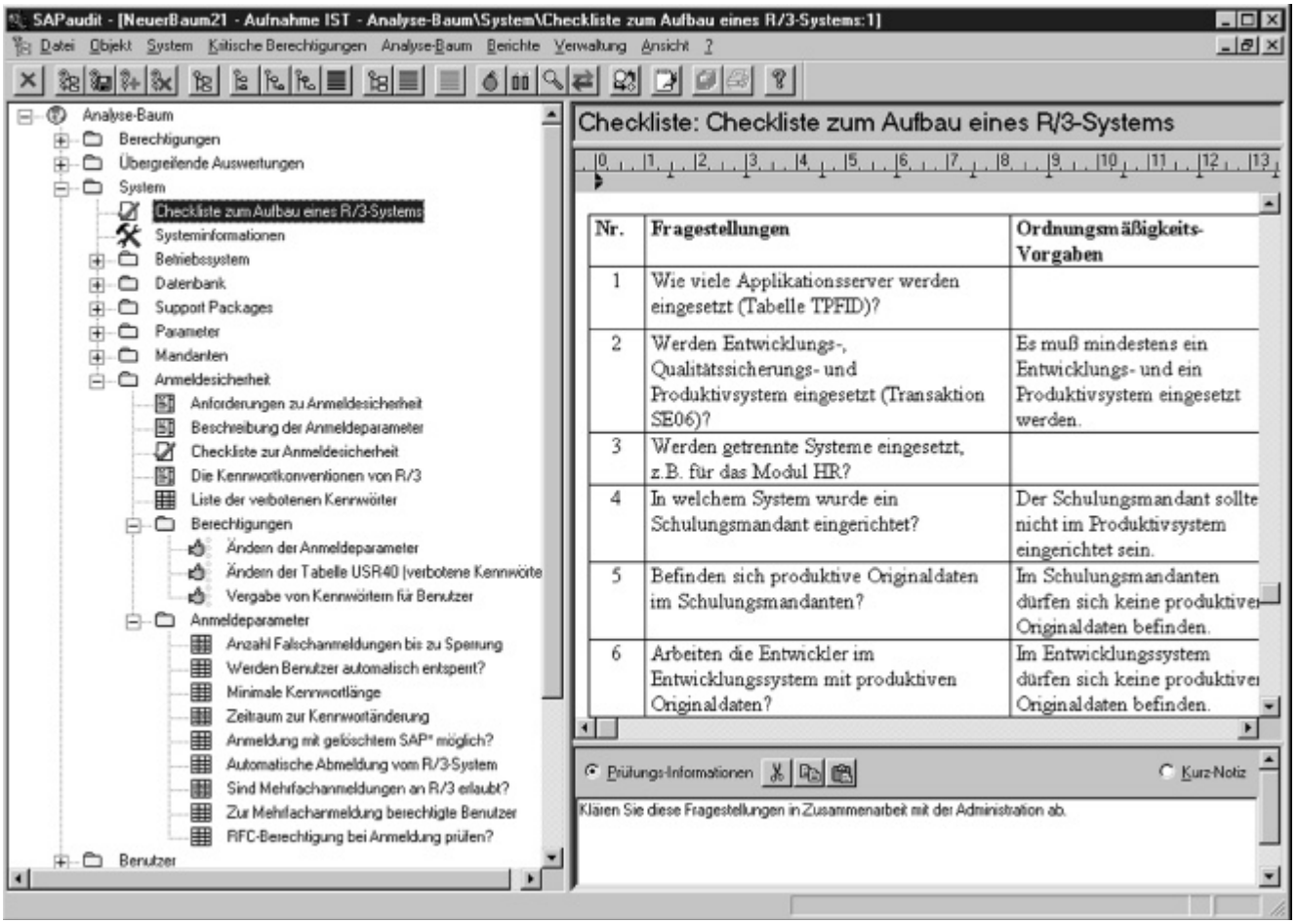

Bild 1: Der Prüfungspunkt System *mit dem geöffneten Unterpunkt* Anmeldesicherheit

- Mögliche Anzahl von Falschanmeldungen bis zur Sperrung (Tabelle)
- Werden gesperrte Benutzer automatisch entsperrt? (Tabelle)
- Minimale Kennwortlänge (Tabelle)
- Zeitraum zur Kennwortänderung (Tabelle)
- Ist eine Anmeldung mit einem gelöschten SAP* möglich? (Tabelle)
- Wann erfolgt eine automatische Abmeldung vom System? (Tabelle)
- Sind Mehrfachanmeldungen an R/3 erlaubt? (Tabelle)
- Welche Benutzer sind zu Mehrfachanmeldungen berechtigt? (Tabelle)
- Wird bei RFC-Anmeldungen die RFC-Berechtigung überprüft? (Tabelle)

Bei den Parametern werden jeweils die aktuellen Inhalte angezeigt. In Bild 2 ist der Parameter login/fails_to_user_lock (Mögliche Anzahl von Falschanmeldungen bis zur Sperrung) abgebildet. Im rechten unteren Teil des Fensters ist das darüber angezeigte Element beschrieben. Somit weiß der Prüfer, welche Auswirkung diese Einstellung hat und was sie bedeutet. Außerdem werden hier Vorgabewerte vorgeschlagen, wie der Parameter zu setzen ist.

Die drei zum Punkt Anmeldesicherheit gehörenden Berechtigungen können vollautomatisiert überprüft werden. Als Ergebnis werden die berechtigten Benutzer inklusive der Herkunft der Rechte angezeigt. In Bild 3 (Auswertung der Berechtigung *Ändern der Anmeldeparameter*) ist z. B. hinterlegt, dass der Benutzer EKEGLER (markiert) dieses Recht besitzt, weil er über die Aktivitätsgruppe *Revision* dieses Recht bekommen hat. Im rechten unteren Teil des Fensters ist die ausgewertete kritische Berechtigung beschrieben.

Zusätzlich werden hier auch alle Profile/Sammelprofile und Aktivitätsgruppen/Sammelaktivitätsgruppen aufgelistet, in denen dieses Recht enthalten ist. Diese Herkunftsermittlung ist mit SAP R/3

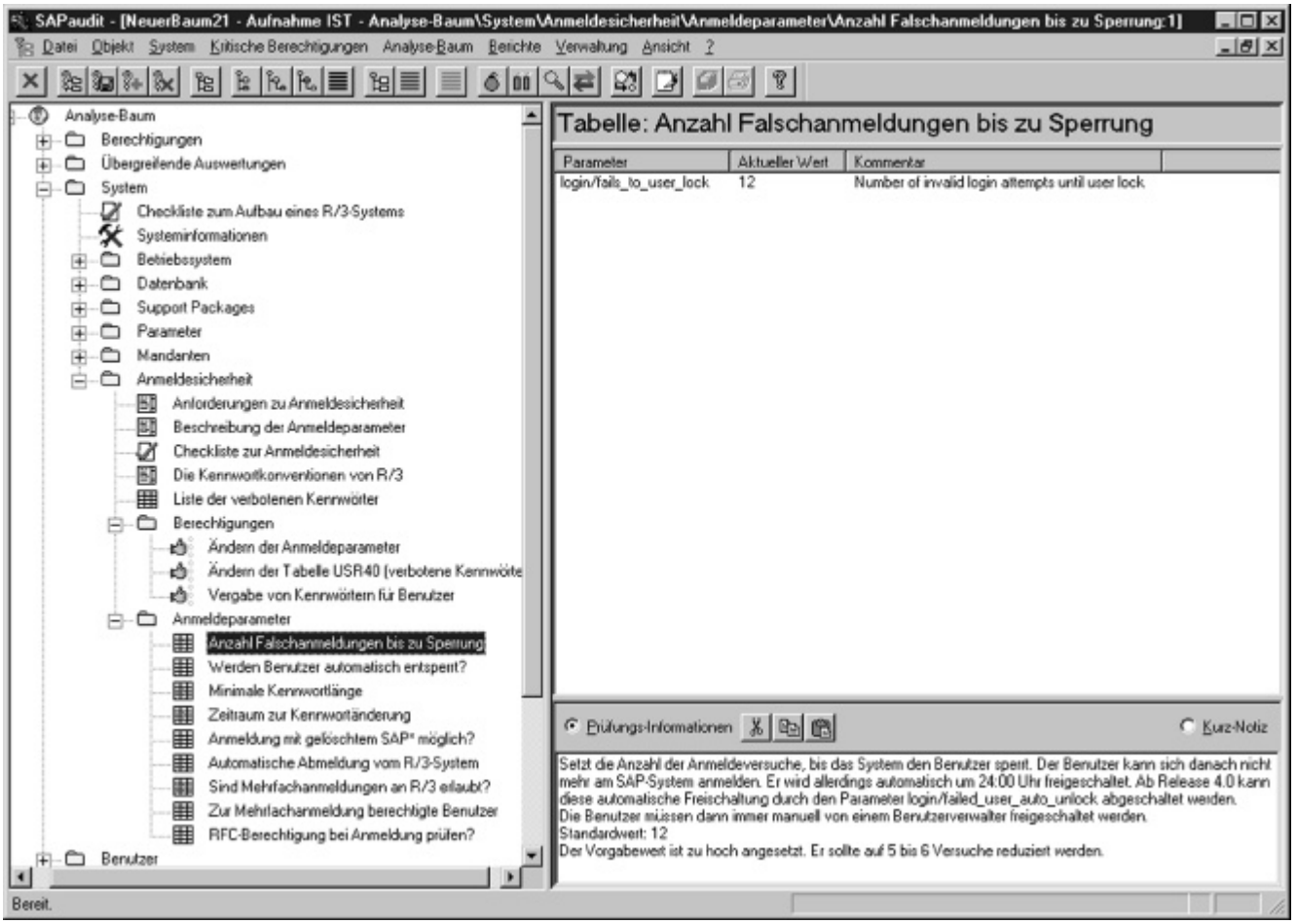

Bild 2: Anzeige einer Parametereinstellung

selbst gar nicht oder, mit viel Wissen, nur mit großem Aufwand möglich.

So können nun alle Punkte zur Prüfung der Anmeldesicherheit abgearbeitet werden. Jedes einzelne Ergebnis kann in einen Prüfbericht ausgegeben werden, welcher mit der SAPaudit-eigenen Textverarbeitung noch mit zusätzlichen Texten ergänzt werden kann.

Durch die integrierten Texte und Checklisten wird dem Prüfer aufgezeigt, was überhaupt zu prüfen ist. Bedingt durch die Komplexität des R/3-Systems wäre ansonsten ein sehr hohes R/3-Wissen über alle Prüfungspunkte erforderlich. Zusätzlich ist jedes einzelne zu prüfende Element im Analysebaum in den Prüfungsinformationen beschrieben. Hierdurch erhält der Prüfer für jeden Punkt den Hinweis, warum er zu prüfen ist und wie das Ergebnis zu deuten ist.

Mit dem Analysebaum können so die einzelnen Prüfungsschritte umfassend und in kürzester Zeit durchgeführt werden. Im Analysebaum sind folgende Elemente integriert:

- Ordner, mit denen die Struktur aufgebaut wird (die Struktur kann unternehmensbezogen beliebig angepasst oder neu aufgebaut werden)
- Kritische Berechtigungen (mit SAPaudit werden ca. 540 vordefinierte kritische Berechtigungen ausgeliefert. Eigene können beliebig definiert werden.)
- Checklisten (es können auch alle eigenen Checklisten eingebunden werden)
- Beliebige Texte (Prüfungsbeschreibungen, Vorgehensweisen, ...)
- Tabellen mit beliebigen Filterungen, z. B. von Benutzern, Profilen, Aktivitätsgruppen, Berechtigungen, Transaktionen, Mandanten, Parametern, Entwickler- und Objektschlüsseln, Buchungskreisen, Geschäftsbereichen, Einkaufs- und Verkaufsorganisationen, dem R/3-Data-Dictionary, ...
- Baumstrukturen, z. B. den Baum der Organisationsstruktur mit allen Verzweigungen oder die komplexen Bäume des Berechtigungskonzeptes (aufsteigende und absteigende Darstellung von Berechtigungsobjekten über Berechtigungen, Profile und Aktivitätsgruppen zu Benutzern)

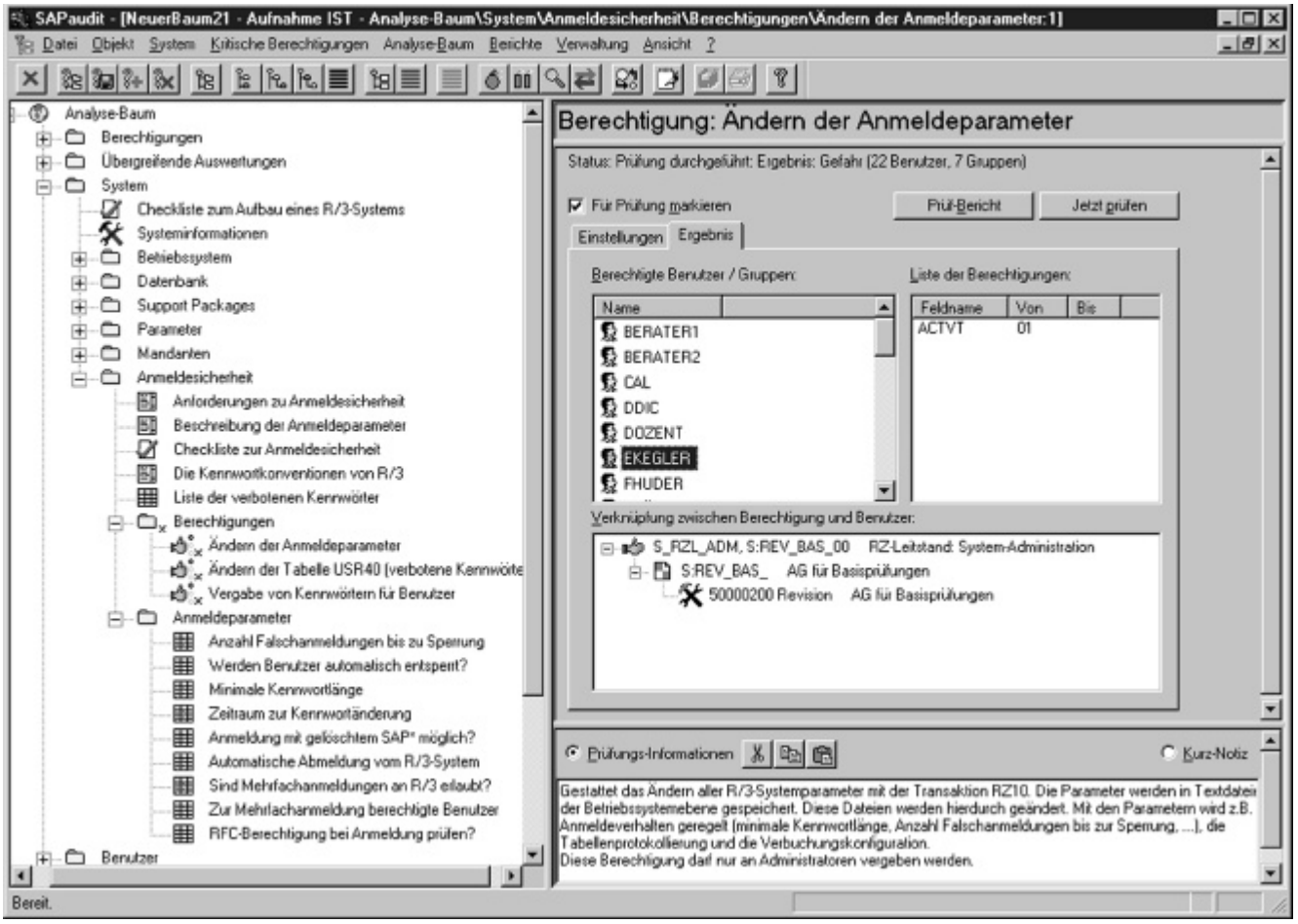

Bild 3: Anzeige der Auswertung einer kritischen Berechtigung

- Standardberichte über Benutzer, Profile, Aktivitätsgruppen, Berechtigungen, Transaktionen und Inkonsistenzen
- Transaktionen (SAPaudit ist in der Lage, im Gegensatz zu R/3 selbst, Berechtigungen auf Transaktionen automatisiert auch mit den zugehörigen Anwendungsberechtigungen auszuwerten)
- SAPaudit-Programmfunktionen wie z. B. Statistiken, Systeminformationen oder die Verwaltung und manuelle Auswertung der kritischen Berechtigungen

Vollständige Automatisierungsmöglichkeiten über den Analysebaum

Im Analysebaum sind die auszuwertenden Elemente nicht einfach nur zur manuellen Auswertung hinterlegt, sie können auch vollautomatisiert ausgewertet werden. Jede kritische Berechtigung und jeder Ordner können für eine automatisierte Prüfung markiert werden. In Bild 4 ist ein Zweig mit Berechtigungen abgebildet, welcher für die automatische Prüfung markiert wurde (zu erkennen am „x“ hinter dem Symbol).

Über einen Menüpunkt wird nun die Analyse gestartet, und SAPaudit wertet alle markierten Berechtigungen aus. Nach der Analyse kann das Ergebnis jeder einzelnen Berechtigung ausgewertet und in einen Bericht übernommen werden.

Als weitere Automation besteht die Möglichkeit, für jede kritische Berechtigung berechtigte oder/und unberechtigte Benutzer zu hinterlegen. Bei der Auswertung wird über eine Ampelsystematik angezeigt, ob z. B. unberechtigte Benutzer dieses Recht besitzen (rote Ampel), ob nur berechtigte Benutzer dieses Recht besitzen (grüne Ampel) oder ob Benutzer dieses Recht besitzen, die nicht in der Vorgabe enthalten waren (gelbe Ampel). Bild 5 zeigt beispielhaft die kritische Berechtigung *Benutzer der Gruppe SUPER* löschen. Berechtigt hierzu sind nur die Mitglieder der Gruppe SUPER. Auf keinen Fall dürfen dieses Recht die Mitglieder der Gruppe ADMIN

sowie die Benutzer JHOST, KLORE und PKROST besitzen.

Mit solchen Vorgaben ist es z. B. möglich, die Umsetzung von Vier-Augen-Prinzipien zu überwachen, z. B. bei der Berechtigungsvergabe oder in der Finanzbuchhaltung beim Anlegen und Bebuchen von Kreditoren oder Debitoren. Durch diese Systematik werden solche Überprüfungen umfassend überhaupt erst möglich.

Der Aufwand für Prüfungen des Berechtigungskonzeptes inklusive solcher Vier-Augen-Prinzipien u. Ä. ist mit SAPaudit minimal (siehe auch weiter hinten: Zeitersparnis und Qualitätssteigerung). Mit den R/3-eigenen Mitteln ist hier sehr großes Fachwissen über das Berechtigungskonzept notwendig sowie ein erheblich größerer Zeitraum. Beispielsweise bietet das für Prüfer gestaltete AIS keine Möglichkeiten zur Überprüfung der Zugriffsberechtigungen, außer dass die Standardreports (RSUSR*) von hier aus aufgerufen werden können. Jede einzelne Berechtigung muss dann trotzdem wieder „zu Fuß“ geprüft werden, wobei jedes Berechtigungsobjekt für jeden Vorgang bekannt sein muss.

Bild 4: Markierte kritische Berechtigungen für die automatische Analyse

Bild 5: Vorgaben berechtigter/unberechtigter Benutzer für eine kritische Berechtigung

Optionen zur Auswertung der kritischen Berechtigungen

Bei der Auswertung von kritischen Berechtigungen ist es immer sehr hilfreich, wenn als Ergebnis nicht nur die

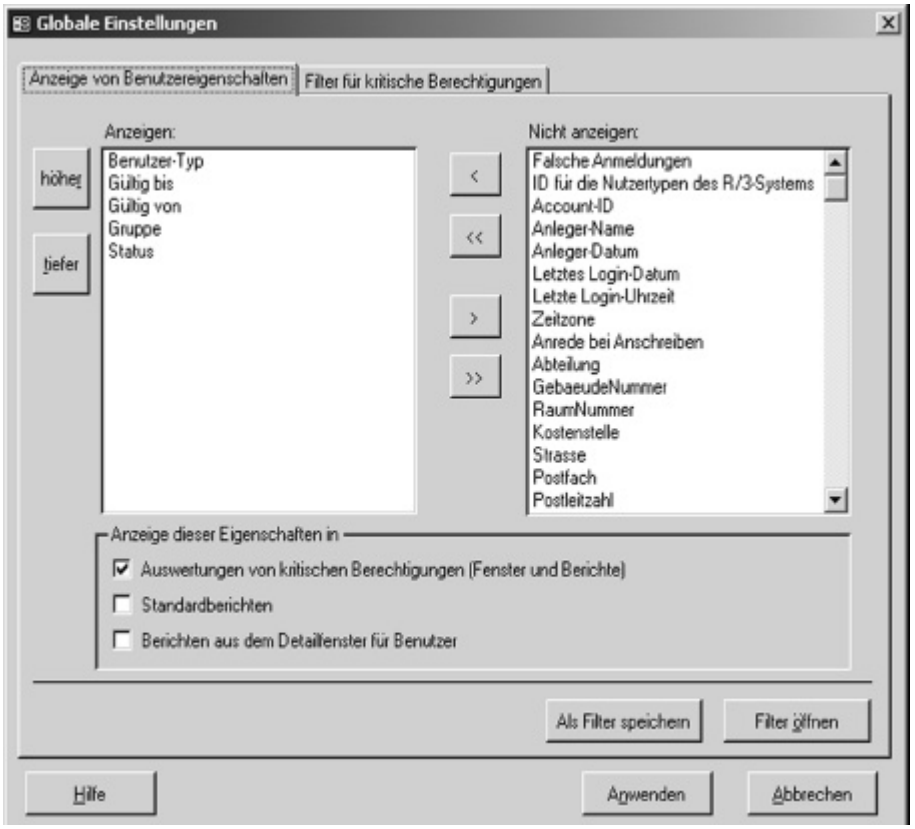

Bild 6: Der globale Filter zur Auswahl der anzuzeigenden Benutzereigenschaften

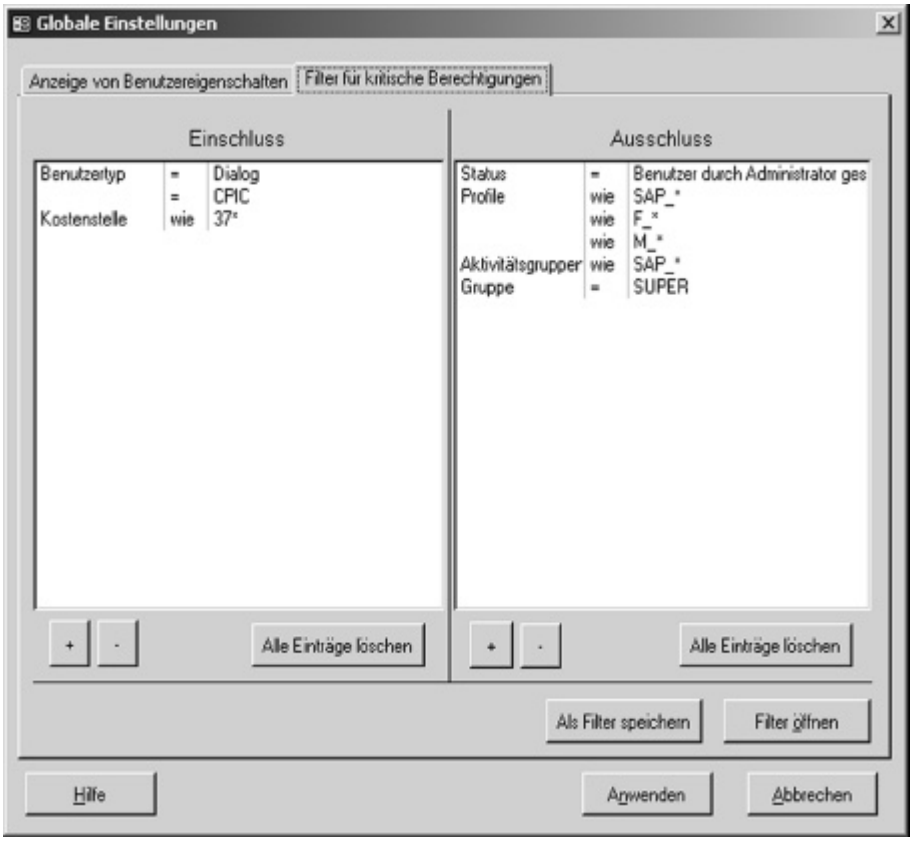

Bild 7: Der globale Filter zur Auswahl der auszuwertenden Benutzer

Benutzernamen angezeigt werden, sondern wenn selektiert werden kann, welche Benutzereigenschaften zusätzlich angezeigt werden sollen, z. B. ob es sich um Dialog-Benutzer handelt, ob der Benutzer gesperrt ist oder seine Kostenstelle. In SAPaudit kann über den globalen Filter eingestellt werden, welche Benutzereigenschaften grundsätzlich mit angezeigt werden sollen. Hier können aus allen Eigenschaften so viele zum Anzeigen ausgewählt werden, wie benötigt. (Bild 6)

Unerlässlich für komplexe Prüfungen ist die Möglichkeit, auszuwählen, welche Benutzer bei der Auswertung der kritischen Berechtigungen beachtet werden sollen und welche nicht. Z. B. reicht es aus, am Anfang der Prüfung festzustellen, welche Benutzer das Profil SAP_ALL besitzen. Diese brauchen bei der Auswertung der einzelnen Berechtigungen nicht mehr beachtet zu werden, da sie sowieso alle Rechte besitzen und das zu beurteilende Ergebnis nur unnötig aufblähen. Ebenso ist es hilfreich, die Batch- und Hintergrund-Benutzer auszublenden und die Auswertung auf die Dialog- und CPIC-Benutzer zu beschränken. Oder man möchte die Prüfung gezielt auf bestimmte Benutzergruppen oder Kostenstellen einschränken. Es kann auch vorkommen, dass nur aktive Benutzer ausgewertet werden sollen, die gesperrten nicht. Die Möglichkeiten sind vielfältig. Auch diese Möglichkeiten können uneinge-

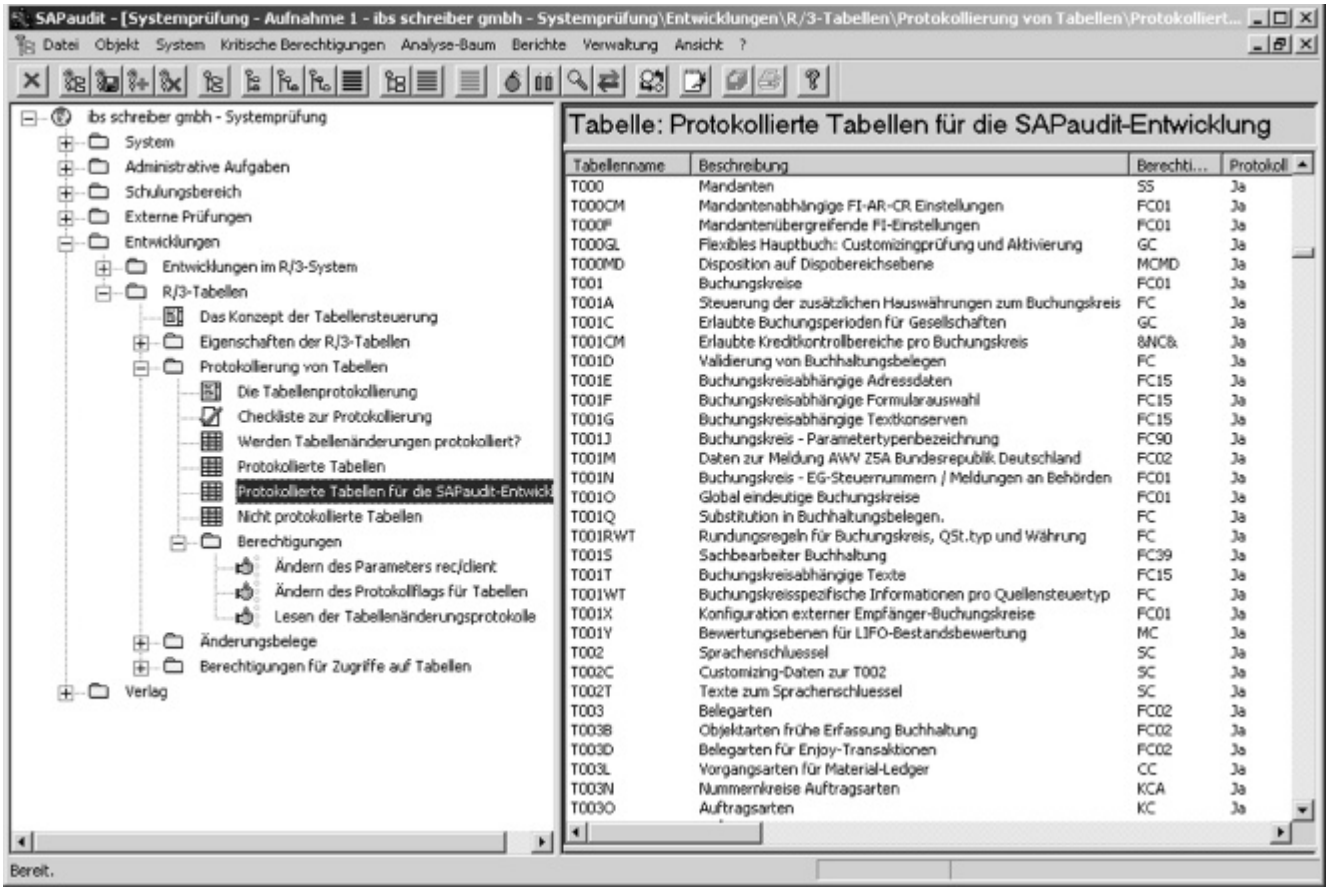

Bild 8: Unternehmensbezogen angepasster Analysebaum

schränkt über den globalen Filter in SAPaudit abgebildet werden. (Bild 7)

Unternehmensbezogene Anpassung des Analysebaumes

Mit SAPaudit wird der Analysebaum im Originalzustand ausgeliefert. Zur Nutzung für Prüfungen ist es meist sinnvoll, den Analysebaum unternehmens- oder prüfungsbezogen anzupassen. Der originale Analysebaum kann beliebig oft kopiert werden. Diese Kopien können an die eigenen Bedürfnisse angepasst werden. Es können vollständig neue Strukturen erstellt werden. So kann z. B. für jede Prüfung ein Baum erstellt werden: für Systemprüfungen, FI-Prüfungen, HR-Prüfungen oder auch Prüfungen aus Datenschutzsicht. Ebenso kann mit dieser Möglichkeit ein Auditing implementiert werden, indem ein Baum für das Tages-Audit, einer für das Wochen-Audit und einer für das Monats-Audit erstellt wird.

In diese Bäume kann alles implementiert werden, was SAPaudit bietet, z. B. Tabellen mit beliebigen Filterungen, die eigenen Checklisten, Dokumente für Prüfungsvorgehensweisen oder die kritischen Berechtigungen. Natürlich können beliebige eigene kritische Berechtigungen definiert werden, welche dann in den Analysebaum zur automatischen Auswertung integriert werden können.

Hierdurch kann SAPaudit vollständig an die Bedürfnisse jeder Unternehmung angepasst werden. (Bild 8)

Zeitersparnis und Qualitätssteigerung

SAPaudit wurde mit der Zielsetzung entwickelt, das Berechtigungskonzept von R/3, die Systemsicherheit und das Customizing transparent abzubilden und auf einfache und komfortable Weise prüfbar zu machen. Gleichzeitig soll der Prüfungsaufwand erheblich reduziert werden, so dass vollständige Prüfungen überhaupt erst möglich werden, und zwar in sehr kurzer Zeit. Durch die Gesamtkonzeption von SAPaudit und die Automatisierungsmechanismen ergeben sich dadurch u. a. folgende Faktoren zur Zeitersparnis, Steigerung der Prüfungsqualität und Steigerung der Systemsicherheit:

Benutzer	Module	Tage manuelle Prüfung (Minimum)	Tage Prüfung mit SAPaudit (mit erheblich höherer Qualität)
100	BC, FI, CO	5	0,5
500	BC, FI, CO, MM	15	1
1000	BC, FI, CO, MM, SD, HR	25	1,5
5000	BC, FI, CO, MM, SD, HR	40	2

Tabelle 1

1. Durch die Automatisierungsmöglichkeiten können Prüfungen der R/3-Systeme häufiger durchgeführt werden, da hier ein sehr viel geringerer Zeitaufwand notwendig ist.
2. Durch die Auditing-Funktionalität kann eine ständige Sicherheitsüberprüfung implementiert werden (z. B. Tages-, Wochen- und Monats-Auditings).
3. Es können sicherheitsrelevante Prüfungen durchgeführt werden, die mit R/3 selber gar nicht oder nur mit erheblichem Aufwand möglich sind.
4. Generell bringt eine Prüfung mit SAPaudit eine große Zeitersparnis mit sich. Um alle sicherheits- und prüfungsrelevanten Informationen zusammenzutragen (Berechtigungen, Parametrisierungen, Customizing-Einstellungen, relevante Tabelleninhalte, ...), werden, je nach Systemgröße, unterschiedliche Zeiträume benötigt. Allein zur manuellen Prüfung der Zugriffsberechtigungen muss Hintergrundwissen für jeden einzelnen Vorgang vorhanden sein, dann müssen zuständige Berechtigungsobjekte ermittelt werden (für die meisten Vorgänge sind mehr als drei Objekte zuständig, es gibt auch optionale), mit welchen dann umständlich über Reports die Berechtigten ermittelt werden können, ohne die Herkunft der Rechte zu kennen. Zur Prüfung der Customizing-Einstellungen muss die entsprechende Tabelle mit den Einträgen bekannt sein, ansonsten muss jede einzelne gesucht werden (es gibt ca. 22.000 Tabellen im Release 4.6x).

Daher ergibt sich aus der Nutzung von SAPaudit für das Zusammentragen der notwendigen Prüfungsinformationen ein erheblicher Zeitvorteil, der für verschiedene Größen von R/3-Systemen (abhängig von der Benutzerzahl und der eingesetzten Module) ca. folgende Zeitersparnis bringt (unter der Voraussetzung, dass der Prüfer über gute R/3-Kenntnisse in den jeweiligen Modulen verfügt): siehe Tabelle 1.

Anmerkung

Auch wenn diese Tabelle 1 unglaubwürdig erscheinen mag: Es handelt sich hier um die Zeitersparnis für das Zusammentragen der benötigten Informationen (wer hat welche Rechte; welche Vorgänge dürfen von welchen Benutzern durchgeführt werden und woher kommen diese Rechte; werden Vier-Augen-Prinzipien eingehalten; welche Customizing-Einstellungen wurden getroffen; ...). Die inhaltliche Deutung der Informationen kann von SAPaudit in der Form erfolgen, dass z. B. für Parameter Vorgaben hinterlegt werden können, welche dann automatisiert überprüft werden oder dass berechtigte/unberechtigte Benutzer für Vorgänge vorgegeben werden, welche dann bei der Rechteüberprüfung beachtet werden. Natürlich müssen diese Daten weiter ausgewertet und bewertet werden.

Und auch für diese Vorgänge ergibt sich wieder eine erhebliche Zeitersparnis durch SAPaudit, da vielfach bereits vorgefertigte Prüfberichte „auf Knopfdruck“ erstellt werden und auch alle (!) anderen Informationen jederzeit in Berichtsform ausgegeben werden können.

<

AUDITmaster: Die moderne Systemlösung für Revisionen

Von Dipl.-Wirtsch.-Ing. (FH) Jutta Faasen,
Deutsche Telekom AG, Bonn

Die Globalisierung der Wirtschaft stellt auch die Interne Revision vor enorme Herausforderungen. Erhöhter Wettbewerbsdruck, schnellere Innovationszyklen und zunehmender Kostendruck zwingen die Unternehmen zur Steigerung ihrer Leistungskraft und Effizienz. Hier hat auch die Revision aktiv wertschaffende Funktionen zu übernehmen. Die klassische Rolle der Internen Revision ist im 21. Jahrhundert nicht mehr zeitgemäß. Die Interne Revision muss ihr Insiderwissen und ihre tiefen Einblicke in das Geschäftsmodell des Unternehmens aktiv im Sinne einer wirksamen Risikoprophylaxe in die Unternehmensführung einbringen. Dazu wird auch die Revision die Effizienz ihrer Arbeit steigern müssen. Der konsequente Einsatz moderner Softwarelösungen wie AUDITmaster ist dabei eine große Hilfe.

Die Konzernrevision der Deutschen Telekom AG

Die zur Zeit 140 Mitarbeiter der Konzernrevision haben im Jahr 2000 ca. 300 Prüfungen im In- und Ausland für die Deutsche Telekom, ihre Tochtergesellschaften und Mehrheitsbeteiligungen durchgeführt. Hinzu kommen zahlreiche Sonderaufträge, Vorstandsanfragen und Joint Audits mit Revisionen von Minderheitsbeteiligungen. Insgesamt werden ausgehend von sechs Pool-Standorten in Deutschland und einem Pool in England ca. 8.000 Organisationseinheiten des Telekom-Konzerns betreut.

Ohne ein effizientes und auf die speziellen Anforderungen der Revision ausgerichtetes IV-System ist dieses Aufgabenspektrum nicht zu bewältigen. In Kooperation mit der Revision der Deutschen Bahn AG hat die Konzernrevision der Deutschen Telekom mit AUDITmaster ein solches IV-System konzipiert und eingeführt. Die Entwicklung dieser Systemlösung wurde von der Multimedia Software GmbH Dresden geleistet, dem Multimedia Systemhaus der Deutschen Telekom.

Erfahrungen bei der Programmeinführung

Die intensive und konsequente Nutzung eines IV-gestützten Computerprogramms für die Revision erfordert eine gewisse Eingewöhnung und ein hohes Maß an Disziplin. So sehr jeder Anwender gerne Informationen und Daten aus solchen Systemen ziehen möchte, sowenig enthusiastisch werden die entsprechenden Daten kontinuierlich eingepflegt. Auch die Konzernrevision der Deutschen Telekom hat in dieser Hinsicht langwierige und schwierige Gewöhnungsprozesse durchlaufen müssen. Insbesondere der zunehmende Zeit- und Erfolgsdruck bei der Durchführung von Prüfungen lässt die Dateneingabe für den Prüfungsleiter manchmal zur lästigen Pflicht werden. Kritisch wird eine solche Haltung immer in den Programmplanungsphasen oder wenn kurzfristig Informationen bereichsübergreifend zu verdichten bzw. aus „fremden“ Themenkreisen aufzubereiten sind. Da werden mögliche Lücken bei der Dateneingabe schnell zum Problem.

Das Problem: kontinuierliche Datenpflege, komplexe Prozesse, uneinheitliche Software

So gilt auch für revisionsspezifische IV-Systeme der Satz „ohne Fleiß kein Preis“. Der Spruch mag reichlich abgegriffen erscheinen, aber ohne konsistente Basisdaten gibt es auch keine fundierten und verwertbaren Auswertungen. Ein Faktum, das für jede Revision gilt, nicht nur für die Konzernrevision der Deutschen Telekom.

Eine Reihe von Prüfungsleitern und Revisionsabteilungen haben auf Basis gängiger Tabellenkalkulations- und Textverarbeitungsprogramme Teilaspekte des Revisionsprozesses abgebildet. Die

Probleme sind bekannt: Medienbrüche samt den daraus resultierenden Doppeleingaben, unzureichende Auswertungsmöglichkeiten, hoher Programmieraufwand für die eigenentwickelte Lösung, sehr unterschiedlicher Qualitätsstandard.

Die komplexen Prozesse bei der Planung und Durchführung von effizienten Revisionen können auf Dauer nicht durch Software abgedeckt werden, die immer nur Teilfunktionen unterstützt. Dies war und ist das Manko zahlreicher spezieller Revisions-Software, die es auf dem Markt gibt. Da kann nur ein modernes und komplexes Revisionstool wie AUDITmaster gewährleisten, dass keine Arbeit doppelt gemacht wird.

Deutsche Telekom und Deutsche Bahn setzen auf AUDITmaster

Vor drei Jahren haben wir erkannt, dass die vorhandene, über einen langen Zeitraum durchaus erfolgreich eingesetzte, Revisionssoftware den gestiegenen und sich erweiternden Anforderungen zunehmend nicht mehr gerecht wurde. Die Konzernrevision der Deutschen Telekom hat sich daher entschlossen, ihre Software auf eine neues Betriebssystem umzustellen und die Benutzeroberflächen den veränderten Rahmenbedingungen anzupassen. Gemeinsam mit der Revision der Deutschen Bahn wurde AUDITmaster in einer Client/Server-Architektur für die Plattformen MS Windows und Lotus Notes entwickelt. Die Entwicklungsarbeit für die MS Windows Lösung wurde von der Multimedia Software GmbH Dresden realisiert.

Akzeptanzsteigerung durch MS Windows-Oberfläche

Die Revision der Deutschen Telekom arbeitet mit der MS Windows Version. Die folgenden Ausführungen beziehen sich daher auf die MS Windows-Plattform des AUDITmaster. Wir haben uns für diese Plattform entschieden, weil sie aus unserer Sicht einige erhebliche Vorteile bietet:

- Die Revisionssoftware fügt sich problemlos in die komplexe IV-Landschaft der Deutschen Telekom ein. Direkte Datenübernahmen aus anderen IV-Anwendungen unter Nutzung automatischer Schnittstellen sind möglich.
- Der Kennwort-geschützte Zugriff ist sowohl über den direkten Netzzugang am festen Arbeitsplatz als auch per IT-Remote-Zugang über Laptops möglich.
- Die Mitarbeiter können wesentlich leichter in die Revisionssoftware eingearbeitet werden.
- Die am Windows-Standard orientierte Menüstruktur steigert zudem die Akzeptanz der Software, da die meisten Mitarbeiter den Umgang mit Windows gewöhnt sind und sich jeder Anwender diese Menüoberfläche an die spezifischen Anforderungen seiner Arbeit anpassen kann. (Bild 1)

Ein Tool für den gesamten Revisionsprozess

AUDITmaster begleitet den gesamten Revisionsprozess: über die Prozessschritte Planung, Disposition, Revisionsdurchführung, Archivierung bis hin zum Follow up - der Revisor findet in der funk-

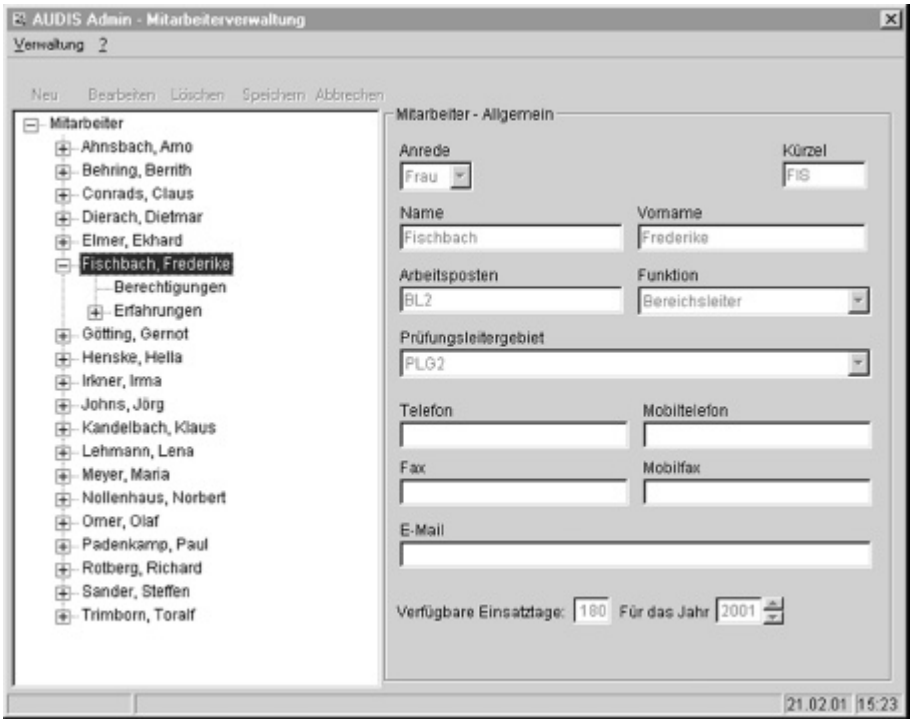

Bild 1: AUDIS Admin - Mitarbeiterverwaltung.

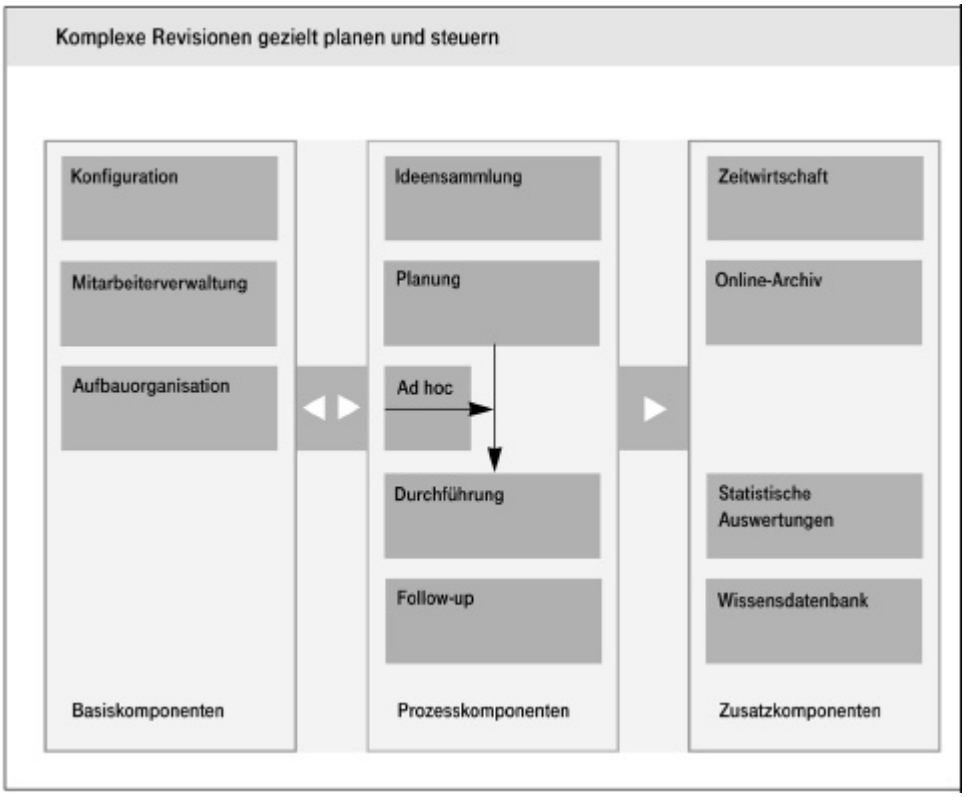

Bild 2: Komplexe Revisionen gezielt planen und steuern

tionellen Software in jeder Arbeitsphase effiziente Unterstützung. (Bild 2)

Planung und Risikoabschätzung

Moderne Revisionsarbeit erfolgt in einer sich dynamisch verändernden Umgebung und vor dem Hintergrund einer Vielzahl von Erkenntnissen, die aus Gesprächen, aktuellen Prüfungsergebnissen sowie neuen Anforderungen resultieren und die - zunächst einmal unstrukturiert und wertfrei - als „Prüfungsidee“ in den Prüfungsprozess einbezogen werden sollten. Jede erkannte

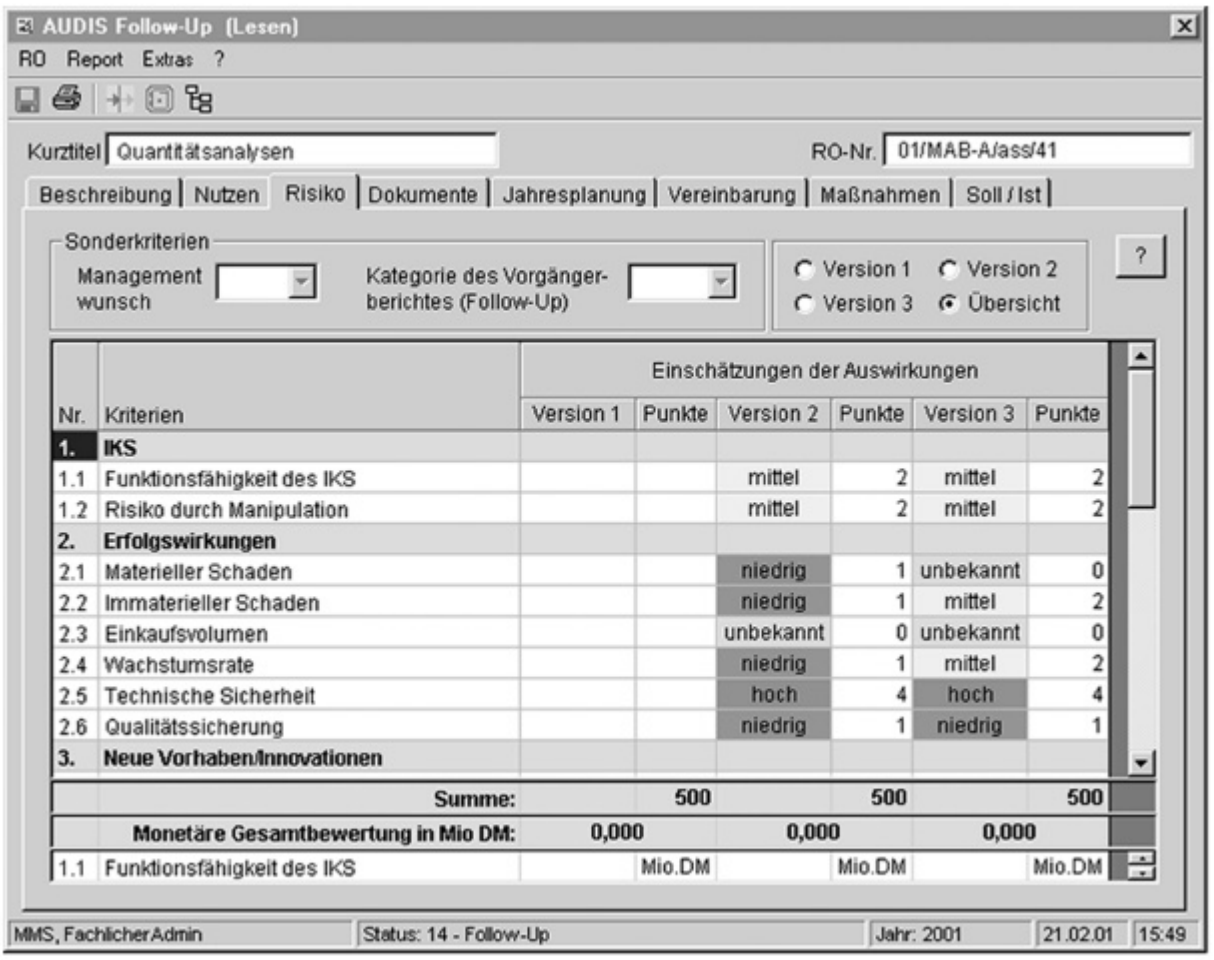

Bild 3: AUDIS Follow-Up (lesen) - Risikobewertung

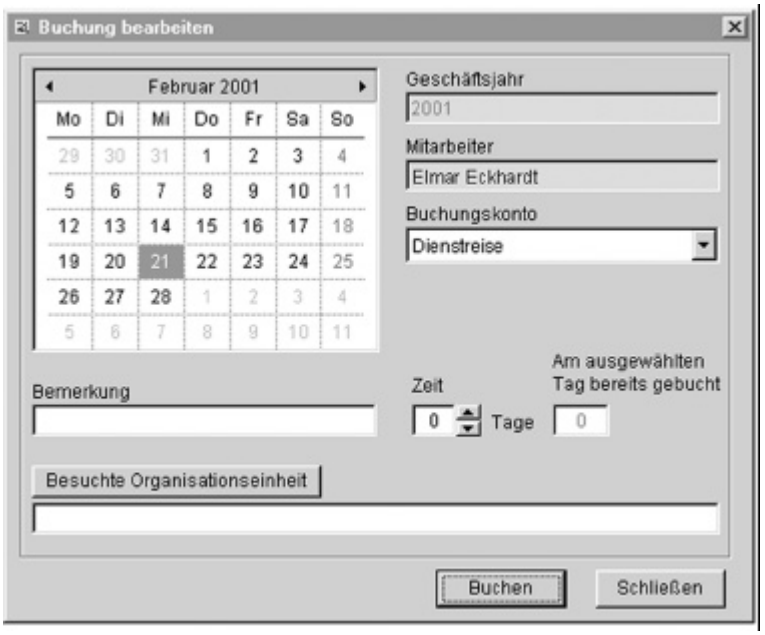

Bild 4: AUDIS Buchung bearbeiten - Zeitwirtschaft

Schwachstelle kann durch AUDITmaster über die Erfassung als Prüfungsidee für eine spätere Bewertung dokumentiert und gesichert werden.

Der Prozessschritt *Planung* beginnt mit der Erfassung dieser Schwachstellen in der Ideensammlung. Schwachstellen können von jedem Mitarbeiter der Revision ins System eingestellt werden und sind für alle zugänglich. Der nächste Schritt ist die Risikobewertung. Sie ermöglicht ein effizientes Risikomanagement von Beginn an. Die Risikobewertung wird im weiteren „Lebenszyklus“ eines Revisionsobjektes noch zwei Mal hinterfragt und gegebenenfalls angepasst. Ein funktionsfähiges, qualitativ gutes, internes Risikomanagement setzt die Erfassung und strukturierte Bewertung der potenziellen Risiken voraus, nur so sind die wesentlichen Risiken für ein Unternehmen identifizierbar. (Bild 3)

An diesen wesentlichen Unternehmensrisiken soll und muss die Revision ihre Arbeit ausrichten. Die Risikoanalyse aus Revisionssicht ist immer unternehmensspezifisch und muss daher mit teilweise sehr unterschiedlichen Prämissen erfolgen. AUDITmaster bietet ein individuell strukturierbares Risiko-Modell. So kann auf Basis eines individuell auf die Belange des Unternehmens ausgerichtetes Punktewertsystem eine transparente Risikoabschätzung vorgenommen werden.

Die Risikobewertung, die Abschätzung des Aufwands für die Durchführung einer Prüfung sowie die Zusammenstellung und Bewertung der Ideen für die Programmplanung erfolgen durch den zuständigen Prüfungsleiter. Er bereitet auch die Umwandlung der Idee in ein Revisionsobjekt für die Programmplanung vor.

Nach umfangreichen Abstimmungsprozessen innerhalb und außerhalb der Revision werden bei der Deutschen Telekom AG zur Zeit ca. 50-60% der Gesamtkapazität eines Prüfungsjahres jeweils zum Jahresbeginn den zu prüfenden Bereichen als Jahresrevisionsprogramm (JRP) bekannt gegeben. Die Veröffentlichung des JRPs mit der gezielten Information der zu prüfenden Bereiche über „ihren“ Teil am JRP wäre ohne die Nutzung von AUDITmaster in einem weltweit tätigen Konzern wie der Deutschen Telekom gar nicht mehr möglich.

Disposition

Die Disposition der verfügbaren Ressourcen, insbesondere der Einsatz der auch in der Zusammensetzung wechselnden Teams im In- und Ausland erfolgt ebenfalls mit Hilfe von AUDITmaster. Hier gibt es enge Verbindungen zur Komponente *Zeitwirtschaft.* Alle an einer Prüfung beteiligten Mitarbeiter der Konzernrevision verbuchen wöchentlich ihre tatsächlichen Einsatzzeiten je Revisionsobjekt. Ein stetiger Abgleich zwischen ursprünglicher Disposition und IST-Ressourcen-Einsatz je Revisionsobjekt ist jederzeit möglich. Darüber hinaus können die kumulierten Werte für jedes Prüfungsteam bzw. jede Organisationseinheit der Revision abgerufen werden. (Bild 4)

Revisionsdurchführung und Archiv

Die Prüfungsdurchführung wird detailliert und lückenlos im System abgebildet. Beginnend mit den ersten Voruntersuchungen, der Prüfungsankündigung und dem Eröffnungsgespräch, setzt sich dies fort mit dem Prozess der Erhebungen vor Ort und dem Berichtsentwurf bis hin zur Berichtsveröffentlichung und Dokumentation der Berichtsverteilung. All diese

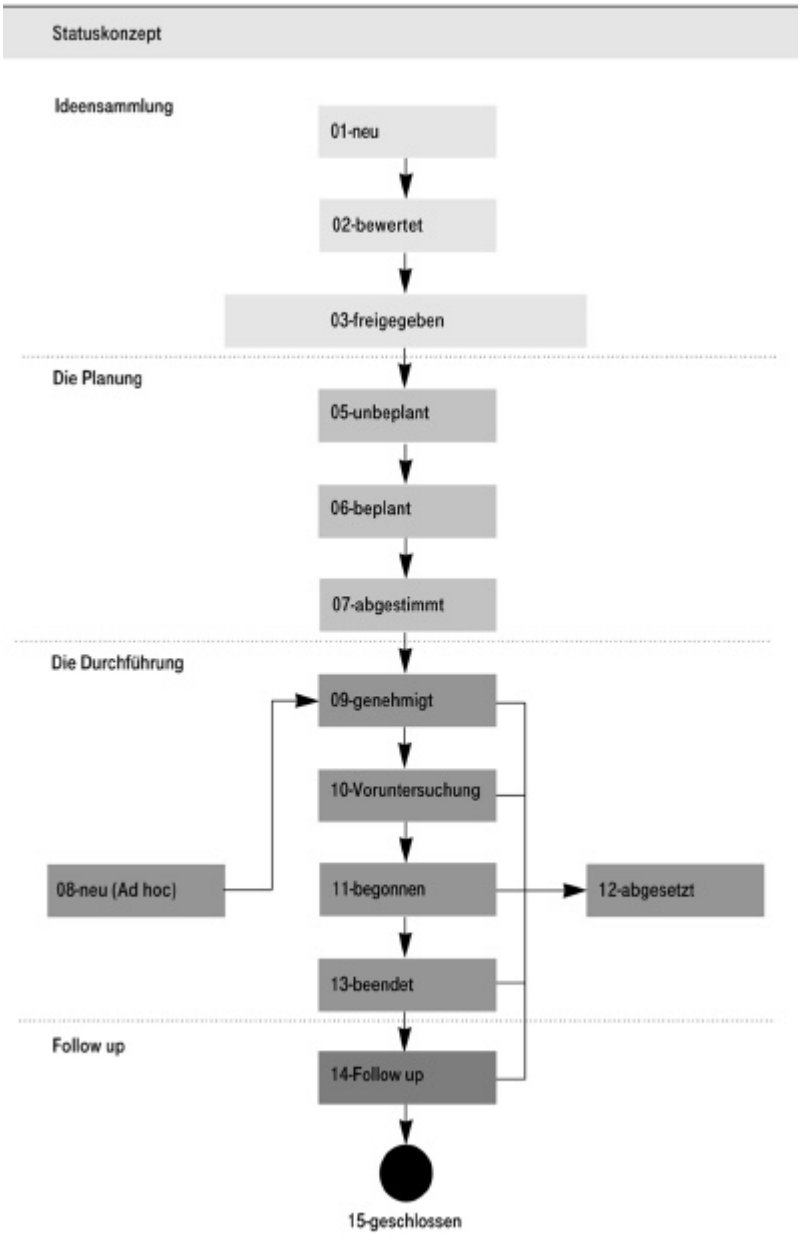

Bild 5: Follow-Up - Statuskonzept

Schritte sind über Termine und weitere Zwangseingaben im System zu dokumentieren. AUDITmaster dient gleichzeitig als Dokumentenablage und Archiv für Schriftwechsel und die veröffentlichten Berichte. Dieses Archiv ist allen Mitarbeitern der Konzernrevision jederzeit zugänglich.

Follow up

Durch die detaillierte Eingabe aller vereinbarten Maßnahmen mit den zugehörigen Terminen wird im Prozessschritt *Follow up* die Überwachung der Maßnahmenumsetzung durch die Fachseiten nachhaltig unterstützt. (Bild 5)

Fazit

Die Komplexität der Revisionsprozesse führt zu einer Flut von Daten, die sich nur mit großer Sorgfalt und großem Fleiß bewältigen lässt. Bei kontinuierlicher Arbeit mit AUDITmaster und konsequenter Datenpflege lassen sich für die Revision sehr gute Ergebnisse erzielen.

Sind während der Bearbeitung eines Revisionsobjektes sämtliche Daten konsequent und vollständig eingepflegt worden, können alle statistischen Auswertungen, wie notwendige Datenverdichtungen für den Konzernvorstand, das Controlling von Revisions-Standards oder die Performance der Konzernrevision jederzeit direkt aus dem System generiert werden.

Und hier schließt sich der Kreis. Denn ohne diese oftmals lästige Eingabe fundierter Informationen und Daten ist es selbstverständlich nicht möglich, qualitativ hochwertige statistische Auswertungen zu fahren.

Wir haben die Erfahrung gemacht, dass es sich lohnt, diesen Fleiß in ein innovatives Tool wie AUDITmaster zu investieren, statt sich mit zahllosen selbstgestrickten und nicht kompatiblen Hilfsprogrammen irgendwie „über Wasser zu halten“. Zudem hat die Daten-Sicherheit mit AUDITmaster einen regelrechten Quantensprung gemacht. Hier sind neben den bereits beschriebenen Kennwort-geschützten Zugriffsmöglichkeiten auch die Belange des personenbezogenen Datenschutzes zu nennen.

Nach Bewältigung der anfänglichen Umstellungs- und Akzeptanzprobleme zeigen sich nun zunehmend die erheblichen Vorteile und Arbeitserleichterungen durch AUDITmaster, so dass sich guten Gewissens sagen lässt: „AUDITmaster ist seinen Preis wert.“

<

DAS QUIZ

Wer wird „Revisions-Millionär“?

Sind Sie ein *guter* Revisor?

Haben sie es gewusst?
Die Hauptgewinner unseres Quiz werden in der nächsten Ausgabe ReVision IV/01 bekanntgegeben. Und hier sind die richtigen Antworten unseres Spieles.

Wir hoffen, Sie hatten viel Spaß!

1. Ein guter Revisor ist
- ❑ Trinkfest
- ❑ Sattelfest
- ☒ Objektiv
- ❑ Blauäugig

2. Früher wurden Revisoren gerne scherzhaft genannt
- ❑ Topfgucker
- ☒ Erbsenzähler
- ❑ Nachtwächter
- ❑ Oberlehrer

3. Interne Revision und Controlling unterscheiden sich durch
- ❑ Gar nichts
- ❑ Soll-/lstvergleich
- ❑ Zahlenakrobatik
- ☒ Planung/Steuerung

4. Was bedeutet der Begriff „Ex ante Prüfung“?
- ❑ Umsatzprüfung
- ☒ Projektbegleitend
- ❑ Kostenanalyse
- ❑ Bestandskontrolle

5. Revisoren gelten gemeinhin als
- ❑ Optimisten
- ❑ Pessimisten
- ☒ Generalisten
- ❑ Fetischisten

6. Eine moderne Revisionsabteilung nutzt ihren Prüfbericht als
- ❑ Racheakt
- ❑ Karrierechance
- ❑ Anklageschrift
- ☒ Ihre Visitenkarte

7. Womit wird eine zusätzliche Stimulanz beim Lesen des Revisionsberichtes erreicht?
- ☒ Graphiken
- ❑ Polemik
- ❑ Spektakuläres
- ❑ Hochrechnungen

8. Welcher Begriff gehört nicht zur Revisionsarbeit?
- ❑ Internal Auditor
- ❑ Systemprüfung
- ❑ Stichproben
- ☒ Ermittlung

9. Eine Revision ist im Unternehmen eine Stabsstelle und damit nicht
- ❑ Glaubwürdig
- ☒ Weisungsberechtigt
- ❑ Zielorientiert
- ❑ Selbstbewusst

10. Was wird ein geschulter Revisor in der Schlussbesprechung einsetzen?
- ❑ Informatik
- ❑ Mantik
- ☒ Rhetorik
- ❑ Ballistik

11. Welchen historischen Ursprung hat der Haken des Prüfers?
- ☒ Veritas
- ❑ Daumenabdruck
- ❑ Markenzeichen
- ❑ keinen

12. Die Umsetzung von Empfehlungen gelingt am Besten durch das Aufzeigen von
- ☒ Konsequenzen
- ❑ Finanzmitteln
- ❑ Vielen Fehlern
- ❑ Drohungen

13. Jemanden, der eine Unterschlagung begangen hat, nennt man einen
- ❑ Glückspilz
- ☒ Defraudant
- ❑ Zocker
- ❑ Delinquent

14. Wie nennt man die „Nachschau“ der Empfehlungen?
- ❑ Blow Up
- ❑ Shut Up
- ☒ Follow Up
- ❑ Follow Me

15. Wie heißt das 1998 erlassene und für die Revision wichtige Gesetz?
- ❑ WiPG
- ☒ KonTraG
- ❑ WeTaG
- ❑ PrüfG

Buchhinweise

IIR-Schriftenreihe Deutsches Institut für Interne Revision e.V. - Berlin

Sicherheit in Kreditinstituten

Handbuch der Arbeits- und Betriebssicherheit

Erich Schmidt Verlag 220 Seiten
ISBN 3-503-05939-3 DM 98,- / € 49,80

Sicherheit ist für Kreditinstitute ein zentrales Anliegen. Zum Schutz von Personen, Einrichtungen, Werten und Wissen ist eine gezielte und umfangreiche Prävention erforderlich. Für die interne Revision erschließt sich damit ein komplexes Prüfungsgebiet. Neben betriebsindividuellen Belangen und technischen Innovationen nimmt auch der Gesetzgeber großen Einfluss auf Regelungen der Arbeits- und Betriebssicherheit. Das Gebiet der Sicherheit in Kreditinstituten ist damit ein höchst dynamisches Arbeitsfeld. Regelungen zur Arbeits- und Betriebssicherheit liegen in der Verantwortung der Unternehmensleitung und bedürfen einer ständigen Beachtung.

Das Handbuch der Arbeits-, und Betriebssicherheit liefert für die Interne Revision, die Unternehmensleitung, Beauftragte zum Arbeitsschutz und zu Unfallverhütung sowie andere Interessenten eine umfassende Betrachtung zum gesamten Komplex der Sicherheit in Kreditinstituten.

<

Konstantin von Schönborn

Die Bankhaftung bei der Überweisung im Internet

Erich Schmidt Verlag 199 Seiten
ISBN 3-503-05945-8 DM 68,- / € 34,80

Internetbanking erfreut sich einer immer größeren Beliebtheit. Die Schnellebigkeit des Internets, die Immaterialität der Finanzprozesse und die teilweise Anonymität der an diesem Prozess Beteiligten wirft aber auch eine Vielzahl von rechtlichen Fragen auf, die bis dato nur unzureichend in der aktuellen Rechtsprechung Eingang gefunden haben.

Das Buch stellt die Probleme der Risikoverteilung und Haftung beim Internetbanking vertiefend dar und fächert diese Thematik in vier Konstellationen auf: Missbrauchfälle durch technische Manipulationen oder durch Unachtsamkeit des Kunden, Fehlfunktionen der Bankhard- und -software und technisch bedingte Störungen des Internetsystems. In diesem Zusammenhang wird die rechtliche Situation in Bezug auf das Missbrauchsrisiko vor dem Hintergrund der einschlägigen Rechtsprechung und Lehre umfassend erläutert.

Daneben wird auf die Vertragsbeziehungen, die zwischen Kreditinstitut und Kunden bestehen, eingegangen und das neue Überweisungsgesetz sowie die unterschiedlichen Authentifizierungssysteme (z. B. Pin/Tan, Chipkarte, MeChip) umfassend dargestellt. Das Werk geht auch der Frage nach, inwieweit vorhandene materiell-rechtliche Ansprüche in der Praxis durchsetzbar sind. Fragen des Urkundenbeweises und des Schriftformerfordernisses bekommen hierbei eine veränderte Bedeutung.

Schaubilder und ein Ausblick auf das von den Banken zur Sicherheit der Kunden favorisierte HBCI Verfahren runden das wissenschaftliche Werk mit Praxisbezug ab.

<

Raimund Weyand

Insolvenzdelikte

Unternehmenszusammenbruch und Strafrecht

Erich Schmidt Verlag 220 Seiten
ISBN 3-503-05789-7 DM 59,80 / € 29,80

Die Zahl der Unternehmenszusammenbrüche steigt seit Jahren stetig an. Im Umfeld zahlreicher Insolvenzen kommt es zu Straftaten, die umfangreiche und meist zeitaufwendige Ermittlungsverfahren nach sich ziehen.

Welche Ursachen führen zu Insolvenzen?

Welche Personenkreise kommen als Täter in Betracht?

Wie werden die Krisenmerkmale der Überschuldung und der Zahlungsunfähigkeit definiert und wie lassen sie sich im Rahmen eines Strafverfahrens überprüfen?

Welche Tathandlungen sind im Einzelnen strafbar?

Wie sieht die Praxis der Ermittlungsbehörden im Bereich der Insolvenzdelikte aus?

Mit welchen Konsequenzen hat der überführte Täter zu rechnen?

Wie können sich Insolvenzverwalter und Rechts- bzw. Steuerberater insolventer Unternehmen strafbar machen?

Auf sämtlicher Fragen gibt dieses Buch unter Berücksichtigung der neuesten Tendenzen in Literatur und Rechtsprechung umfassende praxisorientierte Antworten. Zahlreiche Übersichten und Schaubilder erschließen die relevanten Problemfelder. Der Verfasser, seit vielen Jahren als Staatsanwalt für Wirtschaftsdelikte tätig, beschäftigt sich außerdem ausführlich mit den Konsequenzen der zum 1.1.1999 in Kraft getretenen Reform des Insolvenzrechtes für den Bereich der Strafverfolgung.

<

Jörn Voßbein

Integrierte Sicherheitskonzeptionen für Unternehmen

Stand und Perspektiven

SecuMedia Verlag 335 Seiten
ISBN 3-922746-48-8 DM 78,- / € 39,88

Sicherheit von Informationsverarbeitungssystemen ist das Kernthema moderner Informationsverarbeitung. Die Abhängigkeit der Institutionen von der Verfügbarkeit dieser Systeme steigt ständig durch Hinzunahme neuer Anwendungslösungen. Zunehmend mehr werden sensible Daten verarbeitet, womit die Ansprüche an die Vertraulichkeit der Daten wachsen. Außerdem fordern sowohl die Vertraulichkeit als auch die Abhängigkeit von den Systemen ein hohes Maß an Integrität der Daten und Programme.

Das Buch legt dar, wie es durch ein entsprechendes, konzeptionelles Vorgehen möglich ist, das technisch unterstützte Informationsverarbeitungssystem so abzusichern, dass mit einem vertretbaren Aufwand ein großer Teil der Ursachen für Sicherheitsprobleme von IV-Systemen beherrschbar wird.

Jörn Voßbein ist Geschäftsführer der UIMC Dr. Vossbein GmbH & Co KG und leitet zahlreiche Beratungsprojekte im unternehmensorganisatorischen und IV-Sicherheits-Bereich (Banken, Industrieunternehmen, Versicherungen, Sonstige Unternehmen). Er ist hier insbesondere zuständig für die Beratung von Unternehmen mit IV-gestützen, standardisierten Tools. Er promovierte an der Universität zu Köln über Sicherheitskonzeptionen für Informationssysteme.

<

Volkmar Botta

Kennzahlensysteme als Führungsinstrumente

Planung, Steuerung und Kontrolle der Rentabilität im Unternehmen

Erich Schmidt Verlag 288 Seiten
ISBN 3--503-04033-1 DM 68,- / € 34,80

Globalisierung, Zeitdruck und zahlreiche andere Einflussgrößen machen den Einsatz von Kennzahlen und Kennzahlensystemen als Führungs- und Controlling-Instrumente notwendiger denn je.

Gleichwohl herrscht teils erhebliche Unsicherheit bei Führungsnachwuchs- und Führungskräften bezüglich der Festlegung, der Generierung, der Interpretation von Kennzahlen und ihrer Verknüpfung zu Kennzahlensystemen.

Zur leichteren Behebung dieser Defizite wurden in die 5. Auflage ergänzend Unterschiede zu und Gemeinsamkeiten mit insbesondere dem *Tableau de Bord* und der *Pyramid Structure of Kaitos* sowie neuere Literatur eingearbeitet. Das Beispiel

zur tabellenkalkulationsprogrammgestützten Umsetzung des Du Pont-Systems wurde auf der Basis von MS-EXCEL 7.0 für die drei Spitzenkennzahlen überarbeitet und vereinfacht. Es lässt sich durch Einführung unterlegter Verknüpfungen leicht an differenzierte individuelle Bedürfnisse anpassen.

Diese 5. Auflage konzentriert sich deshalb auch weiterhin auf die Darstellung des Aufbaus und der Arbeitsweise des Du Pont-Systems als Führungsinstrument, die Analyse von Veränderungen der einbezogenen Kennzahlen und die Generierung der daraus ableitbaren Steuerungsimpulse.

Damit will das Buch den Leser bei der kritischen Beurteilung und Weiterentwicklung von Kennzahlen, der Konsistenzanalyse bestehender Kennzahlensysteme sowie bei der eigenständigen Konzeption konsistenter, kennzahlenorientierter Führungssysteme unterstützen.

<

Rainer W. Gerling

Verschlüsselung im betrieblichen Einsatz

Buch-Rezension

Datakontext-Fachverlag 212 Seiten
ISBN 3-89577-139-2 DM 79,- / € 40,39

Der Autor will mit seinem Buch vornehmlich Datenschutzbeauftragte, IT-Verantwortliche und IT-Revisoren ansprechen. Mathematisch-kryptologische Vorkenntnisse sind für das Verständnis des Buches nicht erforderlich.

Nach einem kurzen Ausflug in die Geschichte der Kryptographie werden die im Folgenden benötigten kryptographischen Grundbegriffe in einer knappen und leicht verständlichen Form erläutert.

Der Autor konzentriert sich auf konkrete Anwendungen. Er beschreibt unter anderem, wie eine innerbetriebliche Zertifizierungsstelle aufgebaut oder wie ein Verschlüsselungsprogramm in ein e-mail-System integriert werden kann.

Der Autor beschreibt gängige Formate, Normen und Protokolle und zeigt, wie verbreitete Verschlüsselungssoftware genutzt werden kann. Dabei gibt er mögliche Konfigurationsparameter explizit an, beschreibt Bildschirmmeldungen und Installationen akribisch genau, wobei er sogar auf fehlerhafte (Original-) Beschreibungen eingeht.

Eine beiligende CD erspart dem Anwender zudem die lästige Tipparbeit. Ausführungen zu rechtlichen Aspekten (Exportrestriktionen, Rechtmäßigkeit von Verschlüsselung, politische Rahmenbedingungen, Patentierung und Lizenzen) runden das Buch ab.

Lediglich die Bewertung der Sicherheitseigenschaften einiger kryptographischer Protokolle bzw. Produkte (z. B. PGP) erscheint zu euphorisch. Selbst wenn der Quellcode vorliegt, macht dessen Umfang eine gründliche Evaluierung meist praktisch unmöglich. Gerade bei PGP werden immer wieder (mehr oder minder kritische) Sicherheitslücken entdeckt.

Insgesamt kann dem Autor aber bescheinigt werden, dass er das gesteckte Ziel, der von ihm avisierten Zielgruppe einen brauchbaren Leitfaden in die Hand zu geben, zweifellos erreicht hat.

Rezension von
Privatdozent Dr. Werner Schindler, Sinzig

<

IBS **Prüfen mit**

K o n z e p t

SAP R/3 - Revisionsführerschein

Grundlagenseminar

Inhalte u.a.:

Grundlagen - Systemaufbau - Bedienung - Abfrage- und Berechtigungsmögichkeiten

- Einführung
- R/3 Benutzeroberfläche
- Transaktionscodes
- Individuelle Benutzereinstellungen
- Reports
- R/3-Online-Hilfe

Der Referent:

Marie-Luise Sander, *IBS*, Hamburg

Termin und Ort:

06.-07. September 2001,
Donnerstag 09:30-17:00 Uhr,
Freitag 09:00-ca. 15:30 Uhr
im *IBS*-Schulungscenter,
Hamburg, Friedrich-Ebert-Damm 145.

Teilnehmer:

Revisoren und externe Prüfer

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Susanne Albers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 - 15
schriftl.: IBS, Friedrich-Ebert-Damm 145,
22047 Hamburg

IBS **Prüfen mit**

K o n z e p t

Das SAP R/3-Berechtigungskonzept

Inhalte u.a.:

- Aufbau des Berechtigungskonzeptes
- Die Problematik des Berechtigungskonzeptes
- Konzepte zur Implementierung des Berechtigungskonzeptes
- Tipps und Tricks beim Umgang mit dem Berechtigungskonzept
- Der Profilgenerator

Der Referent:

Marie-Luise Sander, *IBS*, Hamburg,
Thomas Tiede, ibs schreiber gmbh, Hamburg

Termin und Ort:

13.-14. September 2001,
Donnerstag 09:30-17:00 Uhr,
Freitag 09:00-ca. 15:30 Uhr
im *IBS*-Schulungscenter,
Hamburg, Friedrich-Ebert-Damm 145.

Teilnehmer:

für IT-Revisoren, IT-Sicherheitsbeauftragte und Datenschutzbeauftragte

Anmeldung und Auskünfte:

Bitte melden Sie sich bei
Susanne Albers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 - 15
schriftl.: IBS, Friedrich-Ebert-Damm 145,
22047 Hamburg

IBS **Prüfen mit**

K o n z e p t

Systemprüfung in SAP R/3

Aufbauseminar des Revisionsführerscheins

Inhalte u.a.:

Zusammenspiel und Konsequenzen aus Richtlinien und systemeigenen Strukturen habe Auswirkungen auf die Art und Weise, wie Systemprüfungen vorbereitet und durchgeführt werden sollen.

- Die Anwendungsentwicklung
- Praktische Umsetzungen

Der Referent:

Thomas Tiede, ibs schreiber gmbh, Hamburg

Termin und Ort:

19.-21. September 2001,
Mittwoch 09:30-17:00 Uhr,
Donnerstag 09:00-17:30 Uhr,
Freitag 09:00-ca. 15:30 Uhr
im *IBS*-Schulungscenter,
Hamburg, Friedrich-Ebert-Damm 145.

Teilnehmer:

Revisoren und Datenschutzbeauftragte

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Susanne Albers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 - 15
schriftl.: IBS, Friedrich-Ebert-Damm 145,
22047 Hamburg

IBS **Prüfen mit**

K o n z e p t

Projektrevision

Grundlagenseminar

Inhalte u.a.:

Zunehmende Anwendungen des PM vermitteln in der Praxis wachsende Risiken und Chanchen.

- Risiken und Chancen des Projektmanagements (PM)
- Grundlagenwissen des PM
- Fallbeispiele der PM-Revision
- Software und Dokumentation
- IR-Checkliste der Projektrevision
- PM udn Rolle der Revision

Der Referent:

Dipl.-Ing. Paul Rieckmann, Referatsleiter FHH

Termin und Ort:

06.-07. September 2001,
Donnerstag 09:30-17:00 Uhr,
Freitag 09:00-ca. 15:30 Uhr
im *IBS*-Schulungscenter,
Frankfurt/Main, Eschborner Landstr. 55.

Teilnehmer:

Revisoren und Betriebsverantwortliche

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Susanne Albers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 - 15
schriftl.: IBS, Friedrich-Ebert-Damm 145,
22047 Hamburg

IBS **Prüfen mit**

K o n z e p t

SAP R/3-Revisions-Workshop Rechnungswesen

Vertiefungsseminar

Inhalte u.a.:

Dieses Seminar hat das Ziel, die Teilnehmer sachgerecht auf eine Prüfung des SAP-Moduls FI vorzubereiten.

- Systemprüfung
- Aufbau, Funktionalität und Organisation
- Modul FI
- Auswertungsmöglichkeiten mit SAP-Mitteln

Der Referent:

Marie-Luise Sander, *IBS*, Hamburg

Termin und Ort:

10.-11. September 2001,
Montag 09:30-17:00 Uhr,
Dienstag 09:00-ca. 15:30 Uhr
im *IBS*-Schulungscenter,
Frankfurt/Main, Eschborner Landstr. 55.

Teilnehmer:

Revisoren und externe Prüfer

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Susanne Albers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 - 15
schriftl.: IBS, Friedrich-Ebert-Damm 145,
22047 Hamburg

IBS **Prüfen mit**

K o n z e p t

Einführung in die Interne Revision

Grundlagenseminar

Inhalte u.a.:

- Einführung
- Grundsätze der Internen Revision (IR)
- Prüfungsdurchführungen
- Risikomanagement-Systeme (RMS) und Revision
- Organisation und Verwaltung der Revision

Der Referent:

Dipl.-Ing. Ottokar R. Schreiber, *IBS*, Hamburg

Termin und Ort:

17.-18. September 2001,
Montag 09:30-17:00 Uhr,
Dienstag 09:00-ca. 15:30 Uhr
im *IBS*-Schulungscenter,
Hamburg, Friedrich-Ebert-Damm 145.

Teilnehmer:

Revisoren und Betriebsverantwortliche

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Susanne Albers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 - 15
schriftl.: IBS, Friedrich-Ebert-Damm 145,
22047 Hamburg

IBS ***Prüfen mit Konzept***

Access für Revisoren

Inhalte u.a.:

- Einlesen von Prüfdaten in ACCESS
- Erstellen von Feldstatistiken
- Schichten von Datenbeständen
- Analyse der extrahierten Daten
- Verknüpfen von ACCESS-Tabellen und vergleichbare Auswertungen
- SQL-Abfragen
- Zusammenfassung am Beisp. einer kompletten interaktiven Prüfung von Datenbeständen inkl. grafischer Auswertung

Der Referent:

Thomas Tiede, ibs schreiber gmbh Hamburg
Frank Christensen, CCC, Hamburg

Termin und Ort:

24.-26. September 2001,
Montag 09:30-17:00 Uhr,
Dienstag 09:00-17:30 Uhr,
Mittwoch 09:00-ca. 15:30 Uhr
im *IBS*-Schulungscenter,
Hamburg, Friedrich-Ebert-Damm 145.

Teilnehmer:

Revisoren und externe Prüfer

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Susanne Albers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (0 40) 69 69 85 -15
schriftl.: IBS, Friedrich-Ebert-Damm 145,
22047 Hamburg

IBS ***Prüfen mit Konzept***

Einführung in die IT-Revision

Inhalte u.a.:

- Chancen und Risiken der IT-Revision
- Prüfen vernetzter IT-Systeme
- Verfahrensprüfungen
- Einzelfallprüfungen
- Zusammenstellung von Sollvorgaben
- Beispielhafte Prüfberichte zu den vorgestellten IT-Revisions-Kategorien

Der Referent:

Dirk Kirchner, ibs schreiber gmbh, Hamburg
Pascal Rohmann, ibs schreiber gmbh, Hamburg

Termin und Ort:

26.-28 September 2001,
Mittwoch 09:30-17:00 Uhr,
Donnerstag 09:00-17:30 Uhr,
Freitag 09:00-ca. 15:30 Uhr
im *IBS*-Schulungscenter,
Hamburg, Friedrich-Ebert-Damm 145.

Teilnehmer:

Revisoren und Datenschutzbeauftragte

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Susanne Albers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (0 40) 69 69 85 -15
schriftl.: IBS, Friedrich-Ebert-Damm 145,
22047 Hamburg

IBS ***Prüfen mit Konzept***

WindowsNt Server für Revisoren

Inhalte u.a.:

- NT-Philosophie
- NT-Domänen-Konzept
- Benutzerverwaltung/ -profile
- Zugriffsrechte auf Ressourcen
- Systemrichtlinien
- Service Pack - Prüfwerkzeuge
- Mindestrechte für den DV-Revisor
- Vorbereitung einer Prüfung

Der Referent:

Marcus Rasokat, ibs schreiber gmbh, Hamburg,

Termin und Ort:

24.-26. September 2001,
Montag 09:30-17:00 Uhr,
Dienstag 09:00-17:30 Uhr,
Mittwoch 09:00-ca. 15:30 Uhr
im *IBS*-Schulungscenter,
Frankfurt/Main, Eschborner Landstr. 55.

Teilnehmer:

Revisoren und Datenschutzbeauftragte

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Susanne Albers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (0 40) 69 69 85 -15
schriftl.: IBS, Friedrich-Ebert-Damm 145,
22047 Hamburg

IBS ***Prüfen mit Konzept***

SAP R/3 - Workshop „Materialwirtschaft“

Inhalte u.a.:

Die SAP-R/3-Materialwirtschaft bildet für viele betriebswirtschaftliche Vorgänge die Grundlage. Grundverständnis ist für eine Prüfung unerlässlich.

- Bedarfplanung / Prognosen
- Anfragen / Angebote
- Bestellungen / Kontrakte
- Bestandführung / Bewertung
- Inventur / Bilanzwertung

Der Referent:

Dipl.-Betriebswirt, Dipl.-Kfm. Reiner Stein, KPMG, Essen

Termin und Ort:

10.-12. Oktober 2001,
Mittwoch 09:30-17:00 Uhr,
Donnerstag 09:00-17:30 Uhr,
Freitag 09:00-ca. 15:30 Uhr
im *IBS*-Schulungscenter,
Hamburg, Friedrich-Ebert-Damm 145.

Teilnehmer:

Revisoren und externe Prüfer

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Susanne Albers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (0 40) 69 69 85 -15
schriftl.: IBS, Friedrich-Ebert-Damm 145,
22047 Hamburg

IBS ***Prüfen mit Konzept***

SAP R/3-Revisions-Workshop Personalwesen

Inhalte u.a.:

- Berechtigungskonzept und -prüfung im HR
- Grundlagenwissen zur Prüfung der Reisekostenabrechnung
- Grundlagenwissen zur Prüfung der Zeitwirtschaft
- Grundlagenwissen zur Prüfung der Personalplanung
- Revision eines HR-Systems

Der Referent:

Heidemarie Valentin, Siemens Business Services GmbH, Hamburg/Kiel

Termin und Ort:

15.-17. Oktober 2001,
Montag 09:30-17:00 Uhr,
Dienstag 09:00-17:30 Uhr,
Mittwoch 09:00-ca. 15:30 Uhr
im *IBS*-Schulungscenter,
Frankfurt/Main, Eschborner Landstr. 55.

Teilnehmer:

Revisoren und Datenschutzbeauftragte

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Susanne Albers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (0 40) 69 69 85 -15
schriftl.: IBS, Friedrich-Ebert-Damm 145,
22047 Hamburg

IBS ***Prüfen mit Konzept***

Seminare Jul. 2001- Dez. 2002

Inhalte u.a.:

Grundlagen und Management der Revision
Prüfung in SAP R/3
IT-Revision

- Grundlagen der IT-Revision
- Prüfen in Betriebssystemen
- Automatische Datenprüfung
- Sonderseminare für die IT-Revision

Branchenspezifische Prüfungen

- Baurevision
- Umwelt-Auditing
- Prüfung in Banken

Fordern Sie kostenfrei unsere Seminar-Broschüre

Termin und Ort:

Jul. 2001 - Dez. 2002,
in den *IBS*-Schulungscentern,
Hamburg, Friedrich-Ebert-Damm 145
Frankfurt/Main, Eschborner Landstr. 55.

Teilnehmer:

für Revisoren, DV-Revisoren, Manager, Wirtschaftsprüfer, Controller, IT-Sicherheits- und Datenschutzbeauftragte

Anmeldung und Auskünfte:

Bitte melden Sie sich bei
Susanne Albers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (0 40) 69 69 85 -19
schriftl.: IBS, Friedrich-Ebert-Damm 145,

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

Das neue Bundesdatenschutzgesetz

Welche Änderungen kommen auf den Datenschutzpraktiker zu?

Inhalte u.a.:

Das auf der Grundlage der EU-Richtlinie und des Entwurfs der Bündnis90/Die Grünen geänderte Bundesdatenschutzgesetz, trat am 23. Mai 2001 in Kraft.

- Wichtigste Änderungen und Auswirkungen
- Synopse bisheriges Gesetz - künftige Regelungen

Der Referent:

RA Dr. Hans-Jürgen Schaffland, Deutscher Genossenschafts- und Raiffeisenverband e.V.,Bonn
Dipl.-Volkswirt Friedhelm Wolf, Dresdner Bank AG, Frankfurt am Main

Termin und Ort:

28. September 2001,
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 **010922**.

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

Mehrwertsteuer für Kreditinstitute

Inhalte u.a.:

- Einzelfragen aus dem Bereich der Aktivumsätze
- Vorsteuerabzug
- Europarechtliche Aktuelle Enscheidungen und Rechtsentwicklungen
- Abzugsverfahren
- Verschiedenes

Der Referent:

Rolfjosef Hamacher, Rechtsanwalt, Fachanwalt für Steuerrecht, KPMG, Frankfurt am Main

Termin und Ort:

19. Oktober 2001,
im Steigenberger Airport Hotel,
Frankfurt am Main, Unterschweinstiege 1.
Tel: (069) 69 75 -0

Teilnehmer:

Fach- und Führungskräfte aus den Bereichen Risiko Controlling, Risk Management, Controlling, Treasure, Handel, Rechnungswesen und Revision.

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 **011020**.

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

Was muss ein Datenschutzbeauftragter bei vernetzten Systemen beachten?

Intensiv-Seminar

Inhalte u.a.:

- Schwachstellen unter Datenschutzaspekten; Komponenten in Netzwerken
- Datenschutzrechtliche Grundlagen bei vernetzten Systemen: Verpflichtung auf das Datengeheimnis, etc.
- Umsetzung der Datenschutzbestimmungen: Richtlinien im PC-Bereich, Formularwesen, Datenschutzaudit, Mobile personenbezogenen Speicher- und Verarbeitungsmedien

Der Referent:

Harald Dischner, debis Systemhaus GmbH, Nürnberg
Dipl.-Volkswirt Friedhelm Wolf, Dresdner Bank AG, Frankfurt am Main

Termin und Ort:

01. und 02. Oktober 2001,
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 **011032**.

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

Controllung derivativer Finanzinstrumente

Risiko- und Ertragssteuerung

Inhalte u.a.:

- Finanzmathematische Grundlagen
- Grundidee der Marktzinsmethode
- Cash Flow Ermittlung von Swaps, FRAs, Futures und weitere Derivate
- Case-Study: Performancemessung eines Muster-Portfolio sowie Value-at-Risk-Berechnung eines Derivate-Portfolios
- Neue Trends im Aufsichtesrecht: MAK, Internes Rating, Baseler Kreditrisiko-Papiere

Der Referent:

Dr. Thomas Hartschuh, Partner Risk Advisory, Value at Risk AG, Bad Homburg

Termin und Ort:

12. September 2001,
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Teilnehmer:

Fach- und Führungskräfte aus den Bereichen Risiko Controlling, Risk Management, Controlling, Treasure, Handel, Rechnungswesen und Revision.

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 **010969**.

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

Intensiv-Training für Datenschutzbeauftragte

Grundlagenseminar

Inhalte u.a.:

- Das Bundesdatenschutzgesetz (Grundzüge, Definitionen, Zulässigkeit der Datenverarbeitung, Benachrichtigung, Auskunft)
- Der Datenschutzbeauftragte (persönliche Voraussetzungen)
- die Aufgaben des Datenschutzbeauftragten
- Die Erfahrungen mit dem Gesetz und den Aufsichtsbehörden

Der Referent:

RA Dr. Hans-Jürgen Schaffland, Deutscher Genossenschafts- und Raiffeisenverband e.V.,Bonn
Dipl.-Volkswirt Friedhelm Wolf, Dresdner Bank AG, Frankfurt am Main

Termin und Ort:

11. und 12. September 2001,
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 **010933**.

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

Das Geldwäschegesetz in der Praxis

Teil 1: Gesetzliche Grundlagen

Inhalte u.a.:

- Erscheinungsformen der Organisierten Kriminalität und Formen der Geldwäsche
- Internationale Bemühungen zur Bekämpfung der Geldwäsche
- Straftatbestand der Geldwäsche gem. § 261 StGB, organisatorische Vorkehrungen gem. § 14 Abs. 2 GwG und Plicht zur Indentifizierung gem. § 154 AO und GwG
- Aufzeichnung des wirtschaftlich Berechtigten, Anzeige verdächtiger Kunden, Konten, Transaktionen, Risiken für Mitarbeiten und Bank

Der Referent:

Wolfgang Gabriel, Rechtsanwalt, Geldwäschebeauftragter der BfG Bank AG, Frankfurt am Main

Termin und Ort:

10. September 2001,
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 **010937**.

IBS *Prüfen mit Konzept*

IBS-Fachkonferenz 2001

IT-Revision

24.09.-25.09.2001 in München

IT-Revision

Das Themenfeld der IT-Revision ist heterogen und erweitert sich ständig. Ursache ist die permanent steigende interne und externe IT-Vernetzung der Unternehmen. Nicht nur die Prüfung der IT-Infrastruktur unter Ordnungsmäßigkeit-, Sicherheits- (Datenschutz- und Datensicherheit) und Wirtschaftlichkeitsaspekten steht im Prüfungsfokus, sondern zusätzlich die Abläufe von betrieblichen Prozessen und insbesondere Risikomanagementsysteme mit ihren integrierten Frühwarn-, Kennzahlen- und sonstigen Steuerungssystemen; denn fast alle Prozesse und betrieblichen Steuerungsinstrumente werden IT-basiert angelegt und automatisiert.

Ziel dieser Fachkonferenz

Mithin wird speziell die IT-Revision zu einem kardinalen Faktor im Unternehmen, der maßgeblich auf die Ordnungsmäßigkeit, Sicherheit und Wirtschaftlichkeit dieser IT-gestützten Steuerungs- und Führungsinstrumente hinwirken muss: beratend und in „ex ante“- und permanenten „ex post“-Prüfungen. Diese Fachkonferenz gibt hierzu praktische Orientierungshilfe, indem sie Risiken und Soll-Vorgaben aufzeigt und effizient und effektiv nutzbare IT-gestützte Werkzeuge vorstellt.

Diese Veranstaltung richtet sich an

Führungskräfte, IT-Revisoren,
Sicherheitsexperten und Wirtschaftsprüfer

Themen der zwei Tage:

1. Tag

Firewall-Prüfung
Grundlagen
Manuelle Prüfungen
Automatisierte Prüfungen

von Pascal Rohmann,
ibs schreiber gmbh, Hamburg

Neuere Entwicklung bei Computerviren
Computerviren bilden **eine ständige Gefahr** für die elektronische Datenverarbeitung mit Arbeitsplatzcomputern (PC).

von Dipl.-Ing. Manfred Kramer,
BSI, Bonn

Zertifizierung von IT-Sicherheit nach ISO/IEC 17799 - eine neue Aufgabe der IR

- ISO/IEC 17799 - Management der IT-Sicherheit - Inhalte der Norm
- Vorgehensweisen der Auditierung und Zertifizierung von Managementsystemen

von Dr. Jörn Voßbein,
UIMCert, Wuppertal

KonTraG und das Management von IT-Risiken

- Bedeutung und Auswirkung des KonTraG
- Integration des IT-Risikomanagements in das Risikomanagement des Unternehmens

von Alfred Koch, CISA,
KPMG, Düsseldorf

2. Tag

Digitales Dokumentenmanagement

- Rechtliche Rahmenbedingungen
- Auswirkungen ab 2002 durch GDPdU, FAIT 1, neuer § 14 (4) UStG

von Dr. Mathias Philipp,
CISA, KPMG, Mannheim

Software-Projekte unter Revisionsaspekten

Probleme im Entwicklungsprozess
Zur Ordnungsmäßigkeit von Software-Projekten
Zur Sicherheit von Softwareprojekten
Zur Wirtschaftlichkeit von Softwareprojekten

von Christoph Alt,
ibs schreiber gmbh, Hamburg

Aufbau von IT-gestützten Kennzahlensystemen unter Revisionsaspekten

- Kennzahlensysteme: ein Instrument zur Firmensteuerung?
- Kennzahlensysteme als Teil von Frühwarnsystemen
- Methodik zur Entwicklung und IT-Werkzeuge zum Aufbau von Kennzahlensystemen
- Blick in die Zukunft: Balanced ScoreCards

von Dipl.-Ing. Ottokar Schreiber,
IBS, Hamburg

IBS *Prüfen mit Konzept*

Konditionen:

Teilnahmegebühr/Person:
DM 1.900,– / € 971,45 zzgl. MwSt.

Im Preis enthalten sind Fachkonferenzunterlagen, Mittagessen, Kaffee und Pausengetränke **sowie das Abendprogramm** am 24.09.2001(abends).

Termin: **24.-25.09.2001 in München**
Ort: **Hotel Vitalis**

Veranstalter: *IBS* **Hamburg**
Friederich-Ebert-Damm 145
22047 Hamburg
www.ibs-hamburg.com

Zentrale Buchung:
Tel: +49 40 - 69 69 85 -15
Fax: +49 40 - 69 69 85 -31
eMail:seminare@ibs-hamburg.com

Sonstiges: Stornieren ist bis zum 15.09.2001 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.

<

Bestell-/Anmelde-Fax FKIT „IT-Revision“ München

Tel: +49 40 - 69 69 85 -15 / Fax: +49 40 - 69 69 85 -31 / eMail:seminare@ibs-hamburg.com

☐ Senden Sie mir bitte die ausführliche Kongress-Broschüre kostenfrei zu.

☐ Ja, ich nehme an der Fachkonferenz „IT-Revision“ teil.
Gebühr/Pers.: DM 1900,-/ € 971,45 zzgl. MWST

Anzahl der Personen: _____

Hotelreservierung von: _____ bis: _____

☐ Raucher ☐ Nichtraucher

Bei Buchung über *IBS* gewährt das Hotel folgende *IBS*-Sonderkonditionen:

vom 23.09. bis 24.09 2001
☐ Einzelzimmer incl. Frühstück DM 285,-
☐ Einzelzimmer incl. Frühstück DM 385,-

vom 24.09. bis 25.09 2001
☐ Einzelzimmer incl. Frühstück DM 160,-
☐ Einzelzimmer incl. Frühstück DM 210,-

Name: _____

Abteilung: _____

Firma: _____

Straße: _____

PLZ/Ort: _____

Telefon/Fax: _____

eMail: _____

Datum/Unterschrift: _____

IBS *Prüfen mit Konzept*

IBS-Fachkonferenz 2001
Revision von SAP® R/3™

vom 15.10.-16.10.2001

IBS-Strategieseminar 2001
SAP® R/3™

17.10.2001

im Hotel Mercure in Berlin

Wann ist ein SAP® R/3™-System sicher?

Rund um diese Fragestellung werden wir uns mit der Sicherheitsproblematik beim Einsatz eines SAP® R/3™-Systems beschäftigen.

Resultierend aus der stetig steigenden Komplexität der Datenstrukturen und Funktionalitäten gilt es, die diversen Sicherheitsprobleme zu eruieren, aufzunehmen und entsprechende Maßnahmen im Rahmen der Prüfung gegen Ordnungsmäßigkeits-, Sicherheits- und Wirtschaftlichkeitskriterien zu treffen.

Auf diesem Expertenforum werden wir zum einen die Problematiken diskutieren und zum anderen praxisorientierte Lösungskonzepte vorstellen.

Nutzen Sie die Gelegenheit zu einem fachbezogenen Erfahrungsaustausch!

Konkrete Fallbeispiele werden direkt am SAP® R/3™-System erläutert!

Diese Veranstaltung richtet sich an

Interne Revision
Wirtschaftsprüfung
Systemadministration
Datenschutz
Finanz- und Rechnungswesen

Themen der zwei Tage:

1. Tag

Aufbau einer SAP®-R/3™-Sicherheitsarchitektur aus Sicht „Internal-Controls“

- Datenbank-, Betriebssystem und Netzwerksecurity einer SAP® R/3™-Systemlandschaft

von Otto Arnold Schell, OPEL Powertrain GmbH

SAP® R/3™ MM-Testat - Freibrief oder Prüfungsgebot?

SAP® verweist bei Ordnungsmäßigkeitsfragen auf ein für die Materialwirtschaft in 2000 erteiltes Softwaretestat.

von Dipl.-Betriebswirt, Dipl.-Kfm. Reiner Stein, KPMG, Essen

mySAP.com: E-Business Security

- Benutzer- und Rollenverwaltung
- Sicherheit auf Anwendungsebene

von Stefanie Franz, SAP® AG, Walldorf

Berechtigungsadministration in mySAP HR

- Rollendefinitionen in mySAP HR
- mySAP Transaktionen zur Erstellung von Rollen und Berechtigungsprofilen

von Dipl.-Kfm. Gerald Borchert, Siemens Business Services, Hamburg

Abendprogramm

2. Tag

SAP® Benutzer- und Berechtigungsadministration bei der Bayer AG

- Abbildung der Funktionstrennung im SAP®-System
- Anforderungs- und Freigabeverfahren als Workflow in Lotus Notes

von Dipl.-Kfm. Johannes Kumpf, Bayer AG, Leverkusen

RFC (Remote Function Call) - Eine unterschätzte Gefahrenquelle für das R/3™-System

- RFC-Destinationen - Gefahr durch hinterlegte Kennwörter und Vertauensbeziehungen
- Brute-Force-Attacks auf R/3™ über einen RFC-Zugriff
- Zugriff auf R/3™ von anderen Anwendungen, z. B. MS Excel

von Thomas Tiede, ibs schreiber gmbh, Hamburg

Hacken aus SAP® R/3™-Betriebssystemkommandos: Backdoor oder Feature?

Der Vortrag demonstriert, wie aus einem SAP® R/3™-System heraus ein unautorisierter Zugriff auf einen Server erfolgen kann. Daraus resultierend werden Wege zu einem sicheren SAP-System vorgestellt.

von Stefan Hölzner, KPMG, Essen

Abschlussdiskussion

Kongress 2001

ISO/IEC 17799
ein neuer Weg zu mehr IT-Sicherheit

Eine neue Aufgabe für interne Revisoren

12.11.-13.11.2001 in Hamburg

Interne Auditierung der IT-Sicherheit
Der erste Schritt zur Zertifizierung gem. ISO/IEC 17799

Nicht sichere IT-Systeme sind kein Kavaliersdelikt mehr: Je größer die Abhängigkeit von der IT-gestützten Informationsverarbeitung wird, desto wichtiger wird Sicherheit. IT-Sicherheit ist häufig noch keine Chefsache: In nur 20 % aller Unternehmen wird die Unternehmensleitung selbst in Sachen IT-Sicherheit initiativ tätig. Das ist nicht genug im Hinblick darauf, dass auch das KonTraG von Vorstand eine Beschäftigung mit den existenzgefährdenden Risiken, also auch denen der IT-Sicherheit fordert. Die ISO/IEC 17799 liefert die Grundlage für eine Auditierung mit nachfolgender Zertifizierung. Das Problem einer objektiven Prüfgrundlage, die es ermöglicht, die IT-Sicherheit an einer vorgegebenen einheitlichen Norm zu beurteilen, ist nur durch einen vorgegebenen Standard wie die ISO/IEC 17799 zu lösen. Die mit der ISO 9000 gewonnenen allgemeinen Erfahrungen lehren, dass die Vorbereitung auf die Zertifizierung der wichtigste Schritt für das Unternehmen selbst ist: Wie das bei der ISO/IEC 17799 zu erreichen ist, will dieser Kongress zeigen, insbesondere aber, welchen Beitrag die Institutionen des Unternehmens, vor allem die **Interne Revision**, hierzu leisten können. Dies spart Kosten und erhöht die unternehmenseigene Kompetenz.

Themen der zwei Tage:

1. Tag

Einführung in die Problematik: Ist IT-Sicherheit zertifizierbar?
von Prof. Dr. Reinhard Voßbein, UIMCert, Wuppertal

Standards als Grundlage der Zertifizierung
Der Weg vom Orange Book zur ISO 17799: Konzept und Bedeutung
von Dipl. Math. Klaus J. Keus, BSI, Bonn

Auditierung, Zertifizierung und interne Revision
Interne Audits als Vorbereitung der Zertifizierung - eine Aufgabe der internen Revision
von Wolfgang Sigart, Österreichische Lotterien, Wien
Auditierungstools für die Vorbereitung von Audits und Zertifizierung
von Dr. Jörn Voßbein, UIMC, Wuppertal

Praktische Erfahrungen in Unternehmen mit Audits und Zertifizierungen
Warum wollten wir uns sicherheitsauditieren lassen?
von Dipl.-Kfm. Egon Nählen, ZEDA, Wuppertal
Erfahrungen mit dem Sicherheitsaudit und -zertifikat
von Gerhard Hielscher, SIG, Linnich

UIMCert
Unternehmens- und Informations-Management Certification

IBS
Prüfen mit Konzept

Vorteile und Nutzen von IT-Sicherheitsauditierungen und Zertifizierungen
Das KonTraG - eine indirekte Forderung nach IT-Sicherheitszertifizierung
von Alfred Koch, KPMG, Düsseldorf
Interne und externe Nutzen von Auditierung und Zertifizierung auf dem IT-Sicherheitssektor
von Dipl.-Kfm. Detlef Hüggenberg, QMC, Oberhausen

2. Tag

Auditierung und Zertifizierung des IT-Sicherheitsmanagements und die Lösung der ISO 17799: Inhalte, Fragen und Diskussion
von Prof. Dr. R. Voßbein und Mitarbeiter

Technische Revisionstools zur Unterstützung des Auditierungs- und Zertifizierungsprozesses
von Dipl.-Ing. Ottokar Schreiber, *IBS*, Hamburg

Auditierung des Datenschutzes als Sondergebiet der IT-Sicherheit
Datenschutzaudits und Zertifikat - Nutzen für die zertifizierte Institution. Können Datenschutzaudits gem. ISO17799 durchgeführt werden?
von Dr. Heiko Haaz, Universitätsklinikum, Aachen
Gütesiegel und Datenschutzaudit nach dem schleswig-holstein. Landesdatenschutzgesetz
von Dr. Helmut Bäumler, ULD, Kiel

Konditionen:

Teilnahmegebühr/Person:
DM 1900,-/ € 971,45 zzgl. MWST

Im Preis enthalten sind Fachkonferenzunterlagen, Mittagessen, Kaffee und Pausengetränke **sowie das Abendprogramm** am 12.11.2001(abends).

Termin: **12.-13.11.2001 in Hamburg**
Ort: **Steigenberger Hotel, Hamburg**

Veranstalter: **UIMCert GmbH**
Bismarckstraße 45
42115 Wuppertal
www.uimcert.de

IBS **Hamburg**
Friederich-Ebert-Damm 145
22047 Hamburg
www.ibs-hamburg.com

Zentrale Buchung:
Tel: +49 40 - 69 69 85 -15
Fax: +49 40 - 69 69 85 -31
eMail:seminare@ibs-hamburg.com

Sonstiges: Stornieren ist bis zum 19.10.2001 möglich. Danach ist die Veranstaltungsgebühr in voller Höhe zu zahlen. Ersatzteilnehmer können benannt werden.

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

<

Bestell-/Anmelde-Fax Kongress „ISO/IEC 17799“ Hamburg

Tel: +49 40 - 69 69 85 -15 / Fax: +49 40 - 69 69 85 -31 / eMail:seminare@ibs-hamburg.com

☐ Senden Sie mir bitte die ausführliche Kongress-Broschüre kostenfrei zu.

☐ Ja, ich nehme an dem Kongress „ISO/IEC 17799“ teil.
Gebühr/Pers.: DM 1900,-/ € 971,45 zzgl. MWST

Anzahl der Personen: _____

Hotelreservierung von: _____ bis: _____

☐ Raucher ☐ Nichtraucher

Bei Buchung über *IBS* gewährt das Steigenberger Hotel folgende *IBS*-Sonderkonditionen:

☐ EZ incl. Frühstück DM 310,-
☐ DZ incl. Frühstück DM 390,-

Name: _____
Abteilung: _____
Firma: _____
Straße: _____
PLZ/Ort: _____
Telefon/Fax: _____
eMail: _____
Datum/Unterschrift: _____

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.osv-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: DM 90,- (incl. 7% MwSt).

Abo-Bestellschein für die **ReVision**

Tel: +49 40 - 69 69 85 - 11 / Fax: +49 40 - 69 69 85 - 31 / eMail:sales@osv-hamburg.de

Hiermit bestelle ich ReVision im Jahresabonnement zum nächstmöglichen Zeitpunkt. Ein Jahresabonnement (4 Ausgaben) kostet DM 90,- 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: _____