Ottokar R. Schreiber
Herausgeber

Liebe Leserinnen und Leser,

Management-Auditing ist ein häufig diskutiertes, aber kaum umgesetztes Thema: Wie auch, ist doch der Interne Revisor Beauftragter seines eigenen Vorstandes!

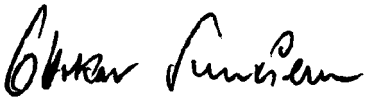
Geschäftsschädigenden Handlungen "auf die Spur" zu kommen und ihnen möglichst mit - durch die Interne Revision empfohlenen - präventiven Maßnahmen zuvorzukommen, ist eine der vornehmsten Aufgabe der Internen Revision. Was aber, wenn das Management selber, und dann i.d.R. für den Betrieb existenzgefährdent, geschäftsschädigend handelt? Firmenidentität und Firmenkultur werden unter modernen Attributen wie "Global Player", "shareholder value" und "Flexibilität" kaputt gemacht, egomanisch veranlagten Vorständen wird freies Feld gelassen.

Die großen - und nur die offenkundigen kennen wir - Pleiten in Amerika lassen Böses ahnen, Holzmann und Babcock-Borsig geben entsprechende aktuelle Beispiele auch hier in Deutschland ab. Und dann soll sich der Interne Revisor auf die - unter solchen Gegebenheiten nur noch marginal erscheinende - Prüfung z.B. von Reisekostenabrechnungen konzentrieren? Geschäftsschädigende Handlungen: ein Dauerthema für die Revision! Frank Haub gibt in seinem aus der täglichen Prüferpraxis gespeisten Beitrag umsetzbare Hinweise und Checklisten auf.

ReVision versteht die Aufgabe des Revisors nicht nur als Kontrollinstrument des Vorstandes, sondern auch als Schnittstelle zwischen externen Prüfern und dem Betrieb. Deshalb werden Sie, liebe Leser, in ReVision in steigendem Maße auch Beiträge in diesem Sinne lesen können. Prof. Carl-Christian Freidank startet in einer mehrteiligen Beitragsfolge mit "IT-gestützte Jahresabschlußgestaltung für mittelständische Unternehmen nach der Steuerreform".

Viele Anregungen für Ihre Prüfarbeit wünscht Ihnen wie immer

Ihr



Ottokar R. Schreiber

Verlagshinweis:
Nächste Ausgabe der
ReVision
Oktober 2002

Redaktions-/Einsendeschluss für diese Ausgabe: 20.09.2002

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
Fon: +49(0)40 /69 69 85 -14 Fax +49(0)40 /69 69 85 -31
eMail: sales@osv-hamburg.de
www.revision-hamburg.de

Beiträge

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

eMail: redaktion@osv-hamburg.de

Anzeigen

Zu den Konditionen rufen Sie bitte unsere aktuellen Mediadaten ab. Zur problemlosen Abwicklung und korrekten Darstellung stellen Sie uns die Anzeigen vorzugsweise als belichteten Film zur Verfügung. Sollte dies nicht möglich sein, bitten wir um Rücksprache hinsichtlich der gelieferten Dateiformate. Telefon 040 / 69 69 85 -11. Design-Erstellung auf Wunsch auch durch unsere Medienabteilung möglich.

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

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

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

Druck: Druckerei Zollenspieker Kollektiv GmbH
Zollenspieker Hauptdeich 54
21037 Hamburg

Printed in Germany.
Gedruckt auf chlorfrei gebleichtem Papier

IT-gestützte Jahresabschlussgestaltung für mittelständische Unternehmen nach der Steuerreform Teil I

Von o. Univ.-Prof. Dr. Carl-Christian Freidank, StB,
Geschäftsführender Direktor des Instituts für
Wirtschaftsprüfung und Steuerwesen der Universität Hamburg
Lehrstuhl für Revisions- und Treuhandwesen

I Problemstellung: Aktualisierung der computergestützten Jahresabschlussoptimierungsmodelle aus den neunziger Jahren

In den 90er Jahren wurden vom Verfasser computergestützte Modelle für Kapitalgesellschaften vorgelegt, die auf die Planung eines zieloptimalen handels- und/oder steuerrechtlichen Jahresabschlusses ausgerichtet sind.[1] Es hat sich gezeigt, dass die Konzepte sowohl im Rahmen der Rechnungslegungspolitik als auch für Zwecke der Finanz- und Bilanzplanung erfolgreich eingesetzt werden können. Diese Basismodelle, die zwischenzeitlich in einigen wichtigen Bereichen weiterentwickelt wurden,[2] sind in menügesteuerte Softwarepakete[3] zu integrieren, wodurch die zielgerichtete Gestaltung des Einzel- und Konzernabschlusses aus nationaler und internationaler Sicht erheblich vereinfacht wird. Allerdings sind die Grundansätze lediglich in der Lage, die aus den Optimierungsergebnissen resultierende Ertragsteuerbelastung vereinfachend zu berücksichtigen. Durch jüngste Forschungen ist es gelungen, die ebenfalls vom Verfasser entwickelten simultanen Matrizenmodelle, die auf eine exakte Ermittlung der ergebnisabhängigen Aufwendungen (Körperschaft-, Gewerbeertragsteuer- und Tantiemenaufwand) ausgerichtet sind,[4] in die rechnungslegungspolitischen Optimierungsmodelle zu integrieren. Die Ergebnisse dieser Forschungsarbeiten, die zu einer unmittelbaren Verwendbarkeit der Ansätze in der betrieblichen Praxis führen dürften, werden nachfolgend anhand von Beispielen dargelegt.

Darüber hinaus hat die handels- und/oder steuerrechtliche Rechnungslegung von Kapitalgesellschaften durch die jüngsten Steuerreformen tiefgreifende Umbrüche erfahren.[5] Zum einen wurden die Bilanzierungs- und Bewertungsvorschriften des Bilanzsteuerrechts durch das Steuerentlastungsgesetz grundlegend novelliert. Zum anderen hat der Wechsel vom Anrechnungsverfahren zum Halbeinkünfteverfahren elementare Änderungen bezüglich der Körperschaftsteuerbelastung von Kapitalgesellschaften mit sich gebracht. Vor diesem Hintergrund wird weiterhin verdeutlicht, wie die Optimierungsmodelle an die Parameter der jüngsten Steuerreformen angepaßt werden können. Die Konzepte sind aus Vereinfachungsgründen auf die Gestaltung der Einheitsbilanz von Kapitalgesellschaften ausgerichtet, obwohl eine vollständige deckungsgleiche handels- und steuerrechtliche Bilanzierung durch die vielfältigen Durchbrechungen des Maßgeblichkeitsprinzips infolge des Steuerentlastungsgesetzes nur noch in Ausnahme-

> „Der Wechsel vom Anrechnungsverfahren zum Halbeinkünfteverfahren hat elementare Änderungen bezüglich der Körperschaftsteuerbelastung von Kapitalgesellschaften mit sich gebracht.“

fällen möglich sein dürfte. Da zum gegenwärtigen Zeitpunkt der Einbezug des deutschen Einzelabschlusses in die internationalen Harmonisierungsbestrebungen nicht zuletzt auch vor dem Hintergrund des in Deutschland gültigen Maßgeblichkeitsprinzips und seiner Umkehrung (§ 5 Abs. 1 EStG) kritisch gesehen und weitgehend abgelehnt wird,[6] weil sie zum Zwecke der Kapitalaufnahme im Ausland nicht erforderlich erscheinen, beziehen sich die folgenden Ausführungen auf den gegenwärtigen Zustand des deutschen Handels- und Steuerrechts.

„Der Einbezug des deutschen Einzelabschlusses in die internationalen Harmonisierungsbestrebungen wird kritisch gesehen und weitgehend abgelehnt.“

Schließlich ist in diesem Zusammenhang von Interesse, dass nach dem jüngsten Verordnungsentwurf der EU-Kommission alle börsennotierten Mutterunternehmen in der Europäischen Union, deren Wertpapiere an einem geregelten Markt notiert werden, ihre Konzernabschlüsse ab 2005 zwingend nach den Regelungen der International Accounting Standards (IAS) aufstellen müssen.[7] Über die definitive Einführung hinaus will der Verordnungsentwurf die Anwendung der IAS durch die Gestaltung eines Mitgliedstaatenwahlrechts fördern. So können diese entweder verbindlich vorschreiben oder aber zulassen, dass Einzelabschlüsse börsennotierter Unternehmen sowie Einzel- und/oder Konzernabschlüsse nicht gelisteter Unternehmen ebenfalls nach IAS erstellt werden. Es ist gegenwärtig noch nicht abzusehen, inwieweit der deutsche Gesetzgeber von seinem Wahlrecht Gebrauch machen wird. Erste informelle Äußerungen aus dem Bundesministerium der Justiz deuten aber darauf hin, dass die große Zahl mittelständischer Unternehmen, die einen organisierten Markt i.S.v. § 2 Abs. 5 WpHG nicht in Anspruch nehmen (z.B. ca. 700.000 Kapitalgesellschaften bzw. Kapitalgesellschaften & Co. in der Rechtsform der GmbH bzw. der GmbH & Co.), nach 2005 weiterhin ihre Einzelabschlüsse nach den Vorschriften des Handelsgesetzbuches aufstellen werden können. Vor allem für diese Unternehmen sind die anschließend präsentierten Entscheidungsmodelle auch für die Zukunft wichtige Instrumente zur zieloptimalen Gestaltung des Jahresabschlusses.

II. Einsatz quantitativer Methoden im Rahmen der Rechnungslegungspolitik

1. Zurückhaltung der Praxis beim Einsatz mathematischer Methoden

Die relativ geringe Beschäftigung mit den Einsatzmöglichkeiten mathematischer Methoden bei der Konzipierung eines optimalen handels- und/oder steuerrechtlichen Jahresabschlusses liegt überwiegend in der Zurückhaltung der Praxis begründet, Verfahren des Operations Research im Rahmen einer zielorientierten Rechnungslegungspolitik zu verwenden.[8] Unter Rechnungslegungspolitik wird im folgenden die legale Gestaltung aller Publikationsinstrumente (z.B. Jahresabschluss, Lagebericht, Zwischen- und Umweltberichte, Sonder-, Ergänzungs- und Sozialbilanzen) mit der Absicht verstanden, das Verhalten der Adressaten der Rechnungslegung (z.B. Aktionäre, Gesellschafter, Lieferanten, Kreditgeber, private Investoren, Öffentlichkeit, Fiskus) im Sinne der verfolgten Unternehmensziele zu beeinflussen.[9] Einerseits läuft die Gestaltung des Jahresabschlusses vor allem bei kleineren Unternehmen i.d.R. als sequentieller und nicht als simultaner Entscheidungsprozess ab. Andererseits dürfte aber auch die immer noch ablehnende Haltung vieler Praktiker gegen den Einsatz der Mathematik dafür verantwortlich sein, dass sich die simultane Optimierung im Bereich der anwendungsorientierten Rechnungslegungspolitik bisher nicht durchsetzen konnte.

2. Struktur der Optimierungsmodelle

Der IT-Fortschritt bietet mit dem Personal Computer und benutzerfreundlicher Software leistungsfähige technische Grundlagen für den Einsatz von rechnungslegungspolitischen Optimierungsmodellen, so dass die betriebswirtschaftliche Modellkonzipierung inzwischen den Engpass darstellt. Vor diesem Hintergrund werden im folgenden computergestützte Optimierungsmodelle vorgestellt, die zum Zwecke der Gestaltung der Einheitsbilanz unter Berücksichtigung der für Kapitalgesellschaften elementaren Zielgrößen und Aktionsparameter eingesetzt werden können. Durch Variationen der ergebnisbezogen definierten Zielfunktion sowie bestimmter Kennzahlen und/oder Bilanzsummenniveaus, die als Neben-

bedingungen zu formulieren sind, bieten die auf einem gemischt-ganzzahligen Optimierungsansatz basierenden Planungsmodelle die Möglichkeit, mit Hilfe eines Personal Computers die Optimallösungen für die wichtigsten rechnungslegungspolitischen Entscheidungsprobleme zu liefern.

Wie Untersuchungen gezeigt haben, wird den Erfordernissen der betrieblichen Praxis bezüglich einer aussagefähigen Planung des handels- und/oder steuerrechtlichen Jahresabschlusses am ehesten durch die Entwicklung möglichst vereinfachender Partialmodelle entsprochen, die aufgrund der Unsicherheit hinsichtlich der Vorausbestimmung der Unternehmensergebnisse bzw. der sonstigen steuerlichen Einkünfte der Anteilseigner sowie des Potentials der künftig zur Verfügung stehenden Gestaltungsobjekte einperiodig ausgerichtet sein sollten. Wie noch zu zeigen sein wird, sind die PC-gestützten Optimierungsmodelle prinzipiell erweiterungsfähig.

3. Prämissen bei der Konzipierung rechnungslegungspolitischer Entscheidungsmodelle

Die Aufstellung von Planungsmodellen bezüglich der Rechnungslegungspolitik ist im Prinzip darauf ausgerichtet, Handlungsempfehlungen über den Einsatz des Instrumentariums in Abhängigkeit von einer operational formulierten Zielfunktion zu geben. Üblicherweise wird das rechnungslegungspolitische Instrumentarium in sachverhaltsgestaltende (z.B. Vor-Bilanzstichtag-Dispositionen) und darstellungsgestaltende Alternativen (z.B. formelle Alternativen wie etwa Ausweis-, Erläuterungs- und Informationswahlrechte sowie materielle Alternativen wie Bilanzierungs-, Bewertungswahlrechte und Ermessensspielräume) unterschieden.[10] Der nachfolgend angeführte Katalog bringt zusammenfassend diejenigen Prämissen zum Ausdruck, die bei der Konzipierung rechnungslegungspolitischer Entscheidungsmodelle zu berücksichtigen sind und deshalb auch für die Entwicklung der folgenden Optimierungsansätze besondere Bedeutung besitzen.[11]

- Insbesondere die Schwierigkeiten im Hinblick auf eine explizite Abbildung des gesamten unternehmerischen Entscheidungsfeldes haben zu der Erkenntnis geführt, dass den Erfordernissen der Praxis bezüglich einer aussagefähigen Planung der Rechnungslegungsobjekte unter Aufgabe des Prinzips einer *größtmöglichen Simultanoptimierung*[12] am ehesten durch die Konzipierung möglichst vereinfachender rechnungslegungspolitischer Teilmodelle entsprochen wird (Kriterium des Rückgriffs auf Partialmodelle).
- Die Lösung ein- und mehrperiodiger rechnungslegungspolitischer Partialmodelle kann durch einen einzigen, alle materiellen Instrumente und den gesamten Zielplan simultan umfassenden Ansatz[13] oder aber auf der Grundlage einer sukzessiven Koordination der zur Verfügung stehenden materiellen Instrumente und zunächst unvollständig formulierter Zielpläne schrittweise erfolgen.[14] Im Falle der Sequentialplanung muss sichergestellt sein, dass durch systematisches Probieren zumindest eine hinreichend gute Lösung gefunden werden kann (Kriterium des Erreichens einer zumindest hinreichend guten Lösung).
- Der Entscheidungsträger muss in der Lage sein, mit hinreichender Sicherheit beurteilen zu können, ob zum einen die Adressaten die beabsichtigten Reaktionen zeigen und ob zum anderen die Auswirkungen des rechnungslegungspolitischen Instrumentariums ggf. durch Reformen der handels-, steuerrechtlichen und/oder internationalen Vorschriften in Frage gestellt sein könnten (Kriterium der hinreichenden Sicherheit).
- Aufgrund der in aller Regel vorliegenden Ungewissheit im Hinblick auf die Vorausbestimmung der Unternehmensergebnisse bzw. der sonstigen (steuerlichen) Einkünfte der Anteilseigner sollten aus pragmatischer Sicht Mehrzeitpunktentscheidungsmodelle nur bei hinreichend sicheren Erwartungen formuliert werden (Kriterium der pragmatischen Begrenzung des Planungshorizonts).
- Aus dem Zielsystem der Unternehmenspolitik müssen sich eindeutig quantifizierbare materielle Handlungsziele für die Rechnungslegungspolitik ableiten lassen, die die Absichten der übergeordneten Teilpolitiken (z.B. Finanz-, Publizitäts- und Individualpolitik des Managements) bestmöglichst repräsentieren (Kriterium der Quantifizierbarkeit von Handlungszielen).[15]
- Im Falle der Verfolgung mehrerer zueinander in Konkurrenz stehender oder sich gegenseitig aus-

„Üblicherweise wird das rechnungslegungspolitische Instrumentarium in sachverhaltsgestaltende und darstellungsgestaltende Alternativen unterschieden.“

schließender Handlungsziele muss es möglich sein, derartige Konflikte durch Zielgewichtung oder durch Aufstellung einer Rangordnung (z.B. Primär- und Sekundärziele) zu lösen (Kriterium der Konfliktlösbarkeit).[16]

- Zur Realisierung der angestrebten Zielsetzungen müssen dem Entscheidungsträger alle zur Zielerreichung relevanten sachverhalts- und darstellungsgestaltenden (formellen und materiellen) Instrumente zur Verfügung stehen (Kriterium der Vollständigkeit des Instrumentariums).
- Um konträre Sekundärwirkungen des Instrumentaleinsatzes beurteilen und ggf. kompensieren zu können, muss der Entscheidungsträger weiterhin den Flexibilitätsgrad der einzelnen rechnungslegungspolitischen Alternativen kennen (Kriterium der Kenntnis der Flexibilität des Instrumentariums).[17]

Fußnoten:

1 Vgl. Freidank, Entscheidungsmodelle der Rechnungslegungspolitik. Computergestützte Lösungsvorschläge für Kapitalgesellschaften vor dem Hintergrund des Bilanzrichtliniengesetzes, 1990; ders., in: Lachnit (Hrsg.), Controllingsysteme für ein PC-gestütztes Erfolgs- und Finanzmanagement, 1992, S. 159-183; ders., in: FS Bloech, 1998, S. 107-143.

2 Vgl. Krog, Rechnungslegungspolitik im internationalen Vergleich. Eine modellorientierte Analyse, 1997; ders., in: Freidank (Hrsg.), Rechnungslegungspolitik. Eine Bestandsaufnahme aus handels- und steuerrechtlicher Sicht, 1998, S. 273-331; Schäfer, Entscheidungsmodelle der Konzernrechnungslegungspolitik. Computergestützte Gestaltungen des Konzernabschlusses nach den Vorschriften des Handelsrechts und der International Accounting Standards, 1999; ders., in: Lachnit/Freidank (Hrsg.), Investororientierte Unternehmenspublizität. Neuere Entwicklungen von Rechnungslegung, Prüfung und Jahresabschlussanalyse, 2000, S. 163-193.

3 Vgl. etwa Layer, in: Freidank (Hrsg.), Rechnungslegungspolitik. Eine Bestandsaufnahme aus handels- und steuerrechtlicher Sicht, 1998, S. 1121-1162.

4 Vgl. Freidank, ZfB 1990, S. 261-279; ders. WPg 1999, S. 811-820; ders. BB 2001, S. 1031-1037.

5 Vgl. Grotherr, in: Lachnit/Freidank (Hrsg.), Investororientierte Unternehmenspublizität. Neuere Entwicklungen von Rechnungslegung, Prüfung und Jahresabschlussanalyse, 2000, S. 255-297; Ott, Steuer- und Bilanzpraxis 2001, 8-20; Scheipers/Schulz, Das bringt die Unternehmenssteuerreform 2001 für mittelständische Unternehmen. Inhalt, Auswirkungen, Gestaltungsempfehlungen, 2000, S. 139-153.

6 Vgl. Küffner/Hoch, BFuP 1998, 57; Hartmann, WPg 1998, 261; Schildbach, BFuP 1998, 21 f.

7 Vgl. Hahn, DStR 2001, S. 1267-1272; Kommission der Europäischen Gemeinschaften (Hrsg.), Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates betreffend die Anwendung internationaler Rechnungslegungsgrundsätze (Stand 13.02.2001); Pellens/Gassner, KoR 2001, S. 137-142.

8 Vgl. Freidank, ZfB 1990, Anmerkung 3, S. 277; Eigenstetter, Entscheidungsmodelle für eine anteilseignerorientierte Steuerpolitik. Zugleich ein Beitrag zur Wahl der Mitunternehmer-GmbH als Gestaltungsinstrument, 1997; Johänntgen-Holthoff, Entscheidungsmodell der Jahresabschlussgestaltung für Publikumsaktiengesellschaften, 1985; Krauss, Integrierte Handels- und Steuerbilanzpolitik. Ein computergestütztes Mehrperioden-Entscheidungsmodell bei mehrfacher Zielsetzung, 1987, Kloock, BFuP 1989, 141-158; Münstermann, in: FS Hintner, 1970, S. 256-290; Schweitzer, Struktur und Funktion der Bilanz. Grundfragen der betriebswirtschaftlichen Bilanz in methodologischer und entscheidungstheoretischer Sicht, 1972, S. 43-154; Seelbach/Fischer, in: Freidank (Hrsg.), in: Rechnungslegungspolitik. Eine Bestandsaufnahme aus handels- und steuerrechtlicher Sicht, 1998, S. 231-271.

9 Vgl. Küting, DStR 1996, 934-944.

10 Vgl. Freidank (Fn. 1), S. 24-39.

11 Vgl. Freidank, WPg 1993, 312-323.

12 Vgl. Bäuerle, ZfB 1989, 175-181.

13 Vgl. Heinhold, DBW 1989, 689-708.

14 Vgl. Freidank, Entscheidungsmodelle der Rechnungslegungspolitik (Fn. 1), S. 95 f.

15 Vgl. Freidank, in: Freidank (Hrsg.), Rechnungslegungspolitik. Eine Bestandsaufnahme aus handels- und steuerrechtlicher Sicht, 1998, S. 91-103.

16 Vgl. Freidank, Entscheidungsmodelle der Rechnungslegungspolitik (Fn. 1), S. 7-21.

17 Vgl. Eigenstetter (Fn. 8), S. 129-164; ders., in: Freidank (Hrsg.), Rechnungslegungspolitik. Eine Bestandsaufnahme aus handels- und steuerrechtlicher Sicht, 1998, S. 449-501.

Das Rollenkonzept in SAP R/3 Gestaltungsmöglichkeiten aus Sicht der IV-Revision

Von Dipl.-Betriebswirt Christoph Wildensee
Stadtwerke Hannover AG

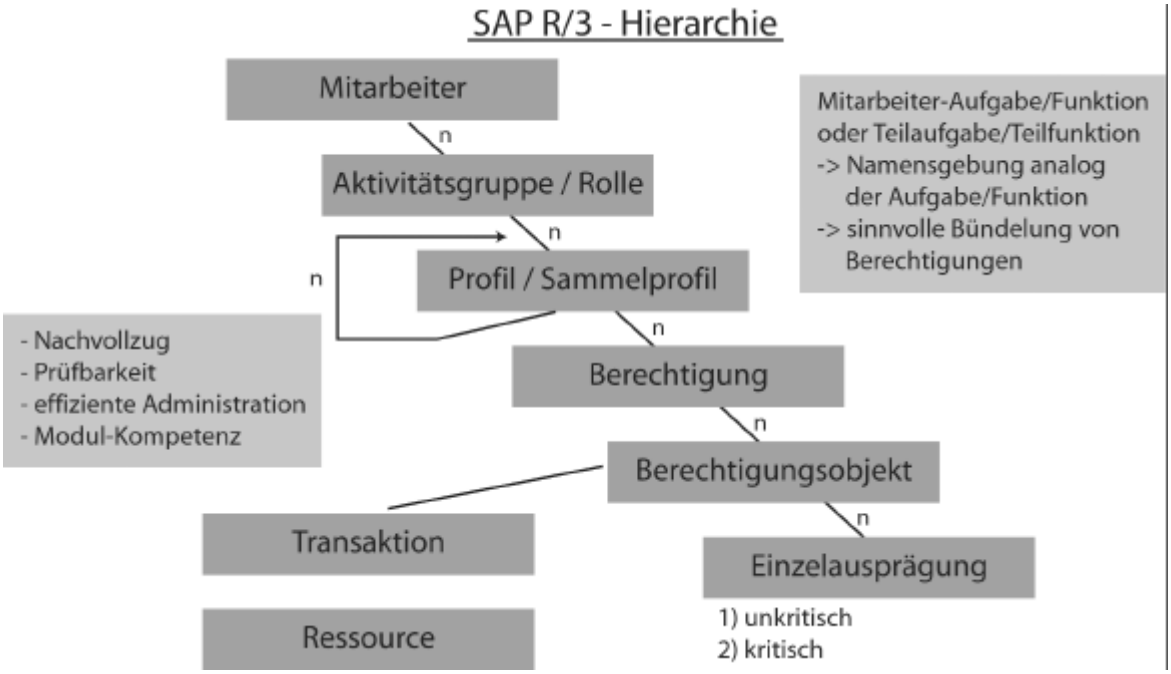
Das Berechtigungskonzept dient als grundlegende Sicherheitsfunktion des SAP R/3-Systems. Elemente dieses Konzeptes sind die Aktivitätsgruppe ([Template- {ab 4.6}]Rolle), das Profil/Sammelprofil, das Berechtigungsobjekt und seine Steuerungsfelder, die Transaktion und letztendlich das Zusammenspiel dieser Komponenten zu einer Berechtigungsstruktur. Die Festlegung von Rahmenbedingungen, die innerhalb des Berechtigungskonzeptes einzuhalten sind, ist eine der wichtigsten Definitionen, bevor die Systemanpassung durchgeführt und das System produktiv gesetzt wird. Im Customizing und der dazugehörigen Dokumentation entscheidet sich der Erfolg oder Misserfolg des zugrundeliegenden Berechtigungskonzeptes. Die Kriterien zur Bemessung sind überschaubar:

Das Berechtigungskonzept muss aus Sicht der Revision

- verständlich, zuverlässig und prüfbar
- ordnungsgemäß gemäß der rechtlichen Rahmen
- somit nachvollziehbar (sowohl aus Sicht der Administration als auch der Revision und des Fachbereiches)
- administrierbar (d.h. Vorhaltung von möglichst wenig Verwaltungsobjekten) und
- praktikabel im Sinne von nutz-/handelbar (insbesondere aus Sicht des Fachbereiches)

sein.

Dieses führt nicht nur dazu, dass es ordnende Elemente geben muss, die als Berechtigungssammler nachvollziehbar/prüfbar und über ein sinnvolles Beantragungswesen zuweisungsfähig sind, sondern auch, dass Funktionen sinnvoll abgegrenzt und in Form von "Berechtigungsbausteinen" vorgehalten werden. Innerhalb des SAP-Systems kann eindeutig definiert werden, wer welche Funktion ausüben soll (Transaktion und Berechtigungsobjekt), was der Einzelne mit Daten durchführen kann (Aktivitätensteuerung Anzeigen, Ändern, Löschen etc.) und innerhalb welcher organisatorischen Grenzen er dies tun darf (Buchungskreis, Einkaufsorganisation etc.).



Entsprechend sind aufgaben-/funktionsorientiert Gruppierungen von Berechtigungen möglich, die zum einen ein Minimum an Verwaltungsobjekten bedeuten, zum anderen aber besonders auch die Administration und die Beantragungsseite in größeren Unternehmen entlasten.

Prüfungsstrukturen

Der IV-Revisor muss sich, wenn er sich im SAP-Umfeld bewegt, mit den Ordnungsbegriffen des SAP-Systems vertraut machen. Einige dieser Begriffe werden im folgenden kurz dargestellt.

Aktivitätsgruppe

Das Konzept von SAP R/3 sieht vor, dass Aktivitätsgruppen als Rollendefinitionen dienen und somit als "Berechtigungssammler" untergeordneter Tätigkeiten oder sonstiger Ordnungskriterien innerhalb des Berechtigungskonzeptes strukturieren (ab Release 4.6 auch [Template-]Rollen genannt). Die Definition von Aktivitätsgruppen kann unterschiedlich erfolgen. Als eine der sinnvollsten Möglichkeiten hat sich die Einrichtung der Aktivitätsgruppen als betriebswirtschaftliche Funktion, Stelle oder Arbeitsplatz herausgestellt, die wiederum ihre Teilfunktionen oder -aufgaben innerhalb der Profile und Sammelprofile abbildet. SAP lässt für die Bezeichnung einer Aktivitätsgruppe bis zu 30 Zeichen zu (siehe über Tabelle DD03L).

Die wichtigsten Prüftabellen für Aktivitätsgruppen sind die folgenden:

Tabelle	Beschreibung
AGR_DEFINE	Aktivitätsgruppe (AktGr.) mit Bezeichnung
AGR_PROF	AktGr. mit zugehörigem Hauptprofil
AGR_1016	AktGr. mit zugehörigen Profilen (auch Teilprofile)
AGR_1250	AktGr. mit zugehörigen Profilen und Berechtigungsobjekten
AGR_1251	wie zuvor, jedoch mit Steuerungsfeldeingrenzung
AGR_USERS	Zuordnung der AktGr. zu den SAP-Nutzern
AGR_SELECT	AktGr. mit zugeordneten Transaktionscode/Menü etc.

Tab. 1: Tabellen zur Prüfung im Bereich Aktivitätsgruppen

Profil / Sammelprofil

Profile und Sammelprofile bieten die weitere Möglichkeit der Untergliederung, Berechtigungen innerhalb des SAP-Systems auf bestimmte Ressourcen zu strukturieren. Profile können dabei als Abbild und Sammler logisch zusammengehöriger, einzelner Berechtigungen im SAP-System im Sinne von Arbeitsschritten verstanden werden. Sammelprofile bündeln diese wiederum zu Tätigkeiten. Hier schließt sich der Kreis, denn diese Arbeitschritt- u/o Tätigkeitsbeschreibungen werden in der Aktivitätsgruppe zu Funktionen/Stellen zusammengefasst. - In vielen Unternehmen werden insbesondere die Sammelprofile nicht genutzt, Profile gelten dort als alleinige Zusammenführung von Ressourcenzuweisungen und Zugriffsdefinitionen. Dies kann zum einen daran liegen, dass die Verwaltung und Einrichtung Schwächen aufweist, zum anderen aber auch, dass die von SAP mitgelieferten Sammelprofile und Rollendefinitionen alter SAP R/3-Releasestände sicherheitstechnische Schwächen aufwiesen (häufige Stern-Berechtigungen). Sie waren zum Teil so eklatant, dass sie nur unter intensiver Nachbearbeitung überhaupt nutzbar waren. So haben viele Unternehmen die vorgefertigten SAP-Bestandteile verworfen und darüber hinaus das Ordnungskriterium Sammelprofil ungenutzt gelassen. - Profile beinhalten die Berechtigungsobjekte (insgesamt gibt es mehr als 800) mit entsprechenden Ausprägungen der Steuerungsfelder, über die die Zugriffe auf die SAP-Ressourcen gesteuert werden, somit also z.B. Aktionen auf Belege (Buchen, Anzeigen, Ändern), Transaktionen und Gruppenzugriffe (Benutzergruppen, Tabellen etc.). Grundsätzlich ist das Profil und seine Unterordnung das Hauptkriterium für den Revisor, da hier die Verbindung zum Berechtigungsobjekt und zur konkreten Ausprägung des Zugriffs geschaffen wird. SAP lässt für die Bezeichnung eines Profiles nur bis zu zehn Zeichen zu.

Die wichtigsten Prüftabellen für Profile sind die folgenden:

Tabelle	Beschreibung
UST12	Objekte und Ausprägungen je Profil
UST04	Profile pro SAP-Nutzer
UST10S	Profile mit Objekt und Berechtigung
UST10C	Sammelprofil mit zugehörigen Profilen
USR11	Texte zu den Profilen

Tab. 2: Tabellen zur Prüfung im Bereich Profile

Profilgenerator

Der Profilgenerator (PFCG) ist als Erleichterung bei der Definition von Berechtigungsstrukturen für die Administration gedacht. Ziel ist die Bereitstellung eines Tools zur Generierung von Berechtigungen und der gleichzeitigen zentralen Ablage der definierten Strukturen nebst Nutzer-Zuweisung. Der Profilgenerator arbeitet in der Form, dass sich der Administrator entweder direkt die notwendigen Berechtigungsobjekte mit entsprechender Ausprägung der Steuerungsfelder oder durch Menübäume die notwendigen SAP-Funktionen auswählt, woraufhin der Profilgenerator die benötigten Berechtigungsobjekte, Transaktionscodes etc. automatisch übernimmt. Die Ablage erfolgt in einem Profil, welches genau einer Aktivitätsgruppe zugeordnet ist. Sofern z.B. buchungskreisabhängige Komponenten bereitgestellt werden müssen, ist die Generierung mehrerer Profile unter einer Aktivitätsgruppe jedoch ohne weiteres möglich. Sofern der Administrator keine Änderungen vornimmt, schlägt der Profilgenerator einen Standard-Profilnamen vor und vergibt ihn automatisch mit fortlaufender Nummerierung.

Typische Ist-Situation

Häufig findet man in Unternehmen - insbesondere durch die schwache personelle Ressourcenversorgung im administrativen Umfeld und die große Anzahl von Systemen (Test/Integration, Qualitätssicherung, Produktion für Classic und HR getrennt, ggf. IS-Module getrennt, jeweils mit eigenen Basis-Komponenten etc.) - eine mehr "kreative" (d.h. unstrukturierte, undokumentierte, vorgabenlose und verfahrensablauftechnisch unzureichende) Berechtigungsverwaltung vor, die oft gipfelt in einer Vielzahl von Verwaltungsobjekten, d.h.

- mehrere tausend Aktivitätsgruppen
- mehrere tausend Profile
- geringfügige Anzahl von genutzten Sammelprofilen
- mehrere zehntausend Zuweisungen von Profilen zur Gesamt-SAP-Nutzer-Zahl.

Ein typisches Beispiel für die Abbildung in einem Unternehmen zeigt die folgende Darstellung:

Betrachtungsgegenstand	Anzahl z.B.
SAP-Nutzer	(pro) 1.000
Aktivitätsgruppen	ca. 2.000 - 2.500
Profile	ca. 2.500 - 3.000
Profilzuweisungen zu SAP-Nutzern	ca. 120.000
kaum Nutzung von Sammelprofilen als Strukturgeber	
Profile/AktGr werden über Profilgenerator erstellt	
kaum Pflege der Texte zu Profilen und Aktivitätsgruppen	
Differenz AktGr. zu Profilen über Direktzuweisung	
somit durchschnittliche Anzahl von Profilen pro SAP-Nutzer	etwa 120

Tab. 3: Zahlenbeispiel - Typisches Ist in einem Unternehmen

Eine derartige Ist-Situation führt zu erheblichen Fehlerquellen in den Verfahrensabläufen der SAP-Berechtigungsvergabe. Welche Gründe führen aber zu einer solchen Ausgestaltung ?

Häufige konzeptionelle Schwächen

Kleinstprofile

Profile sollten wie oben erwähnt als Arbeitsschritt- oder Tätigkeitsabbildung der Mitarbeiter in SAP gesehen werden. Hier sind die notwendigen Berechtigungsobjekt- und Transaktionscodeeingrenzungen vollständig enthalten.

Es ist jedoch oftmals feststellbar, dass Profile jeweils als "Kleinstprofil" definiert werden, d.h. sie beinhalten lediglich wenige Berechtigungsobjekte mit einer bestimmten Ausprägung (z.B. Modul CO: Bestimmte Ausprägung in K_VRGNG [erlaubte Vorgänge in der Kostenrechnung, Ist-Buchung, Verrechnung] zusammen mit einer Transaktionscodezuweisung in S_TCODE). Dieses modulübergreifende Zerstückeln

von zusammengehörigen Berechtigungsobjekten zu den vorgenannten Kleinstprofilen führt dazu, dass oftmals redundante Profile definiert werden. Die häufige Erklärung lautet, dass der zuständige Moduladministrator für eine im Fachbereichsinteresse liegende schnelle Lösung zu sorgen hat. Also wird das benötigte Delta ermittelt, ein Profil hieraus generiert und dem Mitarbeiter zugewiesen. Dass ggf. ein solches Profil oder eines mit einer minimalen Variation bereits existiert, konnte er dann in der Zeit nicht erkennen. Somit erfolgt fast ausschließlich eine Orientierung der Profildefinition an den SAP-Objekten und nicht an Aufgabenabbildungen.

Diese Kleinstprofile führen dazu, dass Mitarbeiter Berechtigungen über eine Vielzahl von Profilen und damit über eine redundante Berechtigungsobjektzuweisung erhalten, die beispielsweise den Entzug einer Berechtigung (z.B. bei Wechsel des Mitarbeiters in einen anderen Fachbereich) massiv erschweren, da erst ermittelt werden muss, welche Profile die Berechtigung zur Verfügung stellen. Zu beachten ist, dass die umfangreichste Berechtigungsobjekteingrenzung in den zugewiesenen Profilen des Mitarbeiters die Berechtigung definiert, gleichgültig, aus welchen Profilen sie stammt. So erhält ein Mitarbeiter eine Berechtigungsobjektzuweisung in Variationen über zwischen zwei und mehr als zehn Zuweisungen. Als Beispiel wird der folgende Block dargestellt (tatsächlich vorgefundenes Ist in einem Unternehmen).

Beispiel einer extremen Minimierung einer Profildefinition - buchungskreisabhängige Trennung:

F_BKPF_BUK	Buchhaltungs-belege	Berechtigung auf Buchungskreise
ACTVT BUKRS	03 0100	Anzeigen

Diese Ausgestaltung ist in neun Profilen definiert. Sie werden mit anderen Profilen in Kombination vergeben, die dann die entsprechend anderen F_BKPF-Berechtigungsobjekte beinhalten. Die Beschreibung dieser neun Profile sieht wie folgt aus:

FI Beleg Anzeigen Buchungskreis 0100
FI Dauerbeleg Anzeigen Buchungskreis 0100
FI Debitoren Konto Posten anzeigen Buchungskreis 0100
FI Debitoren Konto Salden anzeigen Buchungskreis 0100
FI Konto Posten anzeigen Buchungskreis 0100
FI Konto Salden anzeigen Buchungskreis 0100
FI Musterbeleg Anzeigen Buchungskreis 0100
FI Vorerfasste Belege Anzeigen Buchungskreis 0100
MM Rechnungsprüfung anzeigen Buchungskreis 0100

In etwa der selben Anzahl bestehen Profile, die beim Berechtigungsobjekt F_BKPF_BUK die Ausgestaltung ACTVT 03 (Anzeige) und BUKRS * (alle Buchungskreise) bzw. wiederum in etwa der selben Anzahl Profile mit der Ausgestaltung ACTVT 01,02,03,06,08,77 (Hinzufügen, Ändern, Anzeigen, Löschen, Änderungsbelege anzeigen, Vorerfassen) und BUKRS 0100 aufweisen.

Kombinationsprofil

Sofern solche wie zuvor dargestellten Profile in einer hohen Anzahl und in einer solchen Minimalausprägung in allen Modulen vorhanden sind, dienen sie als Kombinationsprofile. Sie definieren also allein nicht zwangsläufig eine kritische Ausprägung, können jedoch im Zusammenspiel mit anderen Profilen kritische Ausprägungen beinhalten. Insofern ist eine Prüfung von kritischen Ausprägungen hier ausgesprochen schwierig, da ja erst das Zusammenspiel mehrerer Berechtigungsobjekte mit einer jeweils bestimmten Ausprägung, ggf. zusätzlich mit einem Transaktionscode, kritische Ausprägungen darstellen.

Profilname	Berechtigungsobjekt	Aktivität	KoKrs	Vorgang CO
T-67011111	K_VRGNG	02	0100	RKL, RKLU
keine weiteren Berechtigungsobjekte				CO-Leistungsverrechnung
oder		Aktivität	WERKS	
T-67022222	M_MRES_WWA	01,02,06	*	Reservierung .anl./änd./löschen
keine weiteren Berechtigungsobjekte				alle Org.-ebenen Werk

Tab. 4: Beispiele für Profile mit nur einem Berechtigungsobjekt, oftmals redundant vorhanden

Für den Revisor ist immer wichtig zu erfahren, aus welchen Quellen kritische Berechtigungen stammen. Die Abfrage im AIS (SECR) "Zeige alle Profile, die eine bestimmte Berechtigungsobjektkombination [mehrerer Objekte] beinhalten" führt zu einem fehlerhaftem Ergebnis, da nur die Profile gezeigt werden, die die gesamte Ausgestaltung aufweisen. Er kann somit nur nach den Mitarbeitern dieser Kombination suchen und muss sich mühsam an die beteiligten Profile "herantasten".

Bei einer solchen Vergabe ist die Kombinationsmöglichkeit dieser Profile derart hoch, dass das Identifizieren der Schwachstellen und somit das Eindämmen von kritischen Berechtigungen mit einem unverhältnismäßig hohen Aufwand verbunden ist. Das hier dargestellte Aufblähen der Profillandschaft (ein nahezu identisches Bild wird auch bei den Aktivitätsgruppen geliefert, da alle hier aufgeführten Profile über den Profilgenerator aufgebaut wurden und entsprechende Aktivitätsgruppenzuweisungen aufweisen) führt im Laufe der Zeit zur vollständigen Intransparenz, da eine Prüfung zur Bereinigung nicht mehr möglich ist - Redundanz ist normal und aufgrund der Komplexität kaum noch zu verhindern.

Konsequenz des Ansatzes

Der vorgenannte Ansatz verleitet dazu, dass Berechtigungsdeltas schnell und unkompliziert eingespeist werden. So entsteht ein nahezu 1:1-Verhältnis zwischen Profilen und Aktivitätsgruppen bei einer unverhältnismäßig hohen Anzahl dieser Elemente. Der Struktureffekt geht verloren. An seine Stelle tritt jedoch ein anderer, der die Konsequenz der vorgenannten Punkte beschreibt: Mitarbeiter erhalten trotz nahezu identischer Aufgaben keine identischen Berechtigungszuweisungen. Im Laufe der Zeit ergibt sich eine "Individualisierung der Berechtigungsvergabe". Diese führt letztlich zu mehr Aufwand bei der Beantragung für neue Mitarbeiter durch den Fachbereich, bei der Administration, und natürlich auch bei der Prüfung. Der Grundgedanke, Berechtigungsstandards zu bilden und Deltas nur in geringer Anzahl zuzulassen, ist so nicht durchzuhalten.

Zwei Möglichkeiten der Ausgestaltung

Erkennbar ist, dass die Ausgestaltung der Berechtigungskonzeption mit einer überwiegenden Orientierung an den SAP-Objekten (mitarbeiterabhängige Delta-Ermittlung und -Zuweisung) nicht zwangsläufig sinnvoll ist, d.h. eine betriebswirtschaftliche Funktionsorientierung ist hierdurch vor dem Hintergrund der Beurteilungskriterien nicht abbildbar.

Die nachfolgenden beiden Gestaltungsmöglichkeiten bieten Chancen zur Bereinigung der vorgenannten Schwächen. Es sind die beiden meistgenutzten Ansätze zur Implementierung eines Berechtigungskonzeptes.

Aufgaben-/Funktionsbezogene Gruppierung

Die aufgaben-/funktionsbezogene Gruppierung stellt die aus den Arbeitsplatzbeschreibungen abgeleiteten Aufgaben in den Vordergrund und lagert diese als SAP-Abbild identifizierten Beschreibungen in Profile aus. Auf Aktivitätsgruppenebene werden diese Aufgaben zusammengefasst und als Stellen- oder Funktionsbeschreibungen abgelegt. Der Vorteil hierbei ist, dass Profile als Abbild von Aufgaben diese vollständig definieren und fachbereichsübergreifend genutzt werden können. Sammelprofile können als Sammler/Bündelungen von Aufgabenabbildungen flankierend wirken.

Beispiel:

- Anfragen anlegen/ändern	alleinige Funktion des Einkäufers
- Anfragen anzeigen	verwendbar auch in anderen Fachbereichen
- Bestellungen anlegen/ändern	alleinige Funktion des Einkäufers
- Bestellungen anzeigen	verwendbar auch in anderen Fachbereichen
- Rahmenverträge anlegen/ändern	alleinige Funktion des Einkäufers
- Rahmenverträge anzeigen	verwendbar auch in anderen Fachbereichen
- Buchhaltungsbelege anzeigen	etc. verwendbar auch in anderen Fachbereichen

Der Einkäufer als zentrale Beschaffungsinstanz muss in seinem Arbeitsumfeld eine Vielzahl an Aufgaben/Tätigkeiten ausführen, so z.B. die folgenden:

Diese Tätigkeiten sind eindeutig zu identifizieren und auch eine Abbildung der SAP-Funktionlität ist mög-

lich. Notwendig ist die Definition der Aufgabenabdeckung auf Profilebene, die sowohl die Eingrenzung der Berechtigungsobjekte als auch der Transaktionen bedeutet.

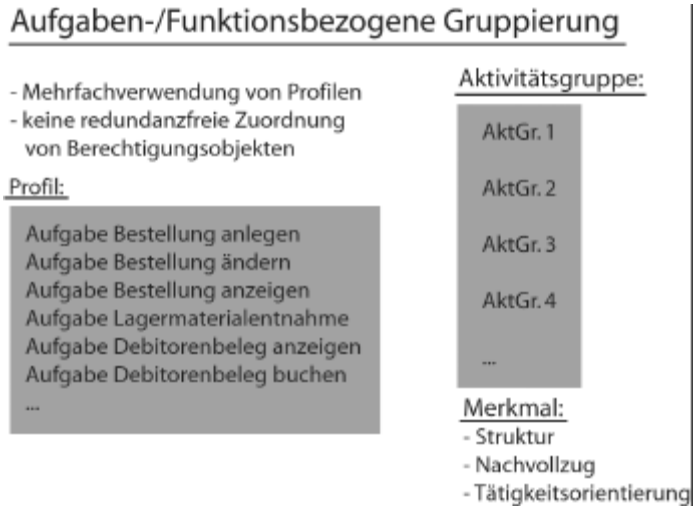
Beispiel Bestellung anzeigen:

Profildefinition:

Berechtigungsobjekt	Steuerungsfelder	Eingrenzung
M_BEST_BSA	ACTVT / BSART	03 / *
M_BEST_EKO	ACTVT / EKORG	03 / *
M_BEST_EKG	ACTVT / EKGRP	03 / *
M_BEST_WRK	ACTVT / WERKS	03 / *
S_TCODE	TCD	ME23 u.a.

Hier sind alle zusammengehörigen Berechtigungsobjekte auch gemeinsam definiert. Ein solches Profil kann auch in anderen Bereichen als Einzelaufgabeabbildung genutzt werden, so dass redundante Profile nicht entstehen sollten.

rung ist nur dort denkbar, wo die Anzahl genau abgegrenzter Aufgaben überschaubar und feststellbar ist, woraus sich wiederum klare Berechtigungseingrenzungen ableiten lassen, d.h. wo die Abbildung der Aufgaben/Tätigkeiten in SAP-Funktionen/Berechtigungsobjekte und den entsprechenden Steuerungsfeldereingrenzungen nebst Transaktionscodes unkompliziert erfolgen kann. Vor allem aber muss diese Abgrenzung von jemandem durchgeführt werden.



Die Aufgabe der genauen Tätigkeitsanalyse der Stellen liegt zwar grundsätzlich im Interesse aller Fachbereiche, wird jedoch im Vorfeld der Berechtigungskonzeption kaum ausreichend durchgeführt. Eine genaue Aufgabenbeschreibung der Fachbereichsmitarbeiter und hieran gespiegelt die Abbildung der Aufgaben in SAP-Funktionalität ist ein schwieriger und langwieriger Pro-

Vorteile	Nachteile
Eindeutige Aufgabenbeschreibungen und Abbild in SAP möglich	Redundante Berechtigungsobjektzuweisungen über mehrere Profile
Bausteinsystem ermöglicht Verwendung der Profile fachbereichsübergreifend; sehr strukturiert gut umsetzbar in Unternehmen kleiner und mittlerer Größe	Notwendig ist die vollständige Identifikation und Analyse der Aufgaben bei den Mitarbeitern und Abbildung in SAP => **kaum leistbar ab einer bestimmten Mitarbeiter- und Aufgabenanzahl (Funktionstrennungsprinzip)**
Identifikation der Profile schnell möglich, Sammelprofile können optimierend wirken	Analyse der beteiligten Berechtigungsobjekt Transaktion, adaptiert auf die Aufgabenbeschreibungen => **langwieriger Prozess**
Zuweisung und Entzug von Funktionalität schnell und unkompliziert	**Keine Reduzierung der Profilanzahl, ergibt zwar Struktur und ggf. Übersicht, ist jedoch zunehmend kaum administrier- und prüfbar**

Tab. 5: Vor- und Nachteile der aufgaben-/funktionsbezogenen Gruppierung

Darstellung des Berechtigungskonzeptansatzes:

Ein entscheidender Nachteil ist hiermit verbunden, der hier nochmals herausgestellt werden muss. Der Ansatz der aufgaben-/funktionsbezogenen Gruppie-

zess. Diesem entziehen sich die Fachbereiche mangels Kapazität und Fachkompetenz sehr häufig. Eine Standardisierung erfolgt somit meist über den Berater oder den IT-Dienstleister selbst - beide mit zu wenig Sach-

kompetenz in den Prozessen ausgestattet, um die Konsequenzen einer Definition für die Mitarbeiter in den Fachbereichen abzuschätzen - "quick&dirty"-Lösungen wird wieder Vorschub geleistet, die Anzahl der Profile wird nicht geringer. Der theoretische Ansatz ist m.E. positiv zu sehen, Erfahrungen haben jedoch gezeigt, dass er langfristig nicht durchzuhalten ist - zumindest nicht in größeren Unternehmen. Die Beurteilungskriterien werden bei hohem Gefahrenpotential nur bedingt erfüllt.

Beispiel "zentraler Einkaufssachbearbeiter":

Profildefinition:

Im Profil finden sich modulübergreifend und redundanzfrei ca. 150 Berechtigungsobjekte nebst Steuerungsfeldeingrenzung wieder, die alle Zugriffsdefinitionen dieser Stelle abbilden. In Zusatzprofilen werden z.B. buchungskreisabhängige Berechtigungsobjekte in die Gesamtberechtigung integriert.

F_BKPF_BED	ACTVT	03	BRGRU	*
F_BKPF_BEK	ACTVT	03	BRGRU	*
F_BKPF_BES	ACTVT	03	BRGRU	*
F_BKPF_BLA	ACTVT	03,08	BRGRU	*
F_BKPF_BUK	ACTVT	03,08	BUKRS	0100
F_BKPF_BUP	BRGRU	*		
F_BKPF_GSB	ACTVT	03	GSBER	*
F_BKPF_KOA	ACTVT	03	KOART	*
F_LFA1_AEN	VGRUP	*		
F_LFA1_APP	ACTVT	01,02,03,05,06,08	APPKZ	M
F_SKA1_BES	ACTVT	03	BRGRU	*
F_SKA1_BUK	ACTVT	03	BUKRS	0100
F_SKA1_KTP	ACTVT	03,08	KTOPL	*
M_BEST_BSA	ACTVT	01,02,03,04,06,08,09,76	BSART	AAA-GAZ, GCA-ZZZ
M_BEST_EKG	ACTVT	01,02,03,04,06,08,09,76	EKGRP	<Einkaufsgruppe>
M_BEST_EKO	ACTVT	01,02,03,04,06,08,09,76	EKORG	<Einkaufsorganisation>
M_BEST_WRK	ACTVT	01,02,03,04,06,08,09,76	WERKS	<Werkseingrenzung>
M_RAHM_BSA	ACTVT	01,02,03,04,06,08,09	BSART	*
M_RAHM_EKG	ACTVT	01,02,03,04,06,08,09	EKGRP	<Einkaufsgruppe>
M_RAHM_EKO	ACTVT	01,02,03,04,06,08,09	EKORG	<Einkaufsorganisation>
M_RAHM_WRK	ACTVT	01,02,03,04,06,08	WERKS	<Werkseingrenzung>

Tab. 6: Auszug aus dem zentralen Einkäuferprofil für BUKRS 0100

Stellenbezogene Gruppierung auf Profilebene

Eine Alternative bietet die stellenbezogene Gruppierung auf Profilebene. Dieser Ansatz stellt das Profil - wie dies in vielen Unternehmen der Fall ist - in den Vordergrund als höchstes Ordnungskriterium. Die Aktivitätsgruppe wird nur als Beschreibungselement genutzt.

Das Entscheidende an diesem Ansatz ist, auf Profilebene eine komplette Stelle mit allen Aufgaben/Tätigkeiten/Funktionen abzubilden und so für eine Standardisierung zu sorgen. Definiert wird ein zentrales Stellenprofil, welches unterstützt wird durch wenige Zusatzprofile, die lediglich customizingabhängige Zusätze beinhalten. So werden beispielsweise zusätzliche buchungskreis- und kostenrechnungskreisabhängige Komponenten über Zusatzprofile bereitgestellt.

Bei diesem Ansatz überwiegen die Vorteile sowohl für den Fachbereich als auch für die Administration und die Revision.

Es wäre wünschenswert, wenn Fachbereiche ihre Funktionen/Stellen sowohl prozess- also auch tätigkeitsorientiert analysieren würden, um hieraus Tätigkeiten und bündelnde Rollen abzuleiten, die dann in SAP-Funktionalität adaptiert werden. Entscheidend ist jedoch, dass Fachbereiche bestrebt sein müssen, Standardisierungen der Funktionsabdeckung/Aufgabenwahrnehmung zuzulassen und der Individualisierung der Berechtigungen entgegenzuwirken. Dies schließt insbesondere auch Zugriffe im Modul CO ein. Notwendig ist also die Vermeidung der Vergabe von Rechten als Statussymbol für bestimmte Mitarbeiter und stattdessen die Rechtezuweisung nach Notwendigkeit in den Hauptprofilen für Mitarbeitergruppen mit identischen Tätigkeiten.

Vorteile	Nachteile
Vollständig nutzbare Rollendefinitionen, Abgrenzung von anderen Rollen, lässt gewisses Maß an Flexibilität zu, unterbindet aber Profilwildwuchs	Administration ist modulübergreifend, d.h. die Administratoren müssen modulübergreifende Kenntnisse besitzen bzw. eng zusammenarbeiten
Bei Änderungen/Zusätzen in der Berechtigung wird das zentrale Rollenprofil angepasst und kein Zusatzprofil definiert	Es bestehen wieder in etwa so viele Aktivitätsgruppen wie Profile, aber siehe Vorteile letzter Punkt !
Redundanz in den Profil- und Berechtigungsobjektzuweisungen nur dort, wo systembedingt notwendig (z.B. K_CCA, K_VRGNG)	Sammelprofilen kommt eine eher untergeordnete Funktion zu
Berechtigungsobjekt definiert zentral im Hauptprofil der Rolle einmalig den höchsten notwendigen Berechtigungswert	Übersicht im Profil ist leicht eingeschränkt
Zusatzprofile nur für steuerungsfeldabhängige Komponenten (BUKRS, KOKRS, EKGRP etc.)	
Optimiertes Beantragungswesen, Fachbereich muss nur die wenigen Profile seiner Rollen und ihre Beschreibung (AktGr.) kennen	
Optimierte Administration durch geringe Anzahl an zu verwaltenden Objekten	
Bei Rollenerweiterungen schnelles und unkompliziertes Handling	
Erheblich geringere Anzahl von Profilen; in einem üblichen größeren Unternehmen dürften nur etwa 300-500 Hauptprofile entstehen	

Tab. 7: Vor- und Nachteile der stellenbezogenen Gruppierung auf Profilebene

Darstellung des Berechtigungskonzeptansatzes:

Schlussbetrachtung

Gerade der Ansatz der stellenbezogenen Gruppierung auf Profilebene, der m.E. zu favorisieren ist, kann als das geeignete Beispiel für die Abbildung in größeren Unternehmen gesehen werden, wo Mitarbeiter keine weitgefächerten, sondern eingegrenzte und genau beschriebene Tätigkeitsabbildungen zugewiesen bekommen. Der Wildwuchs an Profilen kann hierüber eingedämmt werden.

Unter www.wildensee.de/veroeff.htm kann eine funktionstüchtige Muster-Rollendefinition eines Einkaufssachbearbeiters heruntergeladen werden, die - customizing-abhängige Einstellungen vorausgesetzt bzw. angepasst - lauffähig vorliegt.

Ausgesuchte Literatur:

Christoph Wildensee:

Ausgesuchte Berechtigungsobjekte des SAP R/3 - Systems als Prüfungsansatz für die IV-Revision - Eine Übersicht - Teil 1 bis 3 für Basis, FI & CO ReVision III/2001 bis I/2002, Ottokar-Schreiber-Verlag, Hamburg http://www.revision-hamburg.de

Thomas Tiede SAP R/3 Ordnungsmäßigkeit und Prüfung des SAP-Systems (OPSAP) 2000 Ottokar-Schreiber-Verlag, Hamburg http://www.osv-hamburg.com

Revision des Entwicklungsprozesses von Anwendungssoftware

Von Dipl.-Ing. Paul Rieckmann
wissenschaftlicher Angestellter der Freien und Hansestadt Hamburg

Entwicklungsprozesse zeichnen sich durch relativ offene Zielvorgaben und Verlaufsformen aus. Lassen sich Entwicklungsprozesse dann nur visionieren und nicht revisionieren? Entwicklungsprozesse sind kreativ und methodisch immer in einem bestimmten Gestaltungsfreiraum. Revisionen sind dagegen eher striktere Soll-Ist-Abgleiche und grenzen Freiräume bewusst ein, um den erforderlichen Freiraum herauszuarbeiten.

Ex-Ante-Revisionen in Entwicklungsprozessen von Anwendungssoftware können daher leicht in sich verschränkende wie unproduktive Frontstellungen von kreativer Freiraumsuche zu einengender Prüfung hineingleiten. Eine mögliche Lösung liegt in einem für beide Seiten verbindlichen Vorgehensmodell der Softwareentwicklung. Diese methodische Schnittstelle von Entwicklung und Prüfungsgrundlage kann beiden Seiten in ihren jeweiligen Zielen behilflich sein: Ein Optimum an Entwicklungsfreiräumen und ein hinreichender methodischer Prüfrahmen für einen Soll-Ist-Abgleich eines verbindliche Verfahrensmodells, statt einer bloßen Vision

1. Revision von risikoreichen IT-Projekten

Projekte zur Entwicklung neuer Anwendungssoftware oder zur Implementierung anzupassender Standardsoftware dienen i.d.R. der Rationalisierung und Automatisierung bestimmter Geschäftsvorfälle. Effizienz und Effektivität des Outputs und Stärkung der Marktposition reflektieren sich in zunehmend in IT-vermittelten Kreislaufprozessen der Produktion, des Vertriebs, des Einkaufs, des kaufmännischen Rechnungswesens, der Werbung und des Vertriebs. Projekte sind daher i.d.R. IT-Projekte. Die projektbegleitende Revision hat aus diesen Gründen eine zunehmende Bedeutung. In diesem Text liegt der Schwerpunkt in der Ex-Ante-Projektprüfung eines Entwicklungsprozesses im Bereich der Anwendungssoftware.

Projekte - insbesondere IT-Projekte - haben sich in verschiedenen Untersuchungen als stark risikoreich erwiesen. Das Risiko verteilt sich dabei nicht einfach auf einem hohen Anteil tolerabler und einem geringen Anteil ruinöser Risikoentwicklungen. Wenn Untersuchungen von IT-Projekten Anteile von bis zu 50% gescheiterter Vorhaben aufweisen, ist erstens der Anteil des eingetretenen Ruinrisikos zu hoch und zweitens ist davon auszugehen, dass nur ein kleinerer Teil der IT-Projekte einen vollen Erfolg darstellen, weil für die nicht gescheiterten Projekte eine Differenzierung der Bewertung zwischen vollen und ausreichendem Erfolg zu unterstellen ist.

2. Softwareentwicklungsprozesse das Vorgehensmodell als Soll-Grundlage

Besonders risikoreich sind in jedem Fall IT-Projekte mit der Entwicklung und Implementierung einer neuen Anwendungssoftware in Unternehmen und Institutionen, da Erfahrungen und Tests aus anderen Anwendungen wesentlich begrenzter als bei Standardsoftwarelösungen genutzt werden können. Zudem sind in diesen Fällen fehler- und risikobehaftete Leistungskataloge in Pflichtenheften neu zu entwikkeln. D.h., zwischen den Zielen der gesuchten Anwendung und den Möglichkeiten der Softwareentwicklung können sich größere Diskrepanzen ergeben.

Festzuhalten bleibt, dass ein Softwareentwicklungsprozess mit einem individuellen Produkt ein besonders hohes Ruinrisiko haben dürfte. Der Ruin oder das Scheitern kann sich aus einem mangelhaften Antwortzeitverhalten, aus der nicht möglichen Migration von Daten aus der zu übernehmenden Software ergeben, da die ältere Software häufig nicht hinreichend dokumentiert wurde, aus der Darstellung zu komplexer Vorhaben usw. ergeben.

Bei Entwicklungsprozessen individueller Anwendungssoftware ergeben sich IT-Projektrevisionen, die offensichtlich eine Grenzsituation für Interne Revisionen bedeutet:

Die IR soll in der unterstellten Konstellation ohne hinreichende IT-Fachkenntnisse und insbesondere ohne Kenntnisse der Programmierung einen komplexen Softwareentwicklungsprozesse revidieren.

Die unmittelbare Frage lautet: Ist eine Revision ohne spezielle SW-Kenntnisse in der Lage eine solche Prüfung durchzuführen? Bei näherem Zusehen dürfte deutlich werden, dass hier - wie in vielen anderen Fällen - sich ein methodischer Weg durch Anwendung geltender Normen anbietet. Fehlen der Revision fachliche Grundkenntnisse, werden als Grundlage i.d.R. geltende Arbeits- und Entwicklungsnormen gewählt - z.B. die Grundsätze ordnungsgemäßer Buchführung. Auf dieser Basis lassen sich vorgegebene Wege, Ergebnisse, Methoden, Ziele usw. ohne vollständige inhaltliche Grundkenntnisse des Prüffeldes prüfen.

Im Bereich der Softwareentwicklung haben sich verschiedene Vorgehensmodelle[1] als anwendbare Normen ergeben. Das Vorgehensmodell beschreibt die Aktivitäten und Produkte, die während der Entwicklung von Software durchzuführen bzw. zu erstellen sind. Für die Revision der Entwicklung von individueller Anwendungssoftware kann ein Vorgehensmodell der Softwareentwicklung gewählt werden. Dies ermöglicht einmal eine Prüfung des vorgesehenen Ablaufmusters wie der Ablaufelemente und zweitens ergeben sich inhaltliche Prüfansätze auf der Ebene des Pflichtenheftes.

Die Vorteile eines solchen Vorgehens liegen in der Möglichkeit einer mehr formalen und die Nachteile liegen in der nicht inhaltlichen Prüfung (der Codes) einer Softwareentwicklung. Die vorgegebenen Ziele und Vorgehensweisen des Soll-Verfahrens können auf Umsetzung und Realisation geprüft werden. Die sich ergebenden Abweichungen zwischen Ist und Soll verweisen dann auf Risiken, wenn es sich um negative Abweichungen, und auf Chancen, wenn es sich um positive Abweichungen handelt.

Da Revisionen i.d.R. Soll-Ist-Abgleiche beinhalten, wäre eine aufwendige wie fragwürdige Prüfung von Codes ohnehin nicht zu empfehlen. Der Prüfungsschwerpunkt sollte sich dagegen auf vorgegebene Soll-Verfahren beziehen. Diesem vorgegebenen Soll ist in einem Abgleich ein geprüftes Ist-Verfahren gegenüber zu stellen. Für die Prüfung der Entwicklung einer Anwendungssoftware kann als vorgegebenes Soll ein Vorgehensmodell gewählt werden. Liegt kein vereinbartes Vorgehensmodell für die Softwareentwicklung vor, sollte die Revision im Rahmen der Prüfung selbst ein Vorgehensmodell als Grundlage auswählen und dieses f. mit den zu prüfenden Stellen abstimmen.

Ein Vorgehensmodell (V-Modell) zerlegt den SW-Entwicklungsprozess in funktionale Prozessphasen, definiert Aktionen und Produkte / Ergebnisse und fixiert den Phasenwechsel durch verbindliche Übergänge. Wir können unter Teileinbeziehung[2] des Projektmanagement (PM) vier Phasen definieren:

1. Phase	Anforderungs-analyse	Übergänge durch Soll-Konzepte
2. Phase	Softwareent-wicklung	Übergänge durch Prototypen
3. Phase	Testphasen	Übergänge durch Qualitäts-prüfungen
4. Phase	Produktiv-setzung	Übergänge durch Optimierung

Funktion eines V-Modells - Das Vorgehensmodell ermöglicht den Schritt von chaotischer Software-Bastelei zur genormten Software-Produktion. Die Kreativität der Programmierung wird nicht direkt berührt. Die Programmierung erhält einen organisatorischen Rahmen vorgegebener Phasen und Übergänge.

System- und Prozessansatz des V-Modells - Ein unstrukturiertes Vorgehen ist bei Quick & Dirty-Wegwerf-Software auf der Ebene von vereinzelten Teilprozessen tolerierbar. Bei komplexen SW-Systemen, die Kern- und Unterstützungsprozesse von relevanten Geschäftsprozessen einbeziehen und später einer optimierenden Wartung und Weiterentwicklung unterliegen, hat ein unsystematisches Vorgehen hohe Risiken mit entsprechend hohen Schäden zur Folge.

Negative Systemabweichungsregel des V-Modells: Das Fehlen oder Nichtbefolgen eines Vorgehensmodells bedeutet, dass der Software-Entwicklungspro-

zess nicht beherrscht wird und dass Risiken statt Chancen optimiert werden.

3. Zur Praxis der Softwareentwicklung

Zur Beachtung - der fixe Softwareschein oder die Scheinheiligkeit der Masken

Im Unterschied zur Produktion eines Autos liegt die Krux der Software-Entwicklung in der Möglichkeit, Produktänderungen vorzunehmen, die auf der Ebene des Anwenders - den Masken - nicht sofort sichtbar werden.

Die Windows-Masken sind i.d.R. SW-Tools entnommen und lassen sich relativ schnell durch Anpassung programmieren. Die eigentliche Programmierarbeit lauert jedoch hinter den Masken und betrifft die Verknüpfungsebene zwischen Masken und Programmierung der eigentlichen Work- und Dataflows der jeweiligen Geschäftsprozesse. Deshalb sollten Revisionen ihr Hauptaugenmerk auf die Testmethodik und Testergebnisse legen, weil auf dieser Ebene die Soll-Ziele mit den Ist-Ergebnissen abgeglichen werden können.

Testorientierung statt Maskenfixierung

- ✓ Der Zeitaufwand für das Programmieren von Anwendungsmasken sinkt,
- ✓ gleichzeitig steigt der Aufwand für das Programmieren der Zwischenebene bei Anwendungsmasken und den Work- und Dataflows mit der Komplexität der einbezogenen Geschäftsprozesse (E-Commerce, Intranet, Content-SW usw.)
- ✓ und es steigen die bekannten und unbekannten Bugs mit der Komplexität und Anwenderfreundlichkeit der SW-Entwicklungsumgebung,
- ✓ so dass die erforderliche Zeit für notwendige Testläufe massiv steigt.

Das Risiko der unentwegten SW-Bastelei

Risiko der unsichtbaren Änderungen: Die SW-Entwicklungsumgebung gestattet es in der Regel, bis zum letzten Moment an dem Produkt zu ändern, ohne dass man es diesem auf der Anwendungsebene direkt ansieht.

Abweichungsrisiko durch die SW-Entwickler: Dies führt in dynamischen Prozessen zu risikoreichen Abweichungshandlungen der SW-Entwickler.

Risiko der Maskenfixierung: Insbesondere wenn SW-Laien sich von halbgaren Masken (weil die relevanten Verknüpfungen bis dato fehlen) beeindruckt zeigen, steigen die IT-Projektrisiken massiv an.

Ebene von Fehlermeldungen: Dies - z.B. bei MS Access (VBA) - würde den Rahmen der Darstellungsmöglichkeiten sprengen.

Zur Bedeutung individueller Anwendungsprogramme

Software im Sinne von individuellen Anwendungsprogrammen gewinnt durch zwei Entwicklungslinien eine größer werdende Bedeutung:

A. Zum einen werden praktisch alle Facetten der komplexer werdender Geschäftsprozesse durch IT-Technik rationalisiert. D.h., neben übergreifender Software wie SAP R/3 steigt das Bedürfnis für Anwendungsprogramme in den so genannten Nischen oder in Sonderbereichen. Zudem erweisen sich individuelle Programme häufig als preiswerter und es existieren enge bis örtliche Beziehungen zwischen dem Anwender und dem SW-Produzenten.
B. Zum anderen ermöglichen moderne SW-Entwicklungsumgebungen eine schnellere Entwicklung von Anwendungssoftware im Rahmen komplexer werdender SW-Systeme.

4. Zunahme von Chancen und Risiken

Diese Entwicklung führt zu einer risiko-chancen-reichen Komplexitätshäufung:

- ➢ Die eigentlichen Ausgangspunkte in den Geschäftsprozessen werden durch eine globale, nationale, regionale und interne Vernetzung komplexer.
- ➢ Zugleich steigt die Komplexität der IT-Entwicklungsumgebung und der entwickelten und angewandten Programme im Rahmen der vernetzten Betriebssysteme und damit die Fehlerhäufigkeit der erstellten Programme. Die produzierten Anwendungsprogramme werden durch eine komplexe Entwicklungsumgebung - moderne Sprachen, Unterstützungsprogramme usw. - und durch ihre Einbindung in ein größer werdendes SW-Gesamtsystem - Betriebssysteme, Internet, Intranet, unterschiedliche Plattformen (MS, Java, C++ usw.) - zugleich schneller produzierbar wie als Produkt komplexer.

Die Entwicklung spezifischer wie individueller Software zur Steuerung, Unterstützung und Abwicklung ausgewählter Geschäftsprozesse wird angesichts immer kürzerer Produktzyklen, komplexerer Prozesse, SW-Entwicklungstools usw. sowohl erleichtert, als zugleich erschwert. Folgender Widerspruch ist das akute Kennzeichen der Softwareentwicklung:

Je leichter die eigentliche Programmierung fällt, desto höher sind die Fehlerquoten. Je schneller Module z.B. als Masken erstellt sind, umso länger wird die Testphase zur Eliminierung der zwangsläufig auftretenden Fehler. Als Beispiel sei hier auf die eingängige Access-Programmierung verwiesen. Die vielen bekannten VBA-Bugs sind für eine Fehlereinschätzung zu exponieren. D.h., kein neues Programm ohne weitverzweigte Fehler. Die Resultate dieser Risiko-Chancen-Entwicklung sind:

1. Schnelle Programmierergebnisse mit hohen Fehlerquoten.
2. Hohe Zeitanteile für Fehlersuche und -beseitigung.

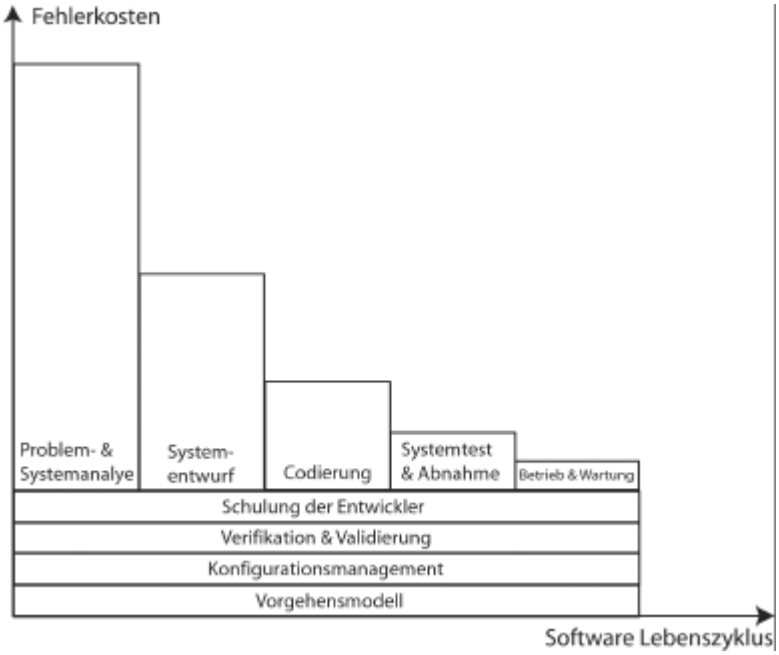
Zur Warnung: Lassen Sie sich niemals von schnellen Zwischenergebnissen, Modulen usw. beeindrucken; dass dicke Fehlerende kommt garantiert. Funktionsfähigkeit: Eine Software funktioniert erst dann, wenn nach erfolgreichen Testläufen in der praktischen Produktivsetzung keine ablaufbehindernden Fehler mehr auftreten. Eine Software muss daher systematisch in Bezug zu den angezielten Geschäftsprozessen, zur Hardware, zum Betriebssystem und sonstigen Software und zur Vernetzung (Intranet, Internet) geplant, geschrieben, getestet, revidiert, produktiv gesetzt, überarbeitet, dokumentiert, abgenommen, gezahlt und gewartet werden.

Hier können nur typische Fehler behandelt werden, die im Rahmen der Softwareentwicklung häufig auftreten. Damit soll das Risiko-Chancen-Bewusstsein der IR-Prüfer zu den Verfahren und Ergebnissen der Softwareentwicklung geschärft werden. Viele der aufgeführten Fehler sind seit langem bekannt. Die Vermeidung dieser Fehler gestaltet sich schwierig, da immer kürzer werdende Entwicklungszyklen, ständig steigende Komplexität der äußeren Rahmenbedingungen und das zur Verfügung stehende Budget im Gegensatz zu folgenden Zielen stehen: In möglichst kurzer Zeit soll qualitativ hochwertige Software entwickelt werden, die den Konkurrenzprodukten überlegen ist. Die oft auftretenden Kosten für die Beseitigung von Produktmängeln stellen dagegen entgangenen Gewinn - wahrlich Unkosten - dar und verschärfen den Projektmanagementstreit.

Der Entwicklungsprozess ist deshalb unter vertretbarem Aufwand so zu organisieren, dass ein systematisches Vorgehen wie z.B. durch die 4 SAP-Phasen ermöglicht wird:

Phase 1	Organisation + Konzept	Übergang = Sollkonzept
Phase 2	Detaillierung + Realisierung	Übergang = Prototyp
Phase 3	Produktions-vorbereitung	Übergang = Produktivsystem
Phase 4	Produktivbetrieb	Übergänge = Wartung/Optimierung

Die Phasen enthalten vorgegebene Subsysteme, die nach Abarbeitung zum Übergang in die nächste Phase und deren Subsysteme ermöglicht. Mängel der Entwicklungsprozesse können so weitgehend vermieden werden. Dies belegt die Fehlerkostenbetrachtung zu SW-Lebenszyklus[3] der "CEFE - CAD/CAM Entwicklungsgesellschaft Arbeitsgruppe 19 Software Engineering" - zitiert aus dem Internet:



Die verursachten Fehlerkosten stehen im direkten Zusammenhang zum zeitlichen Ablauf der Phasen und ihren Subsystemen: Wer sich nicht von Anfang an organisiert, initiiert Fehler und damit vermeidbare Kosten.

5. Zum Grundsatz: Risiko- statt Krisenmanagement

Die Chancen eines SW-Entwicklungsprojektes steigen mit der Umsetzung eines V-Modells und einer projektspezifischen Risikoanalyse.

Chancenorientierung statt sinnloser Risikobastelei

Wir beschäftigen uns hier ausschließlich mit den generellen Methoden der Softwareentwicklung. Dargestellt werden ausschließlich die organisierenden Methoden der Produktion von Software. IR-Systemprüfungen beschäftigen sich bei der SW-Entwicklung mit den generellen und anerkannten Methoden der Entwicklung von Anwendungsprogrammen und nicht mit den Risiken auf der Ebene der unmittelbaren Erstellung von Objekten, Makros, Codierungen usw..

Das V-Modell ermöglicht Planungssicherheit und PM-Realisierungschancen über die Zerlegung des SW-Entwicklungsprozesses in logische Phasen (Aktionen + Ereignisse) und Übergänge. Software-Projekte laufen immer Gefahr, Termine und Budget zu überschreiten. Das Vorgehensmodell ermöglicht durch Phasen, Übergänge, Meilensteine und Verifizierungen ein Lenkungsinstrument, mit dem frühzeitig Abweichungen erkannt und Korrekturmaßnahmen ergriffen werden können. Deshalb gilt der Grundsatz von Risiko- statt Krisenmanagement.

Proaktives Projekt-Risikomanagement

Risikomanagement ist proaktiv und verhindert Schadensfolgen. Krisenmanagement ist reaktiv und mindert bestenfalls eingetretene Schäden. Das Risikomanagement analysiert ex post mit hinreichender Wahrscheinlichkeit intolerable Störprozesse mit Schadensfolgen und vermeidet post festum Krisenmanagement für real bereits eingetretene Risiken und Schäden.

Proaktives Risikomanagement startet vor dem Projektbeginn mit den ersten Planungen und begleitet das gesamte Projekt bis zum Abschluss. Aufgrund der unterschiedlichen und sich ändernden Rahmenbedingungen zu jeder Phase eines Projektes müssen die Risiken kontinuierlich neu identifiziert und analysiert werden, um geeignete Sofort-Gegenmaßnahmen ableiten zu können. Dies gilt insbesondere für den unterstellten Softwareentwicklungsprozess.

6. Checkliste

Eine hilfreiche Checkliste kann in diesem Rahmen nicht dargestellt werden. Sie kann bei Paul Rieckmann unter riekus@aol.com angefordert werden.

7. Revision der Kreativität oder kreative Revision im Softwareentwicklungsprozess?

Ein Konfliktherd ergibt sich unmittelbar aus der Stellung von Prüfer und Softwareentwickler. Der Prüfer führt eine mehr formal-organisierende und der Softwareentwickler eine mehr kreative Rolle aus. Der Softwareentwickler wird in der Revision naturgemäß eine störende Kraft sehen, der zudem aus seiner Sicht keine inhaltlichen Grundkenntnisse besitzt und im Bericht eine Bewertung vornimmt. Über diesen Konfliktherd sollte man sich vor einer Revision im Klaren sein. Im Vorgehen der Revision sollte sich dieser mögliche Konflikt durch ein striktes Prüfen des Vorgehensmodells reflektieren, um Zusatzkonflikte auf der fachlichen Ebene der Codes oder Softwareentwicklung zu vermeiden.

Aus Sicht der Revision sollten kreative Prozesse wie die Programmierung von Codes nicht in ihrem Produktionsprozess durch Prüfungen gestört werden. Vielmehr sollte dagegen das fertige Produkt dieser Entwicklung anhand der Spezifikationen, Ziele, Testergebnisse, Vorgaben usw. in einem Soll-Ist-Abgleich geprüft werden. Eine kreative Revision sollte sich darüber hinaus mit den Prozessphasen des Vorgehensmodells beschäftigen, da eine Prüfung der Prozessphasen und der sich anschließenden Phasenübergänge - z.B. die Soll-Ist-Testergebnisse - die Schwach- und Starkstellen der Entwicklung bzw. Prozesse aufdeckt.

Literaturhinweise:

Agresti, W.W. (Ed.): New Paradigms for Software Development, IEEE Computer Society press, 1986

Beims, H.D.: Praktisches Software Engineering, Hanser Verlag, 1995

Broehl, A.D., Droeschel, W.: Das V-Modell - Der Standard für die Software-Entwicklung mit Praxisleitfaden, Oldenbourg, 1995

Dahme, C., Hesse, W.: Gesellschaft für Informatik: Informatik Spektrum 20: 3-4 Themenheft "Evolutionäre und kooperative Software-Entwicklung", Springer, 1997

Davis, A.D.: 201 Principles of Software Development, McGraw-Hill, 1995

DeMarco, T.: Software-Projektmanagement, Wolframs Fachverlag, 1989

Frick, A.: Der Software-Entwicklungsprozess - Ganzheitliche Sicht, Hanser Verlag, 1995

Frühauf, K., Ludewig J., Sandmayr H.: Software-Projektmanagement und Qualitätssicherung, vdf Verlag der Fachvereine Zürich, 1988

Kimm, R., Koch, W., Simonsmeier, W., Tontsch, F.: Einführung in Software Engineering, de Gruyter, 1979

Martin, J.; Odell, J.: Object Oriented Analysis and Design, Prentice Hall 1992

Myers, Glenford J.: Methodisches Testen von Programmen, 4.Auflage, Oldenbourg, 1991

Schäfer, S.: Objektorientierte Entwurfsmethoden, Addison-Wesley, 1994

Schönthaler, F., Nemeth, T.: Software-Entwicklungswerkzeuge: Methodische Grundlagen, B.G. Teubner 1992 (2.Aufl.)

Wallmüller, E.: Software-Qualitätssicherung in der Praxis, Hanser, 1990

Prüfung der Betriebsbereitschaft von Anwendungssystemen im Rahmen der DV-Revision

Von Dr. sc. G. W. Wähner
REVIDATA Unternehmensberatung GmbH

Im gegebenen Zusammenhang steht der Begriff Betriebsbereitschaft für Zuverlässigkeit und Verfügbarkeit von DV-Anwendungssystemen, einschließlich ihrer Plattformen. Zuverlässigkeit und Verfügbarkeit sind Voraussetzungen für die ordnungsgemäße, sichere und wirtschaftliche Nutzung von DV-Anwendungssystemen, darunter "DV-gestützte Buchführungssysteme", und deshalb Gegenstand der DV-Systemprüfung.

1 Prüfungsgrundlagen

Die Prüfungsschwerpunkte Betriebsbereitsschaft und - als deren letzte Konsequenz - Katastrophenvorsorge lassen sich nicht auf eindeutige Prüfungsmaßstäbe zurückführen. Immerhin gibt es brauchbare Ansätze zur formalen Rechtfertigung dieser Prüfungsschwerpunkte:

1. In den GoBS, Abschnitt 5.2 (vgl. GoBS) werden als schutzbedürftige Informationen auf Datenträgern gespeicherte Daten, Belege und sonstige Aufzeichnungen, aber auch Software (Betriebs- und Anwendungssysteme) bezeichnet. Im Abschnitt 5.3 heißt es dann, "diese Informationen sind gegen Verlust zu schützen". Im Abschnitt 5.5.2 schließlich werden Maßnahmen gefordert "durch die für die gesicherten Programme/Datenbestände die Risiken hinsichtlich Unauffindbarkeit, Vernichtung und Diebstahl im erforderlichen Maß reduziert werden.
2. In der Abgabenordnung, Abschnitt V, wird das Gleiche, in gekürzter Form, vorgegeben.
3. In der FAMA-Checkliste "EDV-Systemprüfung" (vgl. FAMA1) wird im Abschnitt "Datensicherung" mit Frage 3.3.1 nach der Aufbewahrung der Datenbestände "außerhalb des Rechenzentrums in feuerfesten Schränken" gefragt.
4. Die am weitesten greifenden Fragen befinden sich im Abschnitt "Betriebsbereitschaft" der FAMA-Checkliste. Dort wird der Prüfer angehalten, folgende Sachverhalte zu prüfen:
   - ☐ Regelmäßige Wartung der EDV-Anlage
   - ☐ Sicherung des erforderlichen Klimas (Klimaanlage)
   - ☐ Sicherung der Stromversorgung (USV)
   - ☐ Brandschutz
   - ☐ Warnsystem für Feuer und Klima (auch während des "operator-losen" Betriebes)
   - ☐ Existenz eines Katastrophenplanes mit Ausweichmöglichkeiten für den Fall längerer Unterbrechungen

2 Einordnung des Prüfungsgegenstandes

Betriebsbereitschaft ist ein mehr technisch bestimmter Terminus. Der Begriff impliziert Zuverlässigkeit und Verfügbarkeit des betreffenden Anwendungssystems. Beides ist natürlich Voraussetzung für die ordnungsgemäße Nutzung eines Buchführungssystem und deshalb ein - wenn auch nicht der wichtigste - Prüfungsschwerpunkt innerhalb einer Systemprüfung.

Allerdings können Einschränkungen der Systemverfügbarkeit oder dessen Zuverlässigkeit ihre Ursache in Fehlern auf ganz unterschiedlichen Ebenen des Gesamtsystems haben, also auf Ebene der

- Hardware,
- Basis-Software (Betriebs- und Netzbetriebssysteme),
- Anwendungs-Software,
- Datenbestände oder
- sonstigen Bestandteile der IT-Infrastruktur

und das noch dazu in unterschiedlichster Kombination und Konstellation.

Das macht den Prüfungsgegenstand recht komplex.

Während zu Zeiten des "Closed Shop-Betriebes" durch das Operating geführte sogenannte Maschinentagebücher bzw. Schichtbücher Auskunft über Art und Umfang von Unregelmäßigkeiten, Fehlern aller Art und Stillstandszeiten der Rechnersysteme gaben, ist der Prüfer heute auf System-Logs, Error-Logs und andere vom Betriebssystem und einigen Anwendungssystemen erfaßte Daten angewiesen. Diese Daten zu selektieren, auszuwerten und daraus Prüfungsfeststellungen abzuleiten, ist ein aufwendiger Prozeß.

Hinzu kommt, daß eingeschränkte Verfügbarkeit und Zuverlässigkeit nicht zwangsläufig Verstöße gegen die Ordnungsmäßigkeit im Sinne der GoB und GoBS nach sich ziehen müssen.

Eine Tiefenprüfung der die Betriebsbereitschaft beeinflussenden Faktoren wird deshalb Gegenstand thematischer Prüfungen bleiben, die ein spezielles fachliches Profil erfordern.

Mit Blick auf die normale Systemprüfung - bei der Betriebsbereitschaft im allgemeinen ein Randproblem ist - begnügen wir uns nachfolgend mit der Erläuterung einiger Begriffsinhalte und der Berechnungsgrundlagen einiger Kennziffern der Betriebsbereitschaft, um auf dieser Grundlage abschließend einen praktikablen Prüfungsansatz anzubieten.

3 Bestimmung der Zuverlässigkeit von Rechnersystemen

Der Begriff Zuverlässigkeit (reliability) stammt aus dem technischen Bereich und wird auch für Rechnersysteme angewendet.

Nach DIN 40041 ist die Zuverlässigkeit eines technischen Systems definiert als

"die Fähigkeit einer Betrachtungseinheit, innerhalb der vorgegebenen Grenzen denjenigen durch den Verwendungszweck bedingten Anforderungen zu genügen, die an das Verhalten ihrer Eigenschaften während einer gegebenen Zeitdauer gestellt sind".

Es werden drei Zuverlässigkeitszustände unterschieden:

1. Das System ist funktionsfähig
2. Das System ist arbeitsfähig
3. Das System ist nicht verwendbar

Ein Rechnersystem ist beispielsweise nicht mehr voll funktionsfähig, aber unter Umständen noch arbeitsfähig, wenn einzelne Komponenten ausgefallen sind, wie einzelne Prozessoren, Server, Netzkomponenten oder Clients.

Das System ist jedoch nicht verwendbar, wenn es durch Fehler der Hardware, des Betriebssystems, Stromausfall oder aus anderen Gründen heruntergefahren werden muß bzw. nicht neu gestartet werden kann.

Berechnet wird die Zuverlässigkeit eines Rechnersystems anhand

- der mittleren Dauer eines Ereignisses, welches das Rechnersystem vom funktionsfähigen in den nicht verwendbaren Zustand versetzt (auch bezeichnet als MTBF - Mean Time Between Failure oder mittlerer Fehlerabstand),
- der prozentualen Nutzungsdauer (Einschaltzeit) und
- des mittleren Abstandes zwischen zwei derartigen Ereignissen (Fehlern).

(Zu weiteren Einzelheiten vgl. WÄ93).

Es versteht sich, daß der Prüfer diese Daten nicht selbst ermitteln kann.

Sich mit der Zuverlässigkeit im Rahmen einer Ordnungsmäßigkeitsprüfung zu beschäftigen ist demzufolge nur sinnvoll, wenn verläßliche Unterlagen des Betreibers des Systems zur Zuverlässigkeit zur Verfügung stehen. Selbst dann können derartige Daten meist nur indirekt herangezogen werden, etwa im Zusammenhang mit der Klärung der Ursachen für einseitige Buchungen, Nichtverfügbarkeit des Buchführungssystems oder unzureichendem Antwortzeitverhalten.

Immerhin ist die Zuverlässigkeit des Anwendungssystems eine Prüfungsfrage wert.

4 Bestimmung der Verfügbarkeit von Rechnersystemen

Einfacher ist die Prüfung der Verfügbarkeit des Anwendungssystems.

Nach DIN 40042 ist als Verfügbarkeit eines technischen Systems die Wahrscheinlichkeit definiert, das System zu einem vorgegebenen Zeitpunkt in einem funktionsfähigen Zustand anzutreffen.

Die Verfügbarkeit (V) berechnet sich als Quotient aus Einschaltzeit (EZ) des Systems und Einschaltzeit (EZ) plus Ausfallzeit (AZ), also

V = EZ / (EZ + AZ).

Leider stehen selbst Kennziffern der Verfügbarkeit in der Praxis aus folgenden Gründen oft nicht bereit:

1. Die Rechnersysteme sind zwischenzeitlich sehr zuverlässig und ausfallsicher (häufig mit einer Verfügbarkeit von größer, gleich 99,9 %), so daß der Aufwand für den Nachweis der Verfügbarkeit für nicht gerechtfertigt gehalten wird.
2. Kleine Rechnersysteme (unter Betriebsystemen der Familien Windows, UNIX, LINUX u.a.) bieten keine Systemunterstützung für die Erfassung von Einschaltzeiten und Ausfallzeiten und der manuelle Aufwand zur Führung von Maschinentagebüchern etc. erscheint nicht gerechtfertigt.
3. Es herrscht im Anwendungsbereich Nachlässigkeit und / oder Unkenntnis über Möglichkeiten der Berechnung und die Aussagekraft derartiger Kennziffern zur Betriebsbereitschaft.

Immerhin sollte der Prüfer nach diesbezüglichen statistischen Werten fragen und sich ein Bild der Entwicklung der Verfügbarkeit und der sie reduzierenden Ursachen machen.

5 Bestimmung von Antwortzeiten

Jetzt sind wir in vertrautem Fahrwasser:

Die Antwortzeit ist eine Kategorie der Online-Verarbeitung und - neben der Verfügbarkeit - wichtigste Kennziffer des sogenannten Service Level Agreements (SLA), welches häufig Bestandteil von internen oder externen Dienstleistungsverträgen über die Erbringung von EDV-Leistungen ist.

Unter Antwortzeit wird jene Zeitspanne verstanden, die nach Eingabe des letzten zu übertragendenden Zeichens am Terminal bzw. PC des Nutzers verstreicht (meist mittels Drücken der Entertaste), bis das erste Zeichen der Antwort vom Rechnersystem (Host oder Server) auf dem Bildschirm des Nutzers erscheint.

Die Antwortzeit beinhaltet in der Regel folgende Bestandteile:

1. Übertragungszeit vom Endgerät des Nutzers zum Rechnersystem
2. Zeit für Aufruf und Ausführung der vom Nutzer abgesetzten / angeforderten Transaktion im adressierten Rechnersystem
3. Übertragungszeit für die Antwort vom Rechnersystem zum Endgerät des Nutzers

Garantiert werden Antwortzeiten meist nur für festgelegte Standard-Transaktionen, wie Übermittlung eines Datensatzes, Buchen eines Beleges, Anzeige eines Tabelleninhalts etc. Die Einbeziehung von Transaktionen, welche - bezogen auf das SAP R/3-Systems - beispielsweise einen ABAP aufrufen, eine Batch-Input-Mappe einspielen oder ähnliche "Langläufer" darstellen, würde die Aussagekraft der Kennziffer verfälschen.

Soll das Antwortzeitverhalten eines Rechnersystems im Sinne oben genannter Begriffsbestimmung gemessen werden, setzt das geeignete Tools voraus. Diese müssen auf drei - oft dazu noch inhomogenen - Ebenen der Systemarchitektur die Bestandteile der jeweiligen Ebene an der Antwortzeit messen und bereitstellen. Bei diesen Ebenen handelt es sich um

- die Ebene des Nutzers (Client),
- die Übertragungsebene (LAN, INTRANET, WAN oder WWW) und
- die Ebene des Rechnersystems (Host und/oder Server).

Derartige Tools sind sehr teuer. Erfassung, Aufbereitung und Auswertung der Datenbasis sind sehr aufwendig.

Will der Prüfer dem Antwortzeitverhalten auf den Grund gehen, wird er sehr oft feststellen, daß

- keine Tools zur Messung oder zur Aufbereitung der Antwortzeiten vorhanden sind,
- mit Meßgrößen gearbeitet wird, die sich ausschließlich auf den Host oder Server beziehen, weil es nur auf dieser Ebene Software-Unterstützung zur Messung und Aufbereitung der Meßdaten gibt,
- Service Level Agreements, in denen Werte für Antwortzeiten, Verfügbarkeit, Reaktionszeiten und andere die Betriebsbereitschaft betreffenden Vereinbarungen fixiert sind, nur auf dem Papier

stehen oder im gegebenen Zusammenhang - bezogen auf den Nutzer des Buchführungssystems - nicht brauchbar sind.

6 Einflußfaktoren auf die Betriebsbereitschaft

Allein die Ermittlung des Niveaus der Betriebsbereitschaft, so problematisch das im Einzelfall auch sein mag, reicht nicht aus für begründete Prüfungsfestellungen. Weiterhin ist zu prüfen, welche Faktoren die Betriebsbereitschaft positiv oder negativ beinflussen.

Die Betriebsbereitschaft von Anwendungssystemen wird hauptsächlich durch folgende Gruppen von Faktoren beeinflußt:

1. Zuverlässigkeit von Hardware, Basis-Software, Anwendungs-Software
2. Niveau der physischen Sicherheit der Anwendungssysteme, darunter

   - USV,
   - Brandschutz,
   - Einbruchsschutz,
   - Zutrittsschutz.

3. Niveau der organisatorischen und technologischen Sicherheit der Anwendungssysteme, darunter

   - Katastrophenvorsorge,
   - Datensicherung,
   - Maßnahmen für Wiederanlauf / Recovery,
   - Zugriffsrechteverwaltung,
   - Virenschutz, Firewalls etc.
   - Problem- und Fehlermanagement,
   - Changemanagement

Die Faktoren der ersten Gruppe sind zwar quantifizierbar mittels Kennziffern der Zuverlässigkeit, bezogen auf das gesamte Rechnersystem oder einzelne Komponenten, aber - mangels einer entsprechenden Datenbasis - für den Prüfer meist nur an der Oberfläche zugänglich.

Die Faktoren der zweiten Gruppe sind in jedem Falle einen "Grundscheck" wert. In dem Wissen, daß die Beurteilung der Leistungsfähigkeit und Zweckmäßigkeit unterschiedlicher Möglichkeiten der USV, des Brandschutzes oder des Zutrittschutzes Spezialwissen erfordert, wird sich der erfahrene Prüfer bei der Bewertung seiner Prüfungsfeststellungen und der Ableitung von Empfehlungen zurückhalten. Um so mehr, als selbst eine graduelle Erhöhung der Sicherheit in diesem technischen Bereich mit hohem Aufwand verbunden sein kann.

Die eigentliche Frage, ob und inwieweit die technischen Maßnahmen zur Sicherung der Betriebsbereitschaft dem gegebenen Risiko angemessen sind, läßt sich erst auf der Grundlage einer Risikoanalyse und darauf fußender Katastrophenvorsorge mit einiger Sicherheit beantworten.

Die Faktoren der dritten Gruppe sind im Rahmen einer Systemprüfung die wichtigsten. Sie stellen jedoch eigenständige, unverzichtbare Prüfungsschwerpunkte dar, deren Ergebnisse allerdings auch unter dem Blickwinkel möglicher Einflüsse auf die Betriebsbereitschaft gesehen werden sollten.

7 Prüfungsansatz

7.1 Thematische Prüfung

Handelt es sich um eine spezielle Prüfung, mit dem Ziel, die Ursachen für ein desolates System zu ermitteln, bietet eine Prüfung von Zuverlässigkeit, Verfügbarkeit und Antwortzeit, einen guten Einstieg. Dabei muß sich der Prüfer auf die im Anwendungsbereich zur Verfügung stehende Datenbasis stützen können, beispielsweise in der Form von Systemerfassungssätzen der Komponente SMF (System Management Facilities) der Betriebssystemfamilien IBM MVS oder OS/390), von Fehlererfassungssätzen der Fehlerroutinen dieser Betriebssysteme usw.

Ohne derartige - durch den Anwender bereitgestellte, bereits aufbereitete Daten - ist die Prüfung ein sinnloses Unterfangen.

Auch bei Bereitstellung von Verfügbarkeits-, Antwortzeit und Fehlerstatistiken ist das nur ein erster Schritt, dem nunmehr die Analyse der Ursachen für Fehler, Ausfälle oder unzureichende Performance des Anwendungssystems folgen muß.

Dabei bietet sich eine Vorgehensweise an, die der Reihenfolge der Aufzählung der Einflußfaktoren im vorangegangenen Abschnitt folgt:

1. Verifikation der vorhandenen Daten zu Zuverlässigkeit und Verfügbarkeit, verbunden mit dem Versuch, jene Systemkomponenten zu bestim-

men, die Hauptursache für die eingeschränkte Betriebsbereitschaft sind.

2. Analyse der Ursachen eingeschränkter Betriebsbereitschaft, gestützt auf Daten

   - des Problem- und Fehlermanagements (Fehlerstatistiken),
   - der Logführung (Systemlogs, Fehlerlogs, Job-Protokolle u.a.),
   - des Security Managements (Berechtigungskonzept, Zugriffsschutzverletzungen, Viren u.a.)

7.2 Systemprüfung

Auch im Rahmen einer Systemprüfung sollte - sofern das enge Prüfungsbudget nicht zu Abstrichen zwingt - ein Blick auf den Bereich Betriebsbereitsschaft geworfen werden. Zu diesem Zweck sollte der Prüfer folgende Unterlagen anfordern:

1. Verfügbarkeitsstatistik und Abweichungsanalyse
2. Antwortzeitstatistik und Abweichungsanalyse
3. Systemprotokolle über abgebrochene Verbuchungen
4. Fehlerstatistiken und andere verfügbare Aufzeichnungen

Nutzerbefragungen runden das Bild ab, auch wenn die Antworten wegen fehlender statistischer Daten meist subjektiv sind. Derartige Befragungen sind wie folgt zu werten:

a) Verfügbarkeiten, die im Mittel um 98 % liegen und Antwortzeiten, die zu 90 % unter 2 Sekunden in einem LAN oder unter 3 Sekunden in einem WAN liegen, sind normal. Wenn es auch keine Hinweise auf Fehlerhäufungen und ungeklärte Systemabbrüche gibt, kann der Prüfer eine positive Feststellung zur Betriebsbereitschaft treffen.
b) Verfügbarkeiten und Antwortzeiten von Anwendungq2en im WWW (e-Commerce und e-Business) sind sehr stark von den jeweiligen Systemplattformen, genutzten Übertragungsprotokollen und Services sowie weiteren Einflußfaktoren abhängig. Sie liegen - soweit bekannt und verallgemeinerungsfähig - heute noch deutlich über denen in LAN, INTRANET und WAN.

Weichen die verfügbaren statistischen Werte deutlich von diesbezüglichen Erfahrungswerten ab und / oder gibt es sonstige Indikatoren, die auf Probleme im Bereich Betriebsbereitschaft hindeuten, muß der Prüfer eine Entscheidung treffen und mit dem Auftraggeber abstimmen:

- ☐ Entweder wird die Problemstellung ausgeklammert und - unter Verweis auf die Indikatoren - eine thematische Prüfung empfohlen oder

- ☐ der Prüfer ändert sein Prüfungskonzept zugunsten einer Priorisierung des Bereiches Betriebsbereitschaft. Das geht meist nicht ohne Abstriche an anderen Prüfungsschwerpunkten. Selbst ein Verzicht auf ansonsten obligatorische Prüfungsschwerpunkte kann jedoch im Interesse des Auftraggebers / Mandanten sein, wenn das Anliegen richtig vermittelt wird.

Oft wird der Prüfer jedoch mangels einer geeigneten Datenbasis überhaupt nicht in der Lage sein, verifizierbare Feststellungen zur Betriebsbereitschaft zu treffen und deren Einfluß auf den engeren Prüfungsgegenstand - nämlich auf die Ordnungsmäßigkeit, Sicherheit und Wirtschaftlichkeit des zu prüfenden Anwendungssystems. Allein die bei der Prüfung erworbene Kenntnis zum organisatorischen und technischen Niveau im Bereich von Systemadministration und Systembetrieb, ergänzt um die subjektiven Meinungen aus beiläufigen Befragungen von Mitarbeitern, vermittelt oft ein ausreichendes Bild. Ausreichend zur Einschätzung des Prüfungsrisikos im Bereich Betriebsbereitschaft, das um so höher ist, je geringer die Daten- und Informationsbasis auf diesem Gebiet ist und je kritischer sich die Befragten äußern.

Dieser Sachverhalt ist eine Feststellung im Prüfungsbericht wert, erforderlichenfalls verbunden mit der Empfehlung, sich mit den Ursachen eingeschränkter Betriebsbereitschaft und bestehender "Grauzonen" im Rahmen einer thematischen Prüfung zu beschäftigen.

Literaturnachweis

FAMA1 FAMA-Stellungnahme 1/1987, DIE WIRTSCHAFTSPRÜFUNG, IDW-Verlag, Heft 1-2 (1988), S. 1 -27

GoBS Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS) Bundessteuerblatt 1995, Teil 1, S. 738 - 747

IDW01/2 Entwurf IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Informationstechnologie (IDW ERS FAIT 1), Stand 08.03.2001

WÄH93 Wähner, G. W., Datensicherheit und Datenschutz, VDI Verlag, Düsseldorf 1993

WÄH02 Wähner, G. W., DV-Revision - Prüfung der Ordnungsmäßigkeit, Sicherheit und Wirtschaftlichkeit, Friedrich Kiehl Ver-

Prüfung von Windows NT-Umgebungen - Teil III: Prüfen der Organisationsstruktur

Von Marcus Rasokat
IBS Hamburg

In den ersten beiden Teilen wurde auf die "Prüfung aus Sicht der Benutzer" und auf die "Prüfung aus Sicht der Ressourcen" eingegangen. Bereits im ersten Teil wurde klar, dass für einen Großteil der Informationsdefizite (Benutzerleichen) die Administration nicht direkt verantwortlich gemacht werden kann. Dies ist insbesondere dann der Fall, wenn es sich um Benutzerinformationen handelt, die Versetzungen, Entlassungen, Pensionierungen o.ä. betreffen. Dass solche Zustandsänderungen von Benutzern eine elementare Auswirkung auf die IT-Sicherheit haben (und somit absolut "revisionsrelevant" sind), wurde in dem ersten Artikel ausführlich aufgezeigt.

Die Prüfung dieser (organisatorischen Kommunikations-) Bereiche und darüber hinaus Punkte wie Vorgaben, Dokumentation, örtliche Sicherheit und Ausfallsicherheit, umfassen die Prüfung der Organisationsstruktur und sind Kernpunkt dieses dritten und letzten Teils zur Prüfung von NT-Umgebungen.

Benutzerkonten und Gruppen

Nicht nur die Informationen zu den Benutzern und deren Gruppen müssen über Verfahrensanweisungen auf dem neuesten Stand gehalten werden. Ein Regelwerk über die Ersteinrichtung eines Benutzerkontos, Berechtigungen der Gruppen (die in der Regel die Abteilungen wiederspiegeln), Namenskonventionen etc., sowie die eigentliche Handhabe eines Benutzerkontos bei "Benutzerversetzung" in einen anderen Aufgabenbereich, müssen in einem Regelwerk genau festgelegt sein.

Als sehr nützlich für den Entwurf einer Verfahrensregelung zur Handhabung von Benutzerkonten erweist sich die Schriftenreihe Grundschutzhandbuch des BSI (Bundesamt für Sicherheit in der Informationstechnik: www.bsi.de). Hier sind Mindestanforderungen an die IT-Sicherheit von staatlicher Seite exemplarisch definiert. Mittlerweile hat das BSI zahlreiche Prüfer und Unternehmen akkreditiert, die nach dem Grundschutz des BSI die Sicherheit von IT-Umgebungen zertifizieren dürfen.

An dieser Stelle sein auf einige Grundlagen hingewiesen, die die Transparenz erhöhen und damit sowohl die Administration als auch die Prüfung erheblich erleichtern können. Wie in dem zweiten Teil (Prüfen aus Sicht der Ressource) bereits mit der Einführung in das Berechtigungskonzept von Windows NT erwähnt, werden die Abteilungen eines Unternehmens in globalen Gruppen definiert und dargestellt. Die globalen Gruppen werden in lokalen Gruppen zusammengefasst und bekommen Rechte auf Ressourcen. Durch dieses Modell entsteht ein relativ statisches Gerüst aus Gruppen und Rechten. Damit im Laufe der Zeit die ungewollte Rechtekumulation der Benutzer so gering wie möglich gehalten wird, ist der Einsatz von Namenskonventionen für die Benutzer essentiell. Eine bewährte Methodik besteht darin, den (Anmelde-)Namen aus Personalnummer und Abteilungskürzel zusammen zu setzen. Die Personalnummer identifiziert den Benutzer bei Revision und Administration eindeutig. Durch das Kürzel der Abteilung lassen sich innerhalb der globalen Gruppen auf den ersten Blick Fehler im Berechtigungskonzept sichtbar machen. Voraussetzung für dieses Konzept ist die Vorgabe, dass alle Benutzerkonten, deren Anwender die Abteilung wechseln, gelöscht bzw. neu erstellt werden. Durch dieses Verfahren können Gruppenzugehörigkeiten, die eine kritische Kombination darstellen (z.B. Buchhaltung und Entwicklung), weitgehend vermieden bzw. leicht aufgedeckt werden.

Kommunikation und Verantwortung

Wie in der Einleitung angedeutet kann die Administration bei Informationsdefiziten im Personalbereich nicht in die Verantwortung genommen werden. Das Problem an dieser Stelle besteht darin, dass es in den meisten Unternehmen für diese "Kommunikations-

schnittstelle" keine Verantwortlichen "in Person" gibt. Es gilt also eine Vorgabe zu erstellen, wie entsprechende Benutzerinformationen an die Administration weiter zu reichen sind. In der Regel ist, gerade in größeren Unternehmungen, die Personalabteilung die einzige Instanz, die für die rechtzeitige Bereitstellung dieser Informationen in Frage kommt. In besonderen Fällen, z.B. in Abteilungen, in denen eine personell hohe Fluktuation gegeben ist, macht es auch Sinn, die Informationen über die Führungsebene der entsprechenden Abteilungen laufen zu lassen. Hierauf zugeschnittene Verfahrensanweisungen können die Informationsverantwortlichkeiten personell sicherstellen. Wo welches Verfahren am effektivsten ist, hängt von der Infrastruktur der einzelnen Unternehmen ab.

Da Benutzerleichen ein essentielles Sicherheitsrisiko darstellen, sollte aber auch aus administrativer Sicht über eine Verfahrensanweisung eine Rücksicherung implementiert werden. Dies ist insbesondere dann wichtig, wenn Anträge auf Berechtigungen von Benutzern eingehen, die den "üblichen" Verfahren wiedersprechen.

Beispiel: Laut Verfahrensanweisung werden Benutzerberechtigungen im Standardverfahren nur dann geändert, wenn eine schriftliche Benachrichtigung über den Abteilungswechsel eines Benutzers durch die Personalabteilung bei der Administration (oder dem Benutzerservice) eingegangen ist. Meldet sich ein Benutzer telefonisch bei der Administration (oder dem Benutzerservice) wegen fehlender Zugriffsberechtigung, tritt eine Verfahrensanweisung in Kraft, in der eine Rücksprache mit der Personalabteilung über den Benutzerstatus des entsprechenden Benutzers festgelegt ist.

Wichtig: Auch wenn insbesondere dieser Teil des organisatorischen Ablaufs unternehmensabhängig, also in jedem Unternehmen anders strukturiert ist, sollte es hier eine klar definierte Verfahrensanweisung geben, die die Verantwortlichkeiten für die Weiterleitung der Benutzerinformationen regelt. Die Revision sollte in beratender Funktion bei der Erstellung der Verfahrensanweisung und deren Vorgaben involviert werden. Weiterhin sollte bei der Definition der Aufgabenregelung darauf geachtet werden, dass die Administration nur zu einem geringen Teil "aktiv" an der Informationsbeschaffung teil haben kann. Dies ist nur in den vorher genannten Ausnahmefällen möglich. Die "Meldepflicht" zu den Benutzerinformationen kann nur der Personalabteilung bzw. den Abteilungsführungen auferlegt werden.

Datensicherheit

Die Datensicherheit unterscheidet sich in zwei wesentlichen Punkten:

1. Die örtliche Sicherheit
2. Die Sicherung/Verfügbarkeit der Daten

Örtliche Sicherheit

Da Daten grundsätzlich auf Servern zu halten sind, unterliegen die Serverräume besonderen Anforderungen. Der oder die Serverräume müssen

- klimatisiert sein,
- eine Brandschutzanlage haben, die auf Stickstoffbasis arbeitet,
- räumlich gesichert und damit
- vor inautorisiertem Zugang und vor Feuer geschützt sein.

Ein wesentlicher Prüfungsansatz, der oft übersehen wird, besteht in der Dokumentation der oben aufgeführten Daten. Es ist darauf zu achten, dass diese nicht nur innerhalb der Serverräume verfügbar ist, sondern mit einem Notschlüssel/code in einem versiegelten Umschlag an einem sicheren Ort außerhalb der Serverräume für Notfälle eingelagert ist.

Datensicherung

Alle Daten, die für den Betrieb des Unternehmens wichtig sind, müssen über eine Backupstrategie gesichert werden. Von den Backups müssen zwei Serien erstellt werden. Die erste für den schnellen Zugriff vor Ort bei Ausfall eines Servers, die zweite für einen etwaigen Totalausfall. Diese muss an einem Ort, der in einem anderen Gebäude liegt als die Serverräume, gelagert werden. Die Backupmedien müssen in feuerfesten Schränken gelagert werden. Die Backupstrategie muss genauestens dokumentiert sein. Oft vergessene Dokumentationspunkte sind u.a.:

- Kennzeichnung der Medien (welches Medium für welchen Rechner)
- Hardwaredokumentation (Systemvoraussetzungen für die Lauffähigkeit der Systembackups)
- Medienhistorie (Schriftliches Protokoll, wann auf welchem Medium welches Backup erstellt wurde)
- Haltbarkeit der Medien (betr. vor allem Bänder, da die Daten durch Erdstrahlung mit der Zeit verloren gehen. Dieser Punkt muss dokumentiert

sein, damit rechtzeitig neue Kopien der Bänder erstellt werden können, die z.B. Daten enthalten, die der Aufbewahrungsfrist gem. §257-4 HGB unterliegen)

Wichtig: Es muss eine Kopie der Dokumentation geben, die bei dem zweiten Backupsatz gelagert wird, damit auch bei einem Totalausfall eine Dokumentation vorliegt.

Datenverfügbarkeit

In der heutigen Zeit können sich Unternehmen den Ausfall von Teilen oder gar der ganzen DV-Anlage nicht lange leisten. Backups sind nur als "letztes Mittel zur Datenwiederherstellung" gedacht, sie stellen Daten daher nur indirekt (nämlich bei Ausfall) zur Verfügung. Um eine optimale Datenverfügbarkeit zu gewährleisten, müssen verschiedene andere Sicherheitsmechanismen in die Serversysteme integriert sein:

- USV (Unterbrechungsfreie Stromversorgung)
  Ein Akkumulator, der vom Stromnetz unabhängig Strom für eine beschränkte Zeit zur Verfügung stellt. Kleine USVs bieten lange genug Strom, um die Serversysteme "sauber" herunterfahren zu können. Die Server sind so lange offline, bis der Netzstrom wieder verfügbar ist. Große USVs können den Strom länger halten und werden oft dazu eingesetzt, um letzte Backups vor dem Herunterfahren zu ermöglichen, oder um die Zeit zu überbrücken bis die Notstromaggregate angesprungen sind.
- Notstromaggregate
  Diese werden meistens mit Diesel betrieben und stellen über Generatoren Strom zur Verfügung. Sie dienen zur längeren Überbrückung eines Stromausfalls, um zumindest den Serverbetrieb aufrechterhalten zu können.
- RAID-Systeme (Redundant Array of Independent Disks)
  Auf diesem "Plattenfeld" werden die Daten permanent redundant vorgehalten. Standardmäßig werden RAID 1 (Mirroring) und RAID 5 (Stripe Set with Parity) betrieben.
  Beschreibung:
  RAID1 = Plattenspiegelung
  RAID5 = fehlertoleranter Datenträger mit Daten und Paritäten, die über drei oder mehr physische Festplatten verteilt sind. Die Parität ist ein berechneter Wert, der nach Auftreten eines Fehlers zur Datenrekonstruktion verwendet wird. Wenn ein Teil einer physischen Festplatte ausfällt, können die Daten aus diesem fehlerhaften Bereich aus den verbleibenden Daten und der Parität wiederhergestellt werden.

Alle Server, die für einen Betrieb mit hoher Datenverfügbarkeit verfügbar gehalten werden müssen, müssen mit USV und RAID-Systemen ausgestattet sein. USV und Notstromaggregate müssen in regelmäßigen Abständen getestet werden. Darüber hinaus müssen insbesondere ältere USVs aufgrund des Memory-Effekts regelmäßig entladen werden.

Hinweis: Die Praxis hat gezeigt, dass ältere USV-Anlagen bei einem Test oft nur noch 10% der dokumentierten Leistung vorweisen. In einem solchen Fall muss geprüft werden, ob diese Zeit ausreicht, um einen Systemabschluss durchzuführen, evtl. vorgesehene Backups zu erstellen oder etwaige Notstromaggregate in Betrieb zu nehmen.

Not-/Ausfallpläne

Alle Datensicherheitsmechanismen nützen wenig, wenn niemand weiß, was bei einem Ausfall zu tun ist. Insbesondere die oft gegebene Antwort "Bei einem Ausfall rufe ich Herrn/Frau ... an" ist aus Prüfersicht zu belächeln. Denn z.B. ISDN-Telefonanlagen funktionieren i.d.R. ohne externe Stromversorgung, also auch bei einem Stromausfall, nicht. Und was ist, wenn Herr oder Frau ... nicht da ist?

Auch hier ist über eine detaillierte Verfahrensanweisung dafür Sorge zu tragen, dass jeder, der von einem Ausfall betroffen sein könnte, mit einer schnell verfügbaren Checkliste alle Schritte unternehmen kann, die zur Datensicherung oder Aufrechterhaltung des Serverbetriebs notwendig sind.

Updates, Patches und Virenschutz

Zwar wurde der Support von Windows NT 4 offiziell durch Microsoft eingestellt (es wird demnach keine Servicepacks mehr geben), dennoch ist es wichtig, dass Betriebssystemkomponenten, Programme und Virenscanner auf dem neusten Stand gehalten werden. Leider ist immer wieder zu beobachten, dass in einigen Unternehmen solche Updates "aus dem Bauch heraus" gemacht werden. Ohne eine diesbezügliche Vorgabe kann die Administration jedoch nicht in Verantwortung genommen werden. Daher muss sichergestellt sein, dass eine entsprechende Verfahrensanweisung vorliegt zur Vorgehensweise mit Updates, die durch die Softwarehersteller bereitgestellt werden.

Crash-Kurs:
Spam - die Postwurfsendungen des Internets oder „Der heimliche Ressourcenfresser“

Von Dirk Kirchner
ibs schreiber gmbh, Hamburg

Werbemails sind lästig. Sie schöpfen auf raffinierte Art und Weise unsere Ressourcen ab. Ressourcen in Form von Zeit, Netzkapazitäten und Speichermedien. Außerdem ist durch den erhöhten E-Mail-Verkehr die proportionale Zunahme an Möglichkeiten, dass sich ein System mit Viren oder Trojanern infiziert, nicht zu unterschätzen.
Spam ist und wird auch zukünftig ein Problem unserer modernen Welt bleiben. Registrierte die Internetgemeinde doch gerade in den letzten Monaten eine verstärkte Zunahme von Aktivitäten auf diesem Sektor. In Zahlen und Fakten ausgedrückt bedeutet das gerade für die Unternehmen deutliche Verluste, wenn sie diese Form des unkontrollierten "Informationsflusses" zulassen.

Aber wie gelangt eine E-Mailadresse in die Verteiler dubioser Internetagenturen? Wie kann man sich davor schützen und was kann man tun, wenn das Kind schon in den Brunnen gefallen ist, also mein Postfach schier überläuft? Ist der von mir persönlich georderte Newsletter ebenso ein heimlicher Vertreter dieser Zunft wie die durch unsere Marketingabteilung letzte Woche versendete "Wir haben unsere Internetpräsenz für Sie überarbeitet" - Info-Mail an unsere Kunden?

Die Definition

Was ist Spam? Spam beschreibt eigentlich eine Fleischkonserve der Firma Hormel Foods (Spiced Porc and Ham). Es liegt nahe, dass der Verzehr des Inhaltes aus dieser Konserve wenig Anhänger fand. Nur so lässt sich die Namensentleihung für eine der unangenehmsten Begleiterscheinungen des Internet-Hypes erklären. Zurück aber zur Definition. Die Kommission der europäischen Gemeinschaften hat es folgendermaßen definiert: ‚Unter Spam versteht man unverlangt zugestellte Emails'. Diese Definition hat für mein Empfinden allerdings einen kleinen Schönheitsfehler: Denn wenn mir mein Freund aus Berlin eine E-Mail schickt, habe ich in den seltensten Fällen vorher darum gebeten. Mein Freund ein Spammer? Sicher nicht. Einigen wir uns also auf eine Definition, die der Volksmund formuliert hat und der unter Spam alle unerwünschten Mailsendungen versteht, die bei Ihnen oder bei mir im Postfach landen.

Die meisten Spams sind kommerziell und werden wegen der geringen Kosten für den Versender in großen Mengen verschickt. Die Zahlen reichen von 100.000 bis zu mehreren Millionen Exemplare pro Aktion. Nur die allein dadurch entstehenden Download-Kosten werden weltweit auf über 10 Milliarden Euro geschätzt. Übrigens geht der Internet-Dienstleistungsanbieter AOL davon aus, dass 30% aller versandten Nachrichten Spam sind.

Momentan kann man drei Typen unterscheiden:

- Kommerzieller Spam (UCE = Unsoliticed Commercial E-Mail)
- Kettenbriefe / Viruswarnungen (Hoaxes)
- Durch Viren versandte E-Mails

Kommerzieller Spam

Ein kommerzieller Spammer verfügt über riesige Datenbanken, bzw. kauft derartige Datenbestände mit oftmals mehreren Millionen Adressen von einschlägigen Internetagenturen auf. Die Betreiber gehen dabei ganz unterschiedliche Wege, um an die Adressen Ihrer Opfer zu kommen. Ein Verfahren dabei ähnelt sehr dem Vorgehen der Internet-Suchmaschinen. Kleinere Programme, auch Spider oder Robots genannt, durchforsten das gesamte Netz, um alle im Web vorhandenen HTML-Seiten (Webseiten) zu indizieren und thematisch zuzuordnen. Die Programme der Spammer gehen genauso vor. Ihr Interesse besteht aber vielmehr an E-Mailadressen, die sich eventuell in den Dokumenten befinden. Die Suche

nach dem Objekt der Begierde wird durch das charakteristische Klammeraffensymbol "@" in allen E-Mail-adressen für solche Programme zum Kinderspiel und stellt die Entwickler solcher Scripte nicht gerade vor grandiose Herausforderungen.

Manche ‚Agenturen' erraten auch die Adressen Ihrer ‚Kunden'. Dabei werden bekannte Domainnamen in Kombination mit Namenlisten (Dictionary's) nach dem Schema andreas@xyz.de, anton@xyz.de, bernd@xyz.de, ... regelrecht bombardiert. Die Erfolgsquote ist dabei erstaunlich hoch, wie Betroffene immer wieder feststellen müssen.

Damit unsere zweifelhafte Agentur nicht an den vielen Fehlermeldungen über unzustellbare E-Mails erstickt, schützt sie sich mit einer falschen Absenderadresse. Deshalb macht es auch wenig Sinn, eine Beschwerdemail an den vermeintlichen Absender zu schicken. In der Regel wird Ihr Enthusiasmus wenige Augenblicke später mit einer Unzustellbarkeitsmeldung Ihres Mail-Servers quittiert.

Trotzdem hinterlassen Spammer Spuren. Denn sie müssen in der E-Mail mindestens einen Hinweis auf ihren ‚Standort' hinterlegen, damit ihre Produkte oder Dienstleistungen zumindest theoretisch gekauft werden können. Allerdings sollten Sie niemals auf den Gedanken kommen, einen solchen Link in einer Spam-Mail anzuklicken. Spammer sind Lügner. Egal was ein solcher Link Ihnen suggeriert: Ein Klick kann der Beginn einer neuen Serie von Spam-Bekanntschaften sein. Gerade die verlinkten Hinweise auf Deaktivierung (Remove) eines Newsletters bewirken oft genau das Gegenteil. Denn damit signalisieren Sie dem Spammer, dass Sie existieren. Er wird Sie in einen gesonderten Index aufnehmen und Sie zukünftig besonders oft über ‚Neuigkeiten' informieren.

Wenn Sie also ernsthaft erwägen, eine Beschwerde zu formulieren, bleiben oftmals nur alternative Kommunikationsmethoden wie FAX, Telefon oder Postanschrift des Anbieters. Da hier aber wieder erhebliche Kosten auf den Betroffenen zukommen, nehmen viele Spam-Opfer von dieser Variante Abstand.

Sehr wirkungsvoll dagegen kann eine Beschwerde beim Provider des Spammers sein. Erste Hinweise auf diesen finden sie meist, wenn in der Spam-Mail eine Homepage des ‚Anbieters' referenziert ist. Nun müssen Sie nur noch mit einer WHOIS-Abfrage (z.B. http://www.denic.de) den technischen Ansprechpartner oder Zonenverwalter, also den gesuchten Provider, der Domain lokalisieren. Viele Provider neigen angesichts der angespannten wirtschaftlichen Situation dazu, solchen Quälgeistern sofort den Account zu sperren.

Wem das nicht reicht, der kann den E-Mail-Header noch etwas genauer untersuchen. Dort lassen sich bei genauerer Betrachtung oft noch Hinweise über die wahre Herkunft des Spams finden. Mehr Informationen zu diesem speziellen Thema finden Sie unter der Adresse http://sites.inka.de/ancalagon/faq/header-faq.php3

Kettenbriefe / Viruswarnungen

Mit Viruswarnungen oder Kettenbriefen hat früher oder später jeder einmal von uns zu tun. Wobei anzumerken ist, dass die Viruswarnungen, auch Hoaxes genannt, eine ganz besonders perfide Form des Kettenbriefes darstellen. Diese Mails können über einen längeren Zeitraum ganze Firmennetze lahm legen. Denn nicht selten lösen diese zweifelhaften Warnmeldungen eine emsige Massenaktivität des internen und externen Mailverkehrs aus. Hinzu kommen dann meist noch stundenlang belegte Telefonleitungen, da jeder als erstes den Administrator über die vermeintliche Bedrohung aus dem Netz informieren möchte. Wenig später wundern sich dann die ersten Mitarbeiter, dass ihr Postfach überläuft, seltsamerweise mit mehrfachen Exemplaren derselben Mail, die sie gerade vor wenigen Minuten selber weitergeleitet haben.

Diese Szenario ist ein klassisches Beispiel für den sogenannten Schneeballeffekt und kann die Ressourcen Ihres Firmennetzes empfindlich belasten.

Leiten Sie solche Mails niemals weiter. Es ist erwiesen, dass diese Form der ‚Aufklärung' die Verbreitung reeller Viren nicht wirklich bremst. Hier sollten Sie primär den Focus auf Ihren Virenscanner und insbesondere auf dessen Aktualität legen.

Bei anderen Kettenbriefen handelt es sich eher um Streiche oder Unkenntnis der Absender. Oft werden auch größere Geldsummen versprochen, wenn man eine bestimmte Anzahl von Kopien weiterleitet.

Was tun?

So, wie Sie nicht auf der Straße mit einem bedruckten T-Shirt umherlaufen, welches in großen Lettern Ihren Namen der neugierigen Umwelt verrät, so sollten Sie auch nicht leichtfertig mit Ihrer Email-Adresse ver-

fahren. Damit wir uns aber nicht missverstehen: So wie beispielsweise auf Ihr Haustürschild Ihr Name gehört, so gehört Ihre Emailadresse in das Impressum Ihrer Webseite.

Maskieren Sie die E-Mailadressen auf Ihrer Webseite!

- Möglichkeit 1

Fügen Sie Ihre E-Mail-Adresse(n) im Quelltext Ihres HTML-Dokumentes mit Leerzeichen zwischen den einzelnen Buchstaben ein.

Beispiel:

```
<a href=mailto:dirk@ibs - h a m b u
r g.com title=Schreiben Sie mir Ih-
re Meinung!>Mail an den Autor</a>
(Entfernen Sie die Leerzeichen…
```

Benanntes Beispiel würde sich für Ihre Kunden dann folgendermaßen darstellen:

Mail an den Autor (Entfernen Sie die Leerzeichen bevor Sie meine Mailadresse benutzen - Danke für Ihr Verständnis, aber ich bekomme sonst zu viele Spam-Mails / remove spaces to get a working email address - sorry, but I get too much spam otherwise)

Bei Aktivierung des Verweises öffnet sich wie gewohnt der lokale E-Mail-Client des Besuchers (siehe Abb. 1). Er muss lediglich die Leerzeichen entfernen bevor die Mail versendet wird. Für einen Spam-Robot ist diese Mailadresse jedoch zunächst völlig wertlos.

Abbildung 1

- Möglichkeit 2

Dies ist etwas komplizierter in der Durchführung, birgt dafür aber keinerlei Einschränkungen für die Besucher Ihrer Webseite.

Seit HTML 4.0 kann jedes Zeichen aus dem Zeichenvorrat nach ISO 10646 (deckungsgleich mit dem Unicode-Standard) notiert werden. Beliebige Zeichen aus diesem gewaltigen Zeichenvorrat können durch eine spezielle numerische Notation erzeugt werden. (siehe Abb. 2).

A	A	a	a	-	-
B	B	b	b	.	.
C	C	c	c	/	/
D	D	d	d	0	0
E	E	e	e	1	1
F	F	f	f	2	2
G	G	g	g	3	3
H	H	h	h	4	4
I	I	i	i	5	5
J	J	j	j	6	6
K	K	k	k	7	7
L	L	l	l	8	8
M	M	m	m	9	9
N	N	n	n	@	@
O	O	o	o	_	_
P	P	p	p		
Q	Q	q	q		
R	R	r	r		
S	S	s	s		
T	T	t	t		
U	U	u	u		
V	V	v	v		
W	W	w	w		
X	X	x	x		
Y	Y	y	y		
Z	Z	z	z		

/php4/php.exe/home/schnipsel/zeichen.php © Kirchner

Abbildung 2

Beispiel:

```
&#100;&#105;&#114;&#107;&#64;&#105;
&#98;&#115;&#45;&#104;&#97;&#109;&#
98;&#117;&#114;&#103;&#46;&#99;&#11
1;&#109;
```

Im HTML-Quelltext hinterlegt ergibt diese Zeichenkette dann im Browser wieder:

```
dirk@ibs-hamburg.com
```

Das komplette Beispiel:

```
<a href="mailto:
&#100;&#105;&#114;&#107;&#64;&#105;
&#98;&#115;&#45;&#104;&#97;&#109;&#
98;&#117;&#114;&#103;&#46;&#99;&#11
1;&#109;">Mail an den Autor</a>
```

Da die Programme der Spammer technisch bedingt nur den HTML-Quelltext durchsuchen können, bleibt

Ihre Suche nach Anwendung dieser Methode oftmals erfolglos. Für den Besucher Ihrer Webseite ergeben sich jedoch keinerlei Einschränkungen.

Wem die Codierung nach Tabelle zu mühselig ist, der kann sich unter http://ibs-schreiber-gmbh.de/nospam.php seine E-Mailadresse bequem nach dieser Methode ‚verschlüsseln' lassen.

Alternativ können Sie auch folgendes JavaScript (Listing 1) in einer Windowsumgebung erstellen. Sie müssen das Listing lediglich als HTML-Dokument (Dateiextension *.htm oder *.html) abspeichern und anschließend per Doppelklick ‚ausführen'. Ihr Browser (Vorzugsweise Internet Explorer ab Version 5) wird nun ein einfaches Formular darstellen, mit dessen Hilfe Sie ganz bequem Ihre E-Mailadresse codieren können. Der besondere Clou: Das Script kopiert das Generat automatisch in Ihre Zwischenablage und stellt es somit anderen Anwendungen zur Verfügung.

Unterstützen Sie potenzielle Spammer nicht durch falsche Handhabung Ihres E-Mail-Clients

Es ist immer wieder erstaunlich wie viele Zeitgenossen leichtfertig andere E-Mailadressen in den Umlauf bringen. Gemeint ist hier Gebrauch des sogenannten CC (Carbon Copy) - Feldes um die E-Mail an mehrere Empfänger zu versenden. Der Nachteil bei diesem Verfahren liegt auf der Hand: Praktisch jeder Empfänger sieht die E-Mailadresse der anderen Teilnehmer. Egal ob sich die Teilnehmer untereinander kennen oder nicht. Mal abgesehen von der Zulieferungsgefahr für Spam-Datenbanken, können so andere Personen Rückschlüsse über geschäftliche oder private Kontakte der anderen ‚Betroffenen' ziehen. Kurz: Diese Vorgehensweise ist ein klarer Verstoß gegen geltendes Datenschutzrecht.

Abhilfe schafft hier das BCC (Blind Carbon Copy) - Feld. Wie der Name schon verrät, handelt es sich

```
 1  <html>
 2  <head>
 3  <title> E-Mail maskieren </title>
 4  <script>
 5  function G(){
 6    var result = "";
 7    for (i = 0; i < document.f.q.value.length; i++)
 8      result += '&#' + document.f.q.value.charCodeAt(i) + ';';
 9    document.f.q.value = result;
10    document.f.q.select();
11    s = document.selection.createRange();
12    window.clipboardData.setData("Text",s.text);
13  }
14  </script>
15  </head>
16  <body>
17  <form name=f>
18  <textarea name=q cols=50 rows=8></textarea>
19  <br><br>
20  <input type=button value=Generate onClick="G();">
21  </form>
22  </body>
23  </html>
```

Listing 1

hierbei um "blinde" oder "verdeckte" Kopien. Technisch gesehen wird zunächst genau eine Mail an den Mail-Server geschickt. Dort angekommen, kümmert sich dieser dann um die Vervielfältigung und Versendung an die einzelnen Adressaten.

Wenn in Ihrem Unternehmen Mail-Anwendungen laufen, die diese Option nicht unterstützen, so sind diese schlicht für betriebliche Zwecke ungeeignet.

Unter Microsoft Outlook ist diese Option standardmäßig zunächst ausgeblendet. Um diese zu aktivieren gehen Sie so vor: Starten Sie mit Neu/Neue E-Mail-Nachricht. Gehen Sie nun in das Menü <Ansicht> aktivieren Sie dort den Menüpunkt "BCC". (Sie Abb. 3 und 4)

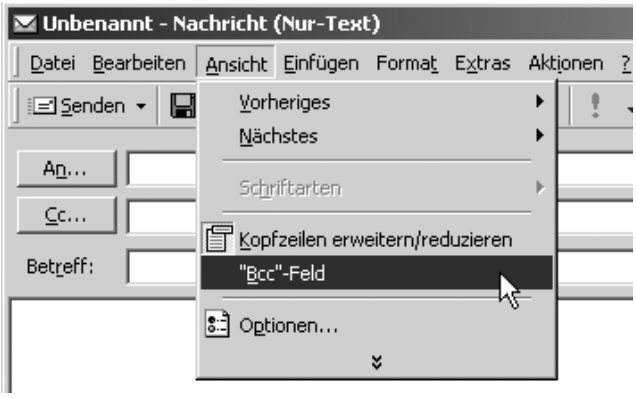


Abbildung 3

Abbildung 4

Fazit

Bedenken Sie stets, dass Ihre Aktivitäten im Web irgendwann im Hinblick auf die Spam-Problematik Konsequenzen haben werden. Das beginnt beim simplen Ausfüllen von Eingabeformularen und endet mit Ihrem Engagement in irgend einer Newsgroup. Verwenden Sie für dieses ‚Einsatzgebiet' am Besten eine extra E-Mailadresse. Wenn Sie Besitzer einer eigenen Domain sind, bietet sich auch eine sogenannte Filter-E-Mail an. In der Regel verfügen Sie als Besitzer einer Domain über mehrere frei belegbare POP3-Konten. Erstellen Sie beispielsweise ein Konto nach dem Schema filter@meinedomain.de. Verwenden Sie diese Adresse bei allen zweifelhaften Interaktionen im Netz. Nun brauchen Sie nur noch Ihre lokale E-Mail-Anwendung für diesen ‚unsicheren' Kandidaten konfigurieren. Leiten Sie Mails, die an diese Adresse gerichtet sind, zum Beispiel in einen separaten Ordner. Oder dirigieren Sie diese auf direktem Wege in den Papierkorb Ihrer Anwendung.

Geschäftsschädigende Handlungen Wo sind schwarze Schafe? oder Ist die Revision ein ungeliebtes Stiefkind?

Von Frank Haub
Geschäftsführer HAUB + PARTNER GmbH, Hamburg

Überteuerte Einkäufe im Beschaffungswesen. Fehlplanungen bei Bauinvestitionen. Bestechliche Mitarbeiter. Unterschlagungen im Finanzbereich. Wirtschaftskriminalität. Luftbuchungen. Geschönte Statistiken. Fast täglich hören wir von solchen Vorgängen.
Was passiert hinter den Kulissen? Warum sind diese teils spektakulären Fälle möglich? Ist das Entdeckungsrisiko so gering? Hat doch die Unternehmensleitung dafür zu sorgen, dass ausreichende Überwachungssysteme eingerichtet sind und mögliche Schwachstellen rechtzeitig genug aufgedeckt werden!?

Ein wesentliches Führungsinstrument ist die Interne Revision auf die in diesem Beitrag näher eingegangen werden soll. Die Mitarbeiter in dieser Abteilung sind zuständig für die Überwachung der Abläufe, die Sicherung des Firmenvermögens, die Wirtschaftlichkeit und Sicherheit aller Vorgänge im Unternehmen.

In großen und mittleren Firmen ist das eine Selbstverständlichkeit. Seit 1998 schreibt sogar ein Gesetz, das KonTraG (Kontroll- und Transparenzgesetz in Unternehmensbereichen) vor, dass ein "angemessenes" Überwachungssystem eingerichtet sein muss. Zunehmend sind in neuerer Zeit aber auch Revisoren in öffentlichen Institutionen, Bundes- und Landesministerien, ja sogar in den politischen Parteien anzutreffen.

Zum Begriff "Geschäftsschädigende Handlungen"

Sie liegen dann vor, wenn eine absichtliche Schädigung gegeben ist, z.B. durch:

- Diebstahl, Betrug, unberechtigter Einblick in Datenbestände
- Untreue, Unterschlagung
- Bestechung, Schmiergelder
- Beleg- und Urkundenfälschung
- Eigene Vorteilsnahme oder durch Dritte

Eine geschäftsschädigende Handlung muss nicht strafbar sein, nämlich dann, wenn es an einer gesetzlichen Grundlage fehlt.

Wann ist eine Veruntreuung zu beanstanden? Wo liegt die Toleranzgrenze?

Kriterien hierzu sind:

- Art des Schadens (z.B. auch Zeitdiebstahl)
- Anzahl der Fälle
- Wertmäßige Größenordnung
- Bewusster oder unbeabsichtigter Fehler

Der Defraudant wird eine Veruntreuung nicht zugeben, weil sein Unrechtsbewusstsein niedrig oder gar nicht vorhanden ist.

Praktische Schwierigkeiten bei den Grauzonen

Handelt es sich um Wirtschaftsdelikte oder sind sie noch zu akzeptieren?

- Unethisches Verhalten
  verstößt nicht gegen Rechtsnormen, sondern gegen die Ethik, "ist das üblich?", akzeptiert die Unternehmensleitung das Verhalten?

- Riskantes Verhalten
  ist noch kein Wirtschaftsdelikt, Risiken und Gefahr von Verlusten wird bewusst in Kauf genommen. Gemeint ist auch die Sorglosigkeit

- Betriebswirtschaftlich fragwürdiges Verhalten

widerspricht wirtschaftlichen Grundsätzen wie z.B. Verzicht auf Abschreibungen, Unterlassungen von Ausgaben für Forschung und Entwicklung

↖ Missmanagement

...„Dolose Handlungen finden auch zum Vorteil des Unternehmens statt“...

ist schwierig zu orten: teure EDV-Lösungen, permanente Reorganisationen, Leistungsbedarf ohne realen Grund ("Geld wird sowieso unnütz verschleudert")

Dolose Handlungen finden auch zum Vorteil des Unternehmens statt. Solche "positiven" Handlungen beruhen im allgemeinen auf der Ausnutzung von Vorteilen, die auf unehrliche Art und Weise erworben wurden. Sie sind oft mit Täuschung Außenstehender verbunden.

Beispiele:

- Schmiergeld- und Bestechungszahlungen an Kunden, Behörden und Top-Entscheider
- Illegale Geschäfte, die gegen Gesetze, Vorschriften, Verordnungen verstoßen
- Vorsätzlich unrichtige Festsetzung von Verrechnungspreisen, z.B. für den Güter- und Dienstleistungsaustausch zwischen verbundenen Unternehmen
- Steuerhinterziehung und/oder -umgehung
- Vorenthalten wichtiger (negativer) Informationen, um die finanzielle Situation des Unternehmens gegenüber Dritten zu beschönigen ("Fensterputzen")

Zusammenfassung

Dieser im groben beschriebene große Graubereich bedeutet eine zusätzliche Herausforderung für die Revision. Ein riskantes Geschäft, das im Nachhinein einen Gewinn abwirft, stellt für die Revision kein Problem dar. Verursacht es hingegen einen Verlust, dann gerät der Prüfer möglicherweise schnell unter einen Rechtfertigungsdruck.

Leitlinien des prüferischen Verhaltens ist der präventive Vermögensschutz und nicht die Ermittlung der Strafbarkeit der Täter. Wir müssen also daher den Begriff "Wirtschaftsdelikt" weiterziehen als bei einer rein strafrechtlichen Betrachtungsweise.

Die häufigsten Unterschlagungsbereiche

Aus der Erfahrung des Verfassers sind folgende Unternehmensfunktionen besonders gefährdet:

Rechnungswesen

- Provisionen
- Kassen, Zahlungsverkehr
- Lohn- und Gehaltsabrechnung, -buchhaltung

Vertriebsbereich

- Verkauf
- Versand
- Kundendienst

Einkaufsbereich

- Einkaufsabteilung
- Wareneingang
- Ersatzteilwesen

Bauwesen

- Unberechtigte Abrechnungen, Abrechnungen nicht erbrachter Leistungen
- Doppelabrechnungen
- Abnahme/ -Aufmassmängel

sonstige Bereiche

- Außenstelle
- Speditionen

Bereich der Computerkriminalität

Die am häufigsten vorkommenden Delikte

- unberechtigter Einblick in Datenbestände
- Programmfälschungen
- Eingabemanipulationen
- Datendiebstahl

Ebenfalls aus der Erfahrung des Verfassers sind folgende Gegenstände und Leistungen im Unternehmen

1.	Schreibzeug	Hand- und Elektrowerkzeuge
2.	Büromaterial	Magazin- und Lagermaterial
3.	Bürogeräte und -maschinen	Technische Geräte und Apparaturen
4.	Bar- und Giralgeld, Wertpapiere	Edelmetalle
5.	Forderungen und Verbindlichkeiten	Gebrauchsgüter aller Art
6.	Telefongespräche, Porto, Warenmuster, Werbegeschenke	
7.	Nicht bestandsmäßig geführte bzw. bereits abgeschriebende Vermögenswerte	
8.	Leistungen der verschiedensten Art, die unmittelbar über Aufwand verbucht werden	
9.	Zeitdiebstahl in der unterschiedlichsten Form	
10.	Reperaturen und Instandsetzungen für den persönlichen Bereich	
11.	Einsatz von Mitarbeitern und Firmenressourcen für private bzw. nicht geschäftsbedingte Zwecke	
12.	Geschäftsfahrten und Geschäftsreisen, die privater bzw. nicht geschäftsbedingter Natur sind	
13.	Bewirtung, Spesen und Repräsentationsaufwendungen	
14.	Inanspruchnahme abteilungs- bzw. funktionsspezifischer Firmenressourcen für andere als geschäftsbedingte Zwecke	
15.	Information der unterschiedlichsten Art zur Erreichung persönlicher Vorteile	

gefährdet, weil ein relativ großer Personenkreis Zugriff auf sie nehmen kann:

Zugriffsmöglichkeiten in den Bereichen

Anfälligkeiten-Katalog

1. Beschaffungswesen
2. Auftragsvergabe durch Fachabteilung (Bau, EDV, Werbung, F+E)
3. Bank- und Kassenvollmachten
4. Außenstellen ("Ein-Mann"-Filialen, Außendienst)
5. IKS-Schwächen (keine Dreiteilung Vorgänge bearbeiten, Bestände verwalten, Vorfälle buchen)

Auffälligkeiten-Katalog

Zu den Problemen privater Natur können gehören...

- Scheidung, Trennung, Tod eines nahestehenden Menschen
- Suchtkrankheiten wie Alkohol, Drogen, Glücksspiel-, Wettsucht
- Zahlungsschwierigkeiten, Verschuldung

Probleme am Arbeitsplatz können u.a. auftreten durch:

- Unzufriedenheit am Arbeitsplatz
- Mangelnde Aufstiegsmöglichkeiten
- Eine "Außenseiter"-Rolle

Anhaltspunkte für die Unangemessenheit des Lebensstandards bieten:

- Bedeutender Grundbesitz (Mehrfamilienhaus, Ferienhäuser, Eigentumswohnung, Luxusvilla)

Zur Annahme von Vorteilen

Voraussetzungen für die Annahme	• Besonderer detailliert festgelegter Anlaß • Einhalten der vorgegebenen Wertgrenze • Mitteilung an Vorgesetzte
Problematik	• Wertgrenze: geringes (?) Überschreiten; Preismanipulation; mangelnde Kenntnis • Unvollständigkeit der Anlaßmöglichkeiten Großzügiges Auslegen der Regeln
Risiko	• "Anfüttern": klein anfangen - ohne Gegenleistung; daran gewöhnen - ohne Gegenleistung; langsam steigern - mit Gegenleistung
Lösungsansätze	• "Null"-Lösung = grs. Ablehnen der Annehmlichkeiten und Geschenke • Entgegennahme unter bestimmten Voraussetzungen - gfs. Weitergabe • Entwickeln höherer Sensibilität hinsichtlich Anfüttern, Unangemessenheit, „Bösen" Absichten und Risiken
Grenzfälle (z.B.)	Einladungen, Richtfest, Dankesgaben, "Höflichkeiten","Aufmerksamkeiten"

„...bei manchen Feststellungen wird die Grauzone zwischen Veruntreuung, unwirtschaftlichem und unethischem Verhalten deutlich...“

- Auffällige andere Besitzgüter (Zweit- und Drittwagen, Sportwagen, Segelyacht, Motorboot, "Luxusschlitten")
- Kostenaufwendige Hobbys (Sportfliegen, Ozeanregatta, Antiquitätensammlung, Bayreuth-Premierenbesuche)

Beispiele wichtiger Prüfungsfeststellungen

Nach Prüfungsfeldern geordnet werden Beispiele aus der Praxis des Verfassers als wichtige und interessante Prüfungsfeststellungen dargestellt. Es ist unschwer zu erkennen, dass bei manchen Feststellungen die Grauzone zwischen Veruntreuung, unwirtschaftlichem und unethischem Verhalten deutlich wird (siehe auch Ausführungen unter Punkt 1.2.).

Wirtschaftlichkeit des Einkaufs

- Durch falsch eingeschätzten Bedarf oder Markt Überbestellungen
- Durch falsche Disposition Überbestände
- Durch zu vorsichtige Einschätzung keine oder zu niedrige Lieferbereitschaft
- Liefertermine werden nicht eingehalten
- Bestellungen von nicht notwendigen oder nicht benötigten Waren
- Artikelpreise sind zu hoch
- Von Revision eingeholte Angebote sind günstiger als die vom Einkauf
- Eigenfertigung bzw. -regie ist kostengünstiger als Fremdbezug oder umgekehrt
- Eigener Fuhrpark teurer als ein Fremdspediteur oder umgekehrt

Schwächen in der Rechnungskontrolle

- Zahlung von Rechnungen ohne Wareneingangs- bzw. Leistungsbestätigung
- Wareneingangsbestätigung liegt vor, aber mangelhafte WE-Kontrolle
- Keine Skontoausnutzung durch falsche oder schleppende Bearbeitung
- Kein Vieraugenprinzip bei Zahlung
- Bestell- und Einkaufskonditionen sowie Preise stimmen nicht mit Rechnung überein
- Lieferungen, Leistungen, Kosten werden doppelt berechnet und auch bezahlt
- Gutschriften des Lieferanten werden nicht als solche erkannt und bezahlt

Administrative Mängel mit möglichen finanziellen Auswirkungen im Bereich Bauleistungen

- Keine Ausschreibungen, Wettbewerbsangebote nicht eingeholt
- Angebote unvollständig, nicht vergleichbar oder nicht schriftlich
- Einseitige Bevorzugung der Haus- und Hoflieferanten
- Stundenlohnarbeiten werden nicht überwacht oder vermischt mit Pauschalarbeiten, damit zusätzliche unberechtigte Berechnung
- Keine Nachtragsaufträge für Leistungserweiterungen
- Berechnete Leistungen und/oder Aufmasse höher als Angebot angegeben
- Abschläge ohne Leistungsaufmass
- Schlussrechnungen ungenügend und ohne Aufmasse geprüft

Manipulation von Rechnungen

- Wareneingangsstelle bestätigt höhere Menge als geliefert
- Höherer Preis auf Rechnung als vereinbart
- Rechnerische Fehler (Addition, Multiplikation)
- Zusätzliche Mengen auf Rechnung akzeptiert ohne tatsächlichen Eingang
- Mengeneinheiten falsch berechnet
- Zahlung von zusätzlichen unberechtigten Rechnungen
- Bewusste oder unbewusste Mehrfachzahlung einer Rechnung
- Veränderung der Rechnung in Absprache mit Lieferanten, die nicht mit Lieferung und Preisvereinbarung übereinstimmt

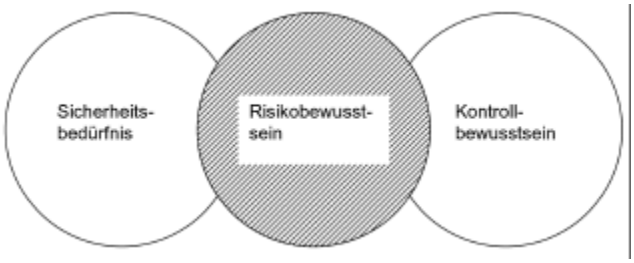
Aufgaben und Grenzen der Unterschlagungsprophylaxe

Ziel der Internen Revision muss es sein, durch Überwachungsmaßnahmen Schäden vom Unternehmen abzuwenden.

- Qualifizierte Prüfungsplanung
- Revisor ist Risikoanalytiker
- Kein Naturschutzparksyndrom

Allerdings sind Risiken nicht quantifizierbar und Sicherheit und Wirtschaftlichkeit wiedersprechen sich

Es kann nicht Aufgabe der Revision sein, Unterschlagung zu verhindern. Aber durch das Aufspüren



von Löchern im IKS, Nichtbeachten von Richtlinien und Vorschriften muss es den Defraudanten ganz schwer gemacht werden!

Im Unternehmen gibt es das

=> Sicherheitsbedürfnis

welches vom geprüften bestimmt wird und es gibt das

=> Kontrollbewusstsein
=> Welches vom Prüfer beeinflusst wird#

Die Summe von Sicherheitsbedürfnis und Kontrollbewusstsein ergibt das

=> Risikobewusstsein

Aufgabe der Revision ist es festzustellen, ob

- Ausreichende Sicherheitsmaßnahmen und -vorkehrungen zur Vermeidung bzw. Aufdeckung möglicher Fehler vorhanden sind (Soll)
- Die vorgesehenen Sicherungsmaßnahmen auch eingehalten sind (ist)
- Die Kontrollkästen den Wert des Risikos nicht übersteigen

Oder gar ein "Kontrollverkill" betrieben wird, der dazu führen kann, dass niemand mehr seriös kontrolliert, weil jeder annimmt, der andere würde es tun.

Wenn geschäftsschädigende Handlungen auftreten, wird immer wieder beobachtet, dass der Hauptgrund darin liegt, dass Funktionstrennungen nicht eingehalten worden sind. Dem Vieraugenprinzip wird heute auch eine noch nicht zu unterschätzende präventive Wirkung zugeschrieben. Je mehr Personen sich an dolosen Handlungen beteiligen, desto weniger lassen sich diese auf Dauer verheimlichen. Einige interessante Beispiele für Funktionstrennungen:

- Niemand darf sich selbst etwas genehmigen
- Wer Geld verwaltet, soll nicht auch buchen dürfen (z.B. Bankvollmacht, Treasurer)
- Besteller darf nicht gleich Annehmer sein

„...es wird schon nichts passieren...“

- Wareneingang, Einkauf, Rechnungsprüfung müssen voneinander unabhängig sein
- Verursacher (z.B. Einkäufer) darf nicht Rechnung zur Zahlung anweisen
- Rechnungsprüfung muss eine andere als die auslösende Stelle sein
- Aufnehmender und Kontrollierender dürfen nicht eine Person sein

Warum sind in Unternehmen Risiken durch geeignete Sicherungsmaßnahmen nicht oder nicht ausreichend abgedeckt? Aus drei Gründen:

- o Sicherheit kostet Geld; es gibt sie nicht zum Nulltarif. Sicherheit und Wirtschaftlichkeit widersprechen sich.
- o Unternehmer sein heißt - wie der Begriff schon sagt - etwas zu unternehmen und damit ein Risiko einzugehen. Unternehmer ("Es wird schon nichts passieren") haben eine andere Denkweise als Revisoren ("Es kann ständig etwas passieren").
- o Risiken lassen sich nicht ausrechnen, sie sind nicht qualifizierbar. Viele Risiken würden nicht bestehen, könnten sie rechnerisch ermittelt werden. Man denke allein an das "Risiko Mensch". Die ganz großen Risiken der Menschheit wie z.B. Atomkraftwerke sind nicht versicherbar.

o Aus diesen Gründen ist es eine ganz wichtige Aufgabe der Revision aufzuzeigen, wo Risiken durch fehlende IKS gegeben sind und wie groß sie sind. Wenn unter Revisoren diskutiert wird, den "angestaubten" Begriff "Revision" einmal auszuwechseln, könnte an dieser Stelle vorgeschlagen werden, ein Abteilungsschild "Risikoanalyse" statt "Revision" an die Tür zu hängen.

Möglichkeiten der Vermeidung doloser Handlungen

Im folgenden sollen einige Gedanken gesammelt und zu Thesen aufgestellt werden, wie zukünftig geschäftsschädigende Handlungen vermieden werden oder mindestens besser eingedämmt werden können.

Aus der Sicht des Unternehmens:

- Es muss eine größere Sensibilisierung des Risikobewusstseins stattfinden. Das Unrechtsbewusstsein muss wieder größer werden durch das Aufstellen von Verhaltenskodexen, Company Policies usw.
- Die Personalauswahl und damit die Personalpolitik muss sorgfältiger werden. Bei der Personalauswahl muss neben den fachlichen Vorraussetzungen besonders die Zuverlässigkeit und Vertrauenswürdigkeit beurteilt und geprüft werden.
- Die Stabsabteilung Interne Revision ist quantitativ besser auszustatten
- Es sollten Überlegungen angestellt werden, wie die Revision eine noch größere Unabhängigkeit erreicht, z.B. durch die Unterstellung beim Aufsichtsrat oder durch die Bildung eines Audit-Comitees.

Sichtweise durch die Revision

- Durch höhere Anforderungen an den Revisor bessere Ausbildung anbieten und garantieren
- Noch mehr ex-ante Prüfungen, d.h. dort projektbegleitende Prüfungen ansetzen, wo "noch etwas zu retten ist", z.B. bei Bauprüfungen

IBS *Prüfen mit Konzept*

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 Wagener, IBS, Hamburg

Termin und Ort:

05.- 06. September 2002,
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
Vera Sievers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -16
schriftl.: IBS, Friedrich-Ebert-Damm 145, 22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: seminare@ibs-hamburg.com
Die Seminarnummer ist **R3GB**.

IBS *Prüfen mit Konzept*

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 Wagener, IBS, Hamburg,

Termin und Ort:

12. 13. September 2002,
Montag 09:30-17:00 Uhr,
Dienstag 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
Vera Sievers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -16
schriftl.: IBS, Friedrich-Ebert-Damm 145, 22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: sales@ibs-hamburg.com
Die Seminarnummer ist **R3BK**.

IBS *Prüfen mit Konzept*

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:

18.- 20. September 2002,
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
Vera Sievers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -16
schriftl.: IBS, Friedrich-Ebert-Damm 145, 22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: seminare@ibs-hamburg.com
Die Seminarnummer ist **R3SY**.

IBS *Prüfen mit Konzept*

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:

09.- 11. September 2002,
Montag 09:30-17:00 Uhr,
Dienstag 09:00-17:00 Uhr
Mittwoch 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
Vera Sievers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -16
schriftl.: IBS, Friedrich-Ebert-Damm 145, 22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: seminare@ibs-hamburg.com
Die Seminarnummer ist **GMPR**.

IBS *Prüfen mit Konzept*

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 Wagener, IBS, Hamburg

Termin und Ort:

26.- 27. September 2002,
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
Vera Sievers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -16
schriftl.: IBS, Friedrich-Ebert-Damm 145, 22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: seminare@ibs-hamburg.com
Die Seminarnummer ist **R3FI**.

IBS *Prüfen mit Konzept*

Ordnungsmäßigkeit und Prüfung von Dokumentenmanagement- und Archiv-Systemen

Spezialseminar

Inhalte u.a.:

Dieses Seminar vermittelt notwendiges Wissen über die Einführungsplanung und Realisierung von elektronischen Archiven und Dokumentenmanagement Systemen.

- Prüfungsmethoden und -grundlagen
- Rechtliches Umfeld (GDPdU)
- DMS- und Archivierungssysteme
- Aufbau / Prüfung am Beispiel PBS, iOXS

Der Referent:

Ralf Salomon, KPMG, Mannheim

Termin und Ort:

09.- 11. September 2002,
Montag 09:30-17:00 Uhr,
Dienstag 09:00-17:00 Uhr
Mittwoch 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
Vera Sievers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -16
schriftl.: IBS, Friedrich-Ebert-Damm 145, 22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: seminare@ibs-hamburg.com
Die Seminarnummer ist **DSDM**.

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:

21.- 23. Oktober 2002
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 Datenschutzbeauftragte

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Vera Sievers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -16
schriftl.: IBS, Friedrich-Ebert-Damm 145, 22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: seminare@ibs-hamburg.com
Die Seminarnummer ist **DSNT**.

IBS *Prüfen mit Konzept*

Kostenrechnung und Kostenmanagement

Inhalte u.a.:

- Grundlagen derbKostenrechnung
- Teilbereiche der Kostenrechnung
- Moderne Gestaltungsformen der Kostenrechnung
- Planungs- und Kontrollrechnungen auf der Grundlage von Kosten und Leistungen
- Systemrichtlinien
- Konzepte zur Kostenbeeinflussung

Der Referent:

Prof. Dr. Carl-Christian Freidank,
IWSt der Universität Hamburg

Termin und Ort:

10.- 11. September 2002
Dienstag 09:30-17:00 Uhr,
Mittwoch 09:00- ca. 16:00 Uhr,
im IBS-Schulungscenter,
Hamburg, Friedrich-Ebert-Damm 145.

Teilnehmer:

Interne u. externe Prüfer, Controller, Steuer- und Unternehmensberater

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Vera Sievers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -16
schriftl.: IBS, Friedrich-Ebert-Damm 145, 22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: seminare@ibs-hamburg.com
Die Seminarnummer ist **GMKK**.

IBS *Prüfen mit Konzept*

Prüfung bilanzieller Herstellungskosten

Inhalte u.a.:

- Herstellungskosten und Maßgeblichkeitsprinzip
- Fallstudie zur Prüfung der Herstellungskosten
- Korrektur der Herstellungskosten bei Normal-, Plan- und Teilkostenrechnung
- Herstellungskosten bei Prozeßkostenrechnung
- Gesamt- und Umsatzkostenverfahren als alternative Formen der Erfolgsrechnung

Der Referent:

Prof. Dr. Carl-Christian Freidank,
IWSt der Universität Hamburg

Termin und Ort:

16.- 17. September 2002
Montag 09:30-17:00 Uhr,
Dienstag 09:00-17:30 Uhr,
im IBS-Schulungscenter,
Hamburg, Friedrich-Ebert-Damm 145.

Teilnehmer:

Revisoren und Datenschutzbeauftragte

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Vera Sievers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -16
schriftl.: IBS, Friedrich-Ebert-Damm 145, 22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: seminare@ibs-hamburg.com
Die Seminarnummer ist **GMHK**.

IBS *Prüfen mit Konzept*

Nutzung des AIS für die Prüfung

Inhalte u.a.:

- Einführung in das AIS
- Erstellung diverser Sichter auf das AIS
- Funktionalität
- Auswertung
- Einführung in Auswertungsmöglickeiten des SAP R/3 Systems via Datentransport in: EXCEL, WINIDEA, ACL usw.

Der Referent:

Mariel-Luise Wagener,
IBS Hamburg

Termin und Ort:

19.- 20. September 2002
Donnerstag 09:30-17:00 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
Vera Sievers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -16
schriftl.: IBS, Friedrich-Ebert-Damm 145, 22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: seminare@ibs-hamburg.com
Die Seminarnummer ist **R3IS**.

IBS *Prüfen mit Konzept*

Prüfen heterogener Netzwerke + Internet/Intranet

Inhalte u.a.:

- Infrastrukturen
- Kopplungselemente
- Standardprotokolle
- Firewalls
- Datenschutz- und Datensicherheitseinrichtungen
- Internet Intranet-Dienste
- Prüffähigkeit der IT-Revision
- IT-gestützte Werkzeuge zur Prüfung

Die Referenten:

Michael Foth, Siemens AG Hamburg
Stefan Hölzner, KPMG Essen

Termin und Ort:

25.- 27. November 2002
Mittwoch 09:30-17:00 Uhr,
Donnerstag 09:00-17:00 Uhr
Freitag 09:00-ca. 15:30 Uhr
im IBS-Schulungscenter,
Hamburg, Friedrich-Ebert-Damm 145.

Teilnehmer:

Revisoren und Datenschutzbeauftragte

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Vera Sievers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -16
schriftl.: IBS, Friedrich-Ebert-Damm 145, 22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: seminare@ibs-hamburg.com
Die Seminarnummer ist **DSHN**.

IBS *Prüfen mit Konzept*

Lotus Notes für Revisoren

Inhalte u.a.:

- Konzeptionierung
- LN-Datenbanken
- Server- + Client-Sicherheit
- Datenbanksicherheit
- Datenbankentwicklung
- Replikation
- Programmierumgebung und -sprachen
- Die wichtigsten Elemente einer Lotus Notes-Datenbank

Der Referent:

Norbert Fußer, LANtana
Lotus Notes Consulting und Training Bereichsleiter

Termin und Ort:

20.- 22. November 2002
Mittwoch 09:30-17:00 Uhr,
Donnerstag 09:00-17:00 Uhr
Freitag 09:00-ca. 15:30 Uhr
im IBS-Schulungscenter,
Hamburg, Friedrich-Ebert-Damm 145.

Teilnehmer:

Revisoren und Datenschutzbeauftragte

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Vera Sievers
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (040) 69 69 85 -16
schriftl.: IBS, Friedrich-Ebert-Damm 145, 22047 Hamburg
per Fax: (040) 69 69 8 5-31
eMail: seminare@ibs-hamburg.com
Die Seminarnummer ist **DSLN**.

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft e.V.

Intensiv-Training für Datenschutzbeauftragte

Grundlagenseminar

Inhalte u.a.:

- Das Bundesdatenschutzgesetz vom 23. Mai 2001
- Der Datenschutzbeauftragte
- Die Aufgaben des Datenschutzbeauftragtem
- Outsourcing und Datenschutz
- Datenschutz und neue Medien

Die Referenten:

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:

19.- 20. Juni 2002
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 **020626**.

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft e.V.

Intensivseminar:

Was muss ein Datenschutzbeauftragter bei vernetzten Systemen beachten?

Inhalte u.a.:

- DV-technische Grundlagen
- Datenschutzrechtliche Grundlagen bei vernetzten Systemen
- Umsetzung der Datenschutzbestimmungen
- Richtlinien im PC-Bereich
- Checklisten für den Datenschutz
- Datenschutzaudit
- Datenschutz und Internet

Die Referenten:

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

Termin und Ort:

16.- 17. Oktober 2002
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 **021042**

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft e.V.

Datenschutz und Bankgeheimnis

Spezialseminar für Kreditinstitute

Inhalte u.a.:

- Grundlagen
- SCHUFA-Verfahren
- Bank-zu-Bank Auskunft über Kunden an Dritte aus Sicht des BDSG
- Auskunftserteilung an Betroffene
- Konzerndatenhaltung und Übermittlungsbegriff nach § 28 BDSG
- Datenschutz-Klauseln bei Rechtsvorschriften
- Outsourcings nach BDSG und KWG
- Cold Calling
- Entsorgung von Geschäftspapieren und Datenträgern

Der Referent:

Dipl.-Volkswirt Friedhelm Wolf, Dresdner Bank AG, Frankfurt am Main

Termin und Ort:

07. November 2002,
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 **021141**.

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft e.V.

Bundesdatenschutzgesetz

Inhalte u.a.:

- Intensiv-Überblick über das neue Bundesdatenschutzgesetz
- Datenschutz bei Multimedia
- Organisation des Datenschutzes
- Datenschutzaspekte beim Einsatz von Personal-Computern (stand alone und in vernetzten Systemen)
- Datenverarbeitung im Unternehmensverbund
- Neueste Rechtsprechung

Die Referenten:

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

Termin und Ort:

25.- 26. September 2002,
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Teilnehmer:

Datenschutzbeauftragte, Mitarbeiter der Revision und der Personalabteilung

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee.
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 **020932**.

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft e.V.

Datenschutz und Multimedia

Inhalte u.a.:

Grundlagen

- Datenschutz und Fernmeldegeheimnis
- Die bereichsspezifischen Regelungen im Multimediabereich
- Unterschiede zu den Regelungen des Bundesdatenschutzgesetzes

Regelungen im Multimediabereich

Die Nutzung der neuen Medien

Die Referenten:

Horst Olpe, Datenschutz Arcor AG & Co., Eschborn
Dipl.-Volksw. Friedhelm Wolf, Konzerndatenschutz, Dresdner Bank AG, Frankfurt am Main

Termin und Ort:

13. November 2002,
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 **021142** .

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft e.V.

Einführung in das Bankgeschäft

Inhalte u.a.:

- Banken im Wirtschaftskreislauf
- Inlandszahlungsverkehr
- Kreditgeschäft
- Außenhandel
- Kontoführung
- Passivgeschäft
- Wertpapiergeschäft
- Trends und Tendenzen

Der Referent:

Alexander Barth, Dipl.-Betriebswirt, Aus- und Weiterbildung für Kreditinstitute, Wiesbaden

Termin und Ort:

17.- 21. Juni 2002,
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 **020646**.

IBS *Prüfen mit Konzept* Jahresfachkonferenz „Prüfen von SAP R/3“

SAP R/3 - Risiken und Risikomanagement

Wie sicher ist Ihr SAP R/3™ wirklich?

Rund um diese Problematik werden wir uns mit der Sicherheitskonzeption beim Einsatz eines SAP R/3™ Systems aus Prüfersicht beschäftigen.

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

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 an einem SAP R/3™ System erläutert!

Diese Veranstaltung richtet sich an Mitarbeiter aus den Bereichen:

Interne Revision
Wirtschaftsprüfung
Systemadministration
Datenschutz
Finanz- und Rechnungswesen

18. November 2002

09:00 Uhr **Empfang**

09:30 Uhr **Begrüßung** durch den Veranstalter IBS

Dipl.-Ing. Ottokar Schreiber

Eröffnung der Fachkonferenz durch den Vorsitzenden

Dipl.-Betriebswirt Uwe Bernd Striebeck

09:45 - 11:00 Uhr

Aufbau einer SAP R/3 Sicherheitsarchitektur aus Sicht `Internal Controls´

Otto Arnold Schell

- Datenbank-, Betriebssystem und Netzwerksecurity einer SAP R/3-Systemlandschaft
- Risiken / Risikomanagement
  Exkurs: Datenmigration/Interfaces
- Einbindung von Intranet / Internet in die Sicherheitsarchitektur
  Übergang / Risikopotentiale
- Prüfansätze ex-post / ex-ante
- Ausblick

11:00 - 11:30 Uhr **Kaffeepause**

11:30 - 12:45 Uhr

Revision und Controlling im Rahmen von Supply Chain Management Projekten

Reiner Stein

- Erfolgskriterien
- Messbarkeit
- Prozessrisiken
- Probleme im Change Management

12:45 - 14:00 Uhr gemeinsames **Mittagessen**

14:00 - 15:30 Uhr

mySAP.com: E-Business Security

Stefanie Garcia Laule

- Benutzer- und Rollenverwaltung
- Sicheres Systemmanagement
- Abbildung von Vertrauensbeziehungen
- Sicherheit auf Anwendungsebene

15:30 - 16:00 Uhr **Kaffeepause**

16:00 - 17:30 Uhr

Berechtigungsadministration in mySAP HR

Dipl.-Kfm. Gerald Borchert

- Evaluierung von Rollen in mySAP HR: Standardrollen vs. Eigenerstellte Rollen
- Automatisierte Rollen-User Zuordnung mit Hilfe von PD-Objekten sowie Problematiken verteilter Systeme
- Zugriff via Internet: Chancen und Risiken von Employee Self Services
- Manager Desktops und strukturelle Berechtigungen in mySAP HR
- Pflege von Berechtigungen eines SAP HR Systems unter Revisionsaspekten

18:30 Uhr **„Hamburger Abend“**
(in Konferenzgebühren enthalten)

19. November 2002

ab 08:45 Uhr **Empfang**

09:00 - 10:30 Uhr

Modulare Prüfkonzeption in SAP R/3

Dipl.-Betriebswirt Christoph Wildensee

- SAP R/3 Modulkonzeption
- Grundsätzliche Problemstellungen im Rahmen von Modulprüfungen
- Risiken und Sicherheitsproblematiken
- Schnittstellenprüfungen
- Systematiken
- Sicherheitskonzepte zur Risikominimierung

10:30 - 11:00 Uhr **Kaffeepause**

11:00 - 12:30 Uhr

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

Thomas Tiede

- RFC-Destination - Gefahren durch hinterlegte Kennwörter und Vertrauensbeziehungen
- Die RFC-Destinationen des TMS (Transport Management System)
- Brute-Force-Attacks auf R/3 über einen RFC-Zugriff
- Zugriff auf R/3 von anderen Anwendungen, z.B. MS Excel
- Nutzung des Audit-Logs zur RFC-Absicherung (Alert-Monitor)
- Sicherung von RFC-Anmeldung durch SNC (Secure Network Communication)

12:30 - 14:00 Uhr gemeinsames **Mittagessen**

14:00 - 15:30 Uhr

Hacken mit SAP R/3

Stefan Hölzner

- Angriffe aus dem Internet
- Externe Betriebssystemkommandos aus SAP R/3
- Ausnutzung der Microsoft Windows Freigabedienste
- Erlangen von Systemadministrator-Rechten
- Ordnungsmäßigkeitsaspekte
- Gegenmaßnahmen: IT Security Policy und Berechtigungskonzepte

15:30 - 16:00 Uhr **Diskussion und Verabschiedung**

Strategieseminar 20. November 2002 (Kann gesondert gebucht werden)

Das Strategieseminar bietet Ihnen eine Einführung in die integrale Funktionalität und die prüfungsrelevanten Risikobereiche von SAP® R/3.

In Anlehnung an die gesetzlichen Bestimmungen erhalten Sie einen Einblick in die systemseitige Umsetzung und die daraus resultierenden Prüfungsansätze.

Im Focus der Betrachtungen stehen die Kriterien der Prüfbarkeit als Voraussetzung für die Prüfungsplanung und Prüfungshandlung.

Themenschwerpunkte sind:

- Systemarchitektur
- Organisationsstruktur
- Verarbeitungsabläufe und Verbuchungsprinzipien
- Tabellensteuerung
- Berechtigungskonzeption
- Ausgewählte Prüfansätze in FI

Alle Themen werden direkt am R/3 System bearbeitet.

Dieses Seminar ist getrennt von der Fachkonferenz buchbar.

Marie-Luise Wagener (vorm. Sander)

Anmeldung

Fachkonferenz 2002 **„Prüfen von SAP R/3“**
18.11.-19.11.2002 und 20.11.2002 in Hamburg

☐ **Ja, ich nehme an der Fachkonferenz „Prüfen von SAP R/3“ teil.**

Teilnahmegebühr/Person: € 1.200,- zzgl. MwSt.

☐ **Ja, ich nehme am Strategieseminar SAP R/3 im IBS-Schulungscenter teil**
(kostenloser Shuttle-Dienst)

Teilnahmegebühr/Person: € 490,- zzgl. MwSt.

Hotelreservierung von: _____ bis: _____

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

☐ Raucher ☐ Nichtraucher

☐ Einzelzimmer ohne Frühstück	€	129,-
☐ Doppelzimmer ohne Frühstück	€	149,-
☐ ELYSÉE-Frühstücksbuffet Pers./Tag	€	14,-
☐ Boulevard-Frühstück Pers./Tag	€	7,-

Name _____

Abteilung _____

Firma _____

Straße _____

PLZ/Ort _____

Telefon/Fax _____

Ort/Datum _____

Unterschrift _____

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

Anmeldung für den Hamburger Abend
(In den Teilnehmergebühren enthalten)

☐ Ja, ich nehme am Hamburger Abend teil
☐ Ja, ich nehme am Hamburger Abend teil und bringe meinen Partner / meine Partnerin mit
☐ Nein, ich nehme nicht am Hamburger Abend teil

Software-Test

CheckAud for Hard- and Software (ursprünglich WiSeHard)

Wie in der letzten ReVision angekündigt hat die ibs schreiber gmbh Hamburg eine neue Prüfsoftware entwickelt, die sich wieder einmal eines bisher noch nicht prüfbaren Bereiches angenommen hat. Das unter dem ursprünglichen Namen WiSeHard entwikkelte Prüftool wurde unter CheckAud for Hard- and Software in die CheckAud-Prüf-Familie integriert.

"Wir haben uns entschieden, alle Prüfprodukte unseres Hauses in einer Audit-Familie unter dem Namen CheckAud zu vereinen. So werden die Prüftools ab sofort z.B. als "CheckAud for Hard- and Software", "CheckAud for SAP R/3®", "CheckAud for Windows2000" etc geführt. Dies weist auch auf die Internationalität unserer Produkte hin. Außer dem Namen hat sich an der Prüfsoftware mit ihren revisionsspezifischen Funktionen jedoch nichts geändert." So Christoph Alt, Entwicklungsleiter der ibs schreiber gmbh.

Die Aufregung in der Redaktion war relativ groß, als das Paket mit der ersten ßeta-Demo-Version von CheckAud for HaS (Hardware and Software) auf dem Tisch lag. Denn die Problemstellung, mit der sich die Software beschäftigt, ist ein bisher durch die Revision gern übersehener Prüfbereich: Ausgelieferte bzw. verwendete Hardware und installierte Software. Zudem hatte die ibs schreiber gmbh angekündigt, dass dies das erste Produkt sei, welches auch ein zentrales Modul für die Administration enthält.

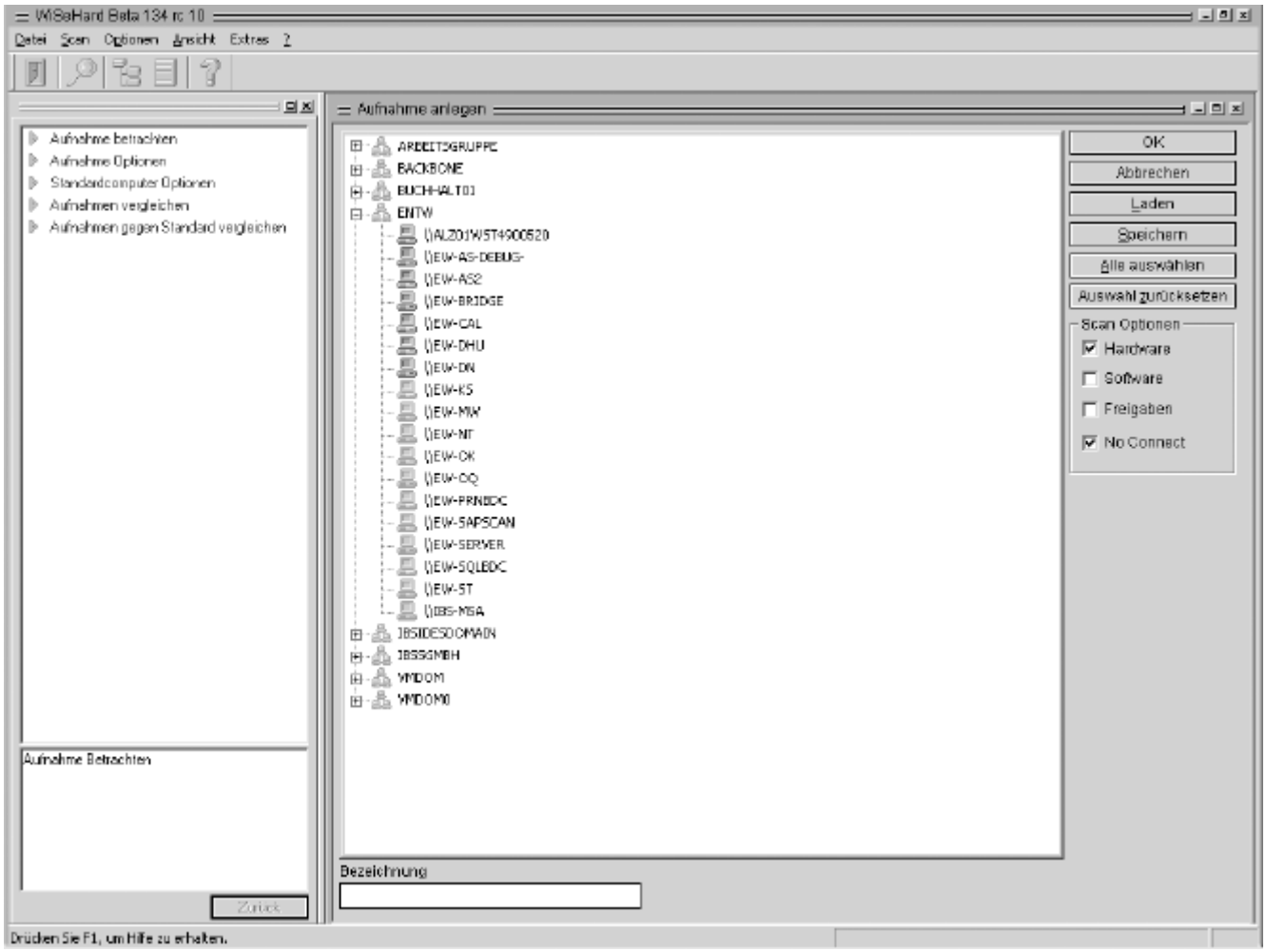


Abb 1: Das Scanmodul

Warum Hard- und Software prüfen?

Die Hardware einer modernen Arbeitsstation ist nicht nur teuer, sondern auch beim Anwender sehr begehrt. Diebstähle, vor allem in großen Unternehmungen, gehören - wenn auch selten offiziell zugegeben - zur Tagesordnung. Zudem kann es vorkommen, dass Lieferanten - nach Bestellung - andere Hardware ausliefern als gefordert bzw. gekauft.

Durch den heute immer wieder verbreiteten Internetzugang am Arbeitsplatz kommt der Benutzer sehr leicht an Fremdsoftware heran, die normalerweise nicht ohne ausdrückliche Zustimmung des Unternehmens installiert werden dürfte. In Verbindung mit einem falschen Berechtigungskonzept auf Betriebssystemebene führt dies schnell dazu, dass rechtlich geschützte Dateien über Freigaben im Intranet verteilt werden.

Zwar ist mit der Einführung des SMS-Servers von Microsoft die Möglichkeit gegeben, Hardware in weitesten Sinne zu erfassen, eine Aufbereitung katalogisierter Daten, ein Vergleich oder der Hinweis auf kritische Bereiche fehlen jedoch gänzlich.

CheckAud for Hard and Software - Der Test

Der Scan

Wie von ibs gewohnt, war das Softwarepaket in zwei Teilen zu installieren: Scanmodul und - für die Revision - das Auswertungsmodul. Einen Unterschied gibt es gegenüber der bisherigen Konzeption allerdings: Es wurde auch an die Administratoren gedacht. Das will heißen, dass in dem Scanmodul ein Auswertungsmodul voll implementiert ist. Die Administration kann also den Scan und die Auswertung über ein und dasselbe Modul durchführen. Da Prüfer nicht scannen können (dafür werden administrative Rechte benötigt), fehlen im Auswertungsmodul die Scanfunktionen.

Als Umgebung für unseren Test haben wir eine Domäne eingerichtet, die mit 5 Arbeitsstationen und 3 Servern ausgestattet war. Das Scanmodul ist weitestgehend selbsterklärend und übersichtlich aufgebaut. Vor dem Scan kann man den Umfang der zu erfassenden Daten einstellen. So kann man z.B. wählen, ob nur Freigaben, Hard- oder Software gescannt werden sollen. Der Scan selber war - auch bei vollem Scanumfang - nach wenigen Sekunden abgeschlossen. Eine messbare Netzwerkbelastung hat es nicht gegeben.

Damit eine Arbeitsstation erfasst werden kann, muss diese hochgefahren sein, ein Benutzer muss jedoch nicht angemeldet sein. Das Scanmodul bietet auch die Möglichkeit, Rechner zu erfassen, die beim Start des Scans "offline" sind. Ist diese Funktion aktiviert, wartet das Scanmodul solange mit dem Scan, bis die Maschine "online" geht und der Abschluss des Scans vollzogen werden kann. Im Test funktionierte dies einwandfrei.

Die Auswertung

Dass der optische Anspruch bei den Entwicklern der ibs hoch ist, wird beim Start des Auswertungsmoduls auf den ersten Blick sichtbar. Übersichtliche Menüs, die sich farblich dezent zurückhalten, prägen das Erscheinungsbild des jüngsten Pferdes im ibs-Rennstall. Wie schon aus den anderen Audit-Produkten bekannt wird Transparenz bei ibs groß

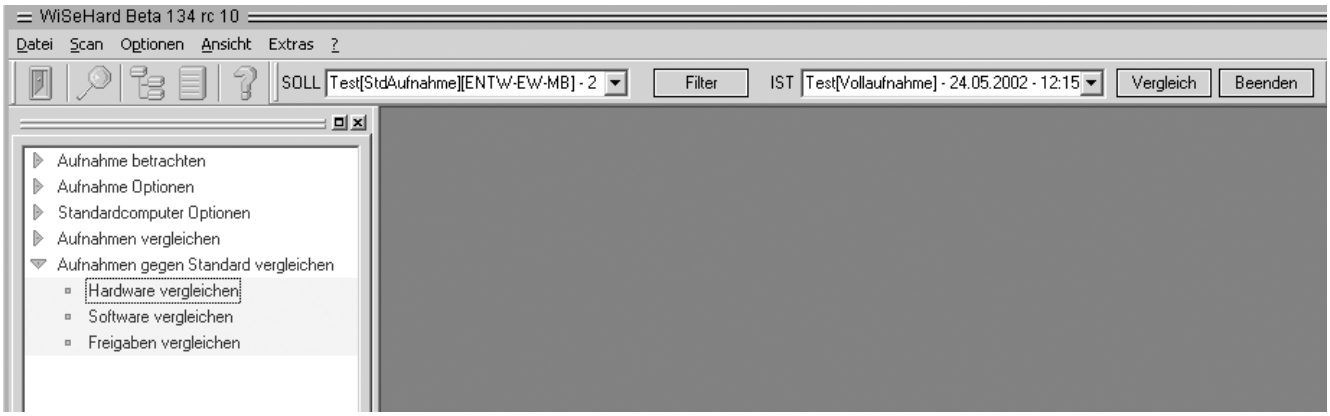


Abb 2: Vergleichsoptionen

geschrieben. Wie mächtig das Tool ist, wird spätestens dann klar, wenn man die einzelnen Auswertungs- und Vergleichsmöglichkeiten genauer unter die Lupe nimmt. So ist es möglich, einen Standardrechner innerhalb einer Aufnahme zu definieren, gegen den alle anderen Rechner geprüft werden sollen. Sieht man bei der Auswertung im linken Fenster den Standardrechner, so sind im rechten Fenster die zu prüfenden Rechner eines Scans zu sehen. Das Tool zeigt auf einen Blick, welche Rechner von dem vordefinierten Standard abweichen. Ein Ampelsystem stellt übersichtlich Übereinstimmungen (grün), Zusätzlichkeiten (gelb) oder Abweichungen bzw. fehlende Komponenten (rot) dar. Dargestellt werden alle Informationen, die der SMS-Dienst von Microsoft zur Verfügung stellt. Diese Form der Darstellung ist nicht nur neu, sondern, wie sich zeigt, auch sehr effizient. So sind in den von uns manipulierten Rechnern alle vorgenommenen Veränderungen auf den ersten Blick aufgedeckt worden, sowohl bei den veränderten Hardwarekomponenten als auch bei neu bzw. gelöschten Programmen.

Über die Filterfunktionen kann schnell und effektiv der Ein- bzw. Ausschluss von Komponenten selektiert werden. Dies hat im Test zu erstaunlich schnellen Ergebnissen geführt. Auch die Berichterstellung ist sehr komfortabel aufgebaut. Ein Klick auf die rechte Maustaste öffnet ein Kontextmenü, mit dem der Bericht und sein Umfang zu einem Objekt sehr genau skaliert werden kann.

Natürlich bietet die Software auch einen Komplettvergleich. D.h. es können zwei verschiedene Komplettaufnahmen gegeneinander abgeglichen werden. Mit dieser Funktion kann z.B. ein halbes Jahr nach einer Neubeschaffung festgestellt werden, an welchen Rechnern auf Hard- oder Softwarebene manipuliert wurde.

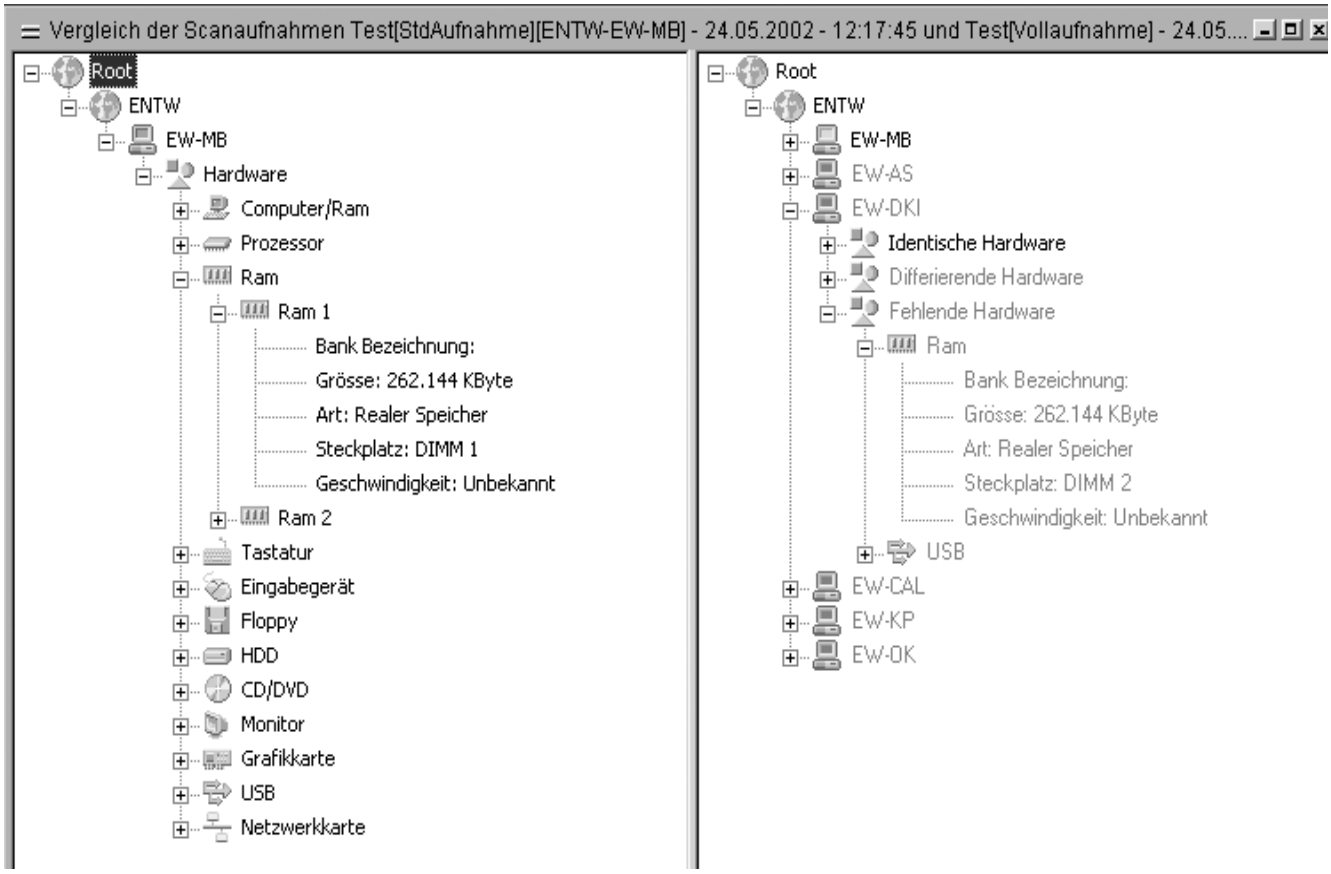


Abb 3: Vergleich gegen einen Standard

Sehr interessant aus Revisionssicht dürfte auch die Funktion "Freigabenvergleich" sein. Dieses Feature dürfte gerade bei den Benutzern mit krimineller Energie für schlaflose Nächte sorgen. Denn die Software ermittelt genau, welche Freigaben (und damit Downloadmöglichkeiten für andere Benutzer im Intranet) vorhanden sind.

Das bringt die Zukunft

Die ibs schreiber gmbh hat schon jetzt konkrete Vorstellungen über zukünftige Versionen. Alles wollte man uns zwar nicht verraten, aber es ist z.B. die Rede von einem Realtime-Monitor (Watchdog), der sofort nach Veränderung eines Hard- oder Softwarezustandes eine E-Mail an einen bestimmten Personenkreis schickt. Des weiteren ist angedacht, einen neuen Agenten zu implementieren, der in der Lage ist, nach bestimmten Dateitypen auf Arbeitsstationen zu suchen. (z.B. *.exe, *.mp3, *.jpg ...etc.).

Fazit

Schon die Betaversion von CheckAud for Hard and Software hat uns begeistert. Endlich ist es der Revision und auch der Administration möglich, ganzheitliche Prüfungen in einem bisher als rotes Tuch beschriebenen Bereich zu tätigen. Für Administratoren bedeutet das Tool endlich "leichte Dokumentation im Hard- und Softwarebereich" sowie "detaillierte Katalogisierung". Die Revision bekommt mit dem Tool erstmalig die Möglichkeit in die Hand, Hardwarediebstähle- und Unterschlagungen umfassend und zeitnah aufzudecken. Die Software bedeutet auch eine Präventivmaßname gegen die illegale Verbreitung von Software im Intranet. (mr)

In der nächsten ReVision:

Testbericht: USEIT

Tool zum Prüfen von UNIX

Herausgegeben von: Martin Richter

Theorie und Praxis der Wirtschaftsprüfung

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

Am 9. und 10. Oktober 1998 fand in Potsdam das zweite Symposium zur "Theorie und Praxis der Wirtschaftsprüfung" statt. Diese Veröffentlichung enthält die Langfassungen der gehaltenen Vorträge und ein Ko-Referat. Zusätzlich wurde ein wissenschaftsprogrammatischer Vortrag mit dem Titel "Konzeptioneller Bezugsrahmen für eine realwissenschaftliche Theorie betriebswirtschaftlicher Prüfungen" aufgenommen.

Das erste Symposium im Jahre 1996 gab Anstöße, um die Stagnation der Forschung zur Betriebswirtschaflichen Prüfungslehre im deutschen Sprachraum zu überwinden. Primäres Ziel des zweiten Symposiums war es, den State-of-the-Art der Prüfungsforschung aufzuzeigen. Die Autoren unterzogen sich dazu der sehr arbeitsintensiven Aufgabe, die reichhaltige und im wesentlichen angloamerikanische Literatur auf den Gebieten Wirtschaftsprüfung und ökonomische Theorie, Prüfungsmarkt, Prüfungsmethoden sowie Urteilsbildung auszuwerten und kritisch zu würdigen.

In einem Beitrag über die Weiterentwicklung des risikoorientierten Prüfungsansatzes wird gezeigt, wie wissenschaftliche Erkenntnisse für die Prüfungspraxis nutzbar gemacht werden können

---

Herausgegeben von:
Prof. Dr. Dr. h.c. Wolfgang Ballwieser
Prof. Dr. Dr. h.c. Adolf G. Coenenberg
Prof. Dr. Dr. h.c. Klaus v. Wysocki

Handwörterbuch der Rechnungslegung und Prüfung (HWRP)

Schäffer Poeschel Verlag
1430 Seiten
ISBN: 3-7910-8046-6
€ 199,90

Vor dem Hintergrund der nationalen und internationalen Entwicklung im Bereich der Rechnungslegung und Prüfung erscheint die 3. Auflage des „Handwörter der Revision (HWRev)“ unter dem Titel „Handwörterbuch der Rechnungslegung und Prüfung (HWRP)“. Die tiefgreifenden Änderungen der letzten Jahre, deren Ursache insbesondere in der fortschreitenden Globalisierung der Unternehmen sowie der Kapitalmärkte liegt, haben eine völlige Neukonzeption des Werkes erforderlich gemacht. Sämtliche Beitragsstichworte wurden unter dem Blickwinkel nationaler und internationaler Rechnungslegungs- und Prüfungsnormen (IAS, US-GAAP bzw. ISA) werden nicht nur isoliert und themenbezogen in einzelnen Beitragsstichworten behandelt, sie ziehen sich vielmehr in Form von Gegenüberstellungen durch alle einschlägigen Themenbereiche. Die bedeutenden internationalen und nationalen Standardsetter und deren System von Verlautbarungen werden charakterisiert und wichtige Fachausdrücke aus den unterschiedlichen Regelungskreisen seperat auf der Grundlage des deutschen Verständnisses behandelt.

In insgesamt nahezu 260 alphabetisch angeordneten Beiträgen setzen sich Experten aus Bilanzierungs- und Prüfungspraxis sowie der Wissenschaft mit dem Themenbereich Rechnungslegung und Prüfung auseinander. Die Systematische Zuordnung, die Lösung von Teilproblemen und vertiefende Antworten auf Einzelfragen werden durch Querverweise und Literaturhinweise in jedem Beitrag sowie durch umfangreiche Register ermöglicht.

Hrsg.: Institut der Wirtschaftsprüfer

Abschlussprüfung nach International Standards on Auditing (ISA)

Vergleichende Darstellung deutscher und internationaler Prüfungsgrundsätze

IDW Verlag
1392 Seiten, gebunden
ISBN: 3-8021-0771-3
€ 110,00

Die ISA werden in zunehmendem Maße als Konsens über die internationalen Anforderungen an eine Abschlußprüfung im Rahmen weltweiter Verhandlungen anerkannt. Derzeit strebt die IFAC die Anerkennung der Prüfungsstandards durch die IOSCO, die internationale Organisation der Börsenaufsichtsbehörden, an. Im Zuge der zunehmenden Globalisierung der Wirtschaft ist ein gestiegenes Interesse deutscher Un-

ternehmen zu verzeichnen, zur internationalen Präsentation ihrer Konzernabschlüsse einen Bestätigungsbericht zu erhalten, der ausdrücklich darauf hinweist, daß die Prüfung in Einklang mit den ISA erfolgte.

„Derzeit strebt die IFAC die Anerkennung der Prüfungsstandards durch die IOSCO an.“

In diesem Zusammenhang ist die Zielsetzung der vorliegenden Studie zu sehen, die ISA ausführlich darzustellen und deren Anforderungen mit den deutschen Regelungen zu vergleichen.

Die Untersuchung umfaßt sämtliche 28 für die Abschlußprüfung relevanten ISA. Sie baut auf dem im IFAC-Handbook 1997 "Technical Pronouncements" dokumentierten Stand auf. Darüber hinaus werden im Sinne der Aktualität der Untersuchung und angesichts der Tragweite der (vorgesehenen) Änderungen die von IAPC im November 1997 verabschiedete Überarbeitung von ISA 530 "Audit Sampling and Other Selective Testing Procedures" und der im September 1997 veröffentlichte Entwurf für eine Überarbeitung von ISA 570 "Going Concern" berücksichtigt.

Der Vergleich der ISA mit den deutschen Regelungen erfolgt in der Reihenfolge der von der IFAC entwikkelten Systematik und umfaßt je ISA ein dreistufiges Vorgehen:

- Abschnitt "I. ISA" gibt den englischen Originalwortlaut des jeweils behandelten ISA wieder. Die Zwischenüberschriften folgen in der Regel den Vorgaben aus dem ISA. In manchen Fällen wurden zur besseren Übersichtlichkeit und Verständlichkeit der Darstellung deutsche Zwischenüberschriften ergänzt.
- Abschnitt "II. Referenzstellen für den Vergleich" enthält als Ausgangspunkt für den Vergleich Auszüge aus den einschlägigen gesetzlichen Vorschriften (z. B. HGB, AktG, GmbHG, WPO, Berufssatzung der WPK) und den Fachgutachten und Stellungnahmen des IDW einschließlich der mit der WPK gemeinsam herausgegebenen Vorstandsverlautbarung zur Qualitätssicherung in der Wirtschaftsprüferpraxis (VO 1/1995).
- Abschnitt "III. Darstellung des ISA und Vergleich" stellt zunächst den Inhalt des jeweiligen ISA dar. Die Angabe der jeweiligen Textziffern aus dem ISA soll helfen, den Bezug zum englischen Originaltext herzustellen. Für die Darstellung werden - soweit wie möglich - bestimmte Fachausdrücke der ISA vor dem Hintergrund der deutschen Gegebenheiten nach einer in der gesamten Studie grundsätzlich einheitlich verwendeten Begriffsbildung in die deutsche Sprache übertragen. Die Begriffsbildung ist in einem der Untersuchung vorangestellten Glossar festgehalten. Soweit Begriffe nur schwer oder gar nicht zu übertragen sind, werden die englischen Originalausdrücke entweder unmittelbar im Text verwendet oder als Klammerzusatz der deutschen Darstellung hinzugefügt. Die deutschen Regelungen werden im Rahmen des Vergleichs nur kurz beschrieben, da sich die Studie vorwiegend an den sachkundigen deutschen Leser richtet.

Die Grundlage des sich anschließenden Vergleichs des ISA mit den deutschen Regelungen bildet das im Preface to International Standards on Auditing and Related Parties (vgl. Anhang) festgehaltene Verständnis der IFAC zur Anwendung der ISA: Danach enthalten die ISA wesentliche Grundsätze und Prüfungshandlungen (basic principles and essential procedures), die im Originaltext durch Fettdruck hervorgehoben sind sowie erläuternde Ausführungen hierzu (related guidance). Die wesentlichen Grundsätze und Prüfungshandlungen sind im Kontext der erläuternden Ausführungen zu verstehen. Nach dem Preface ist es erforderlich, zum Verständnis und zur Anwendung der wesentlichen Grundsätze und Prüfungshandlungen den gesamten Text des jeweiligen ISA einschließlich der erläuternden Ausführungen zu würdigen.

In den Anhängen werden sowohl die englischen Orginaltexte der IFAC als auch die wesentlichen deutschen Referenzstellen geschlossen wiedergegeben. Dabei werden auch der Text von ISA 530 "Audit Sampling and Other Selective Testing Procedures" in seiner überarbeiteten Form und der Entwurf für eine Überarbeitung des ISA "Going Concern" berücksichtigt. Die geschlossene Wiedergabe der deutschen Referenzstellen soll es ermöglichen, die in "II. Referenzstellen für den Vergleich" auszugsweise angeführten Stellen vollständig und in ihrem jeweiligen Kontext zu würdigen.

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: € 47,- (incl. 7% MwSt).

Abo-Bestellschein für die ReVision

Tel: +49 40 - 69 69 85 - 14 / 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 € 47,- incl. 7% MwSt. Die Abo-Gebühren zahle ich

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

meine Konto-Nr.: _____ Bankleitzahl: _____

Bank: _____ Kontoinhaber: _____

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

Name: _____ Vorname: _____

Abteilung: _____ Telefon/Fax: _____

Firma: _____ eMail: _____

Straße: _____ PLZ/Ort: _____

Ort/Datum: _____ Unterschrift: _____