Artikel_KonTraG

KonTraG

und (EDV)-Verfahrensprüfung

Roger Odenthal

Inhaltsverzeichnis

Seite

1 Einführung

Das im Jahre 1998 verabschiedete Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) sowie die hiermit verbundene Novellierung von Aktienrecht und Handelsgesetzbuch *verschärfen die Überwachungs- und Berichtspflichten der Unternehmensleitung*. Weiterhin werden die *Anforderungen an die Abschlussprüfung* und die hieran gebundene Berichterstattung *erweitert*. Beides unterstützt die Kontrollfunktion der prüfenden Stellen und hat weitreichende Wirkung auf die Gestaltung und Ausichtung der Abschlussprüfung.

2 Anwendungsbereich des Gesetzes

In der Öffentlichkeit wird vielfach die – unzutreffende – Auffassung vertreten, dass das KonTraG ausschliesslich Angelegenheiten im Zusammenhang mit der Führung und Prüfung börsennotierter Aktiengesellschaften regele. Tatsächlich betreffen eine Reihe von Vorschriften andere prüfungs- und publizitätspflichtige Gesellschaftsformen.[1]

Gesetzliche Anforderung	Betroffene Gesellschaftsformen	Adressat	Bewertung/Stichworte
Treffen geeigneter Maßnahmen und Einrichtung eines Überwachungssystems zur frühzeitigen Erkennung bestandsgefährdender Risiken § 91 Abs. 2 AktG	Aktiengesellschaften	Vorstand	Grundlage für zukünftige Anforderungen an andere Gesellschaftsformen - Interne Revision? - Dokumentation der Geschäftsabläufe? - Controlling? - Regelungen von Vollmachten?
Berichtspflicht unter Einbeziehung von Risiken für die künftige Unternehmensentwicklung. • im Lagebericht § 289 Abs. 1 HGB • im Konzernlagebericht § 315 Abs. 1 HGB	prüfungs- und publizitäts-pflichtige Gesellschaften	Vorstand oder Geschäftsführung	- Interne und externe Risikofaktoren - System zur Erfassung von Risikofaktoren und zukünftigen Risiken
Ausrichtung der Abschlußprüfung auf das „zuverlässige" Erkennen wesentlicher Verstöße gegen Rechnungslegungsvorschriften § 317 Abs. 1 u. 3 HGB	prüfungs- und publizitäts-pflichtige Gesellschaften	Abschlußprüfer	Vertiefte Prüfung und zusätzliche berufsmäßige Skepsis versus Kooperation mit dem Vorstand
Prüfung des Lageberichtes unter Einbeziehung möglicher Risiken für zukünftige Unternehmensentwicklungen. § 317 Abs. 2 HGB	prüfungs- und publizitäts-pflichtige Gesellschaften	Abschlußprüfer	- Kenntnis interner und externer Risikofaktoren - System zur Erfassung und Bewertung zukünftiger Risiken
Prüfung der Maßnahmen des Vorstandes zur Einrichtung und Funktionsfähigkeit des Überwachungssystem § 317 Abs. 4 HGB	börsennotierte (amtlicher Handel) Aktiengesellschaften	Abschlußprüfer	
Umfassend erweiterte risikoorientierte Berichtspflicht im Prüfungsbericht § 321 Abs. 1 bis 3 HGB	prüfungs- und publizitäts-pflichtige Gesellschaften	Abschlußprüfer	Detaillierte Darstellung der durchgeführten Prüfungshandlungen und -tiefe mit Rückwirkung auf die Ausrichtung der Prüfung
Gesonderte Berichtserstellung zur Einrichtung sowie zur Funktionsfähigkeit des Überwachungssystems einschließlich der Darstellung von Maßnahmen zu dessen Verbesserung § 321 Abs. 4 HGB Bestätigungsvermerk	börsennotierte (amtlicher Handel) Aktiengesellschaften	Abschlußprüfer	Übernahme von Beratungsfunktionen durch den Abschlußprüfer
Differenzierter Bestätigungsvermerk mit Darstellung wesentlicher „bestandsgefährdender" Risiken § 322 HGB	prüfungs- und publizitäts-pflichtige Gesellschaften	Abschlußprüfer	Rückwirkung auf die Ausrichtung der Prüfung

Abbildung 1 Darstellung ausgewählter Regelungen des KonTraG

Aus der vorstehenden Übersicht wird ersichtlich, dass sich lediglich die Vorschriften zur Einrichtung, zum Betrieb sowie zur Prüfung und Beurteilung eines *funktionierenden internen Überwachungssystems* ausschliesslich auf (teilweise) börsennotierte und für den amtlichen Handel zugelassene Aktiengesellschaften beziehen.

[1] Zur Darstellung der Anforderungen sowie zu den Adressaten vergl. Dörner, WPG 7/1998, S. 302 ff.

Hierbei sollte allerdings nicht übersehen werden, dass die im Aktienrecht formulierte Pflicht und Verantwortung des Vorstandes einer Aktiengesellsellschaft für ein funktionierendes Überwachungssystem sicherlich zukünftig z.B. in der Rechtssprechung eine Grundlage für die *Beurteilung ordnungsgemäßen Handelns geschäftsführender Personen anderer Gesellschaftsformen* darstellen wird.[2]

Die der *Unternehmensleitung* auferlegte *weitergehende Auskunftspflicht* im Lagebericht sowie die *grundlegende Neuausrichtung der Abschlussprüfung* auf das zuverlässige Erkennen wesentlicher Verstösse gegen Rechnungslegungsvorschriften bzw. die Beurteilung des Lageberichts im Hinblick auf die zutreffende Darstellung bestandsgefährdender Risiken betreffen hingegen *alle prüfungs- und publizitätspflichtigen Gesellschaften*. Sie machen es für beide Stellen gleichermaßen notwendig, sich mit in- sowie externen Risikofaktoren auseinanderzusetzen und ein System zur Erfassung, Beurteilung und Beherrschung solcher Risikofaktoren zu entwickeln.

Die für den *Bericht des Abschlußprüfers* geforderten *detaillierten Angaben* zu möglichen Risiken sowie der *differenziert zu gestaltende Bestätigungsvermerk* haben weiterhin *generelle Rückwirkungen* auf Ausrichtung und Inhalt von Abschlussprüfungen.

Es bleibt daher festzuhalten, dass im Hinblick auf die Beschäftigung mit risikobehafteten Geschäftsfaktoren, Geschäftsprozesse und deren Überwachung sowohl für die Unternehmensleitung als auch für den Abschlussprüfer eine *Differenzierung nach Gesellschaftsformen wenig sinnvoll erscheint.*

Bei der Bewertung von Risiken sich u.a. ergebende Fragen nach:

- der Transparenz und Dokumentation kritischer Geschäftsprozesse sowie
- nach einem wirksamen Überwachungssystem, bestehend aus einem funktionierenden IKS und Interner Revision,

haben dabei einen *direkten Beziehungszusammenhang zur EDV-Verfahrensprüfung*.

Dem Begriff der EDV-Verfahrensprüfung liegt dabei ein tradiertes, *funktionsorientiertes Verständnis des „Prüfungsobjektes EDV“* zugrunde. Hiernach wird das jeweilige fachliche Verfahren, wie z.B. die Personalabrechnung, Materialverwaltung oder Finanzbuchhaltung durch mehr oder weniger komplexe EDV-Module unterstützt. Diese „Hilfsfunktion“ hat einen primär technischen Charakter, spielt sich in Rechenzentren oder *in den Händen von Computerspezialisten* ab. Dieses rechtfertigt es demzufolge, ein eigenständiges, von der fachlichen bzw. kaufmännischen Prüfung weitgehend losgelöstes „Prüffeld“ zu entwickeln und es in die Hände von Spezialisten (EDV-Revisoren) zu legen.

Das beschriebene Verständnis führte in der Vergangenheit häufig dazu, die EDV als Randthema eines (budgetarmen) Prüfungsauftrages zu betrachten. Die sich aus *den Merkmalen und der Wirkungsweise moderner EDV-Systeme ergebenden Risiken blieben dabei weitgehend unberücksichtigt*. Zukünftig zwingen nun die Bestimmungen des KonTraG, sich hiermit verstärkt auseinanderzusetzen.

[2] vgl. Pollanz, Der Betrieb, 1999, S. 1277 ff.

3 Merkmale und Risiken moderner EDV-Verfahren

3.1 Entwicklungstendenzen

Die EDV-Landschaften vieler Unternehmen wandeln sich derzeit in rasantem Tempo. Neue technologische Optionen der computerverarbeitenden Industrie sowie ein Management, welches der Informationsverarbeitung zunehmend strategische Bedeutung zumisst, befruchten sich gegenseitig und erschliessen der EDV in immer kürzeren Zyklen neue und komplexere Aufgabenfelder.

Stichwörter der aufgezeigten Entwicklung sind: Client-/Server-Umgebung, Workflow und Workgroup, Internet sowie E-Commerce und E-Business, skalierbare Geschäftsprozesse mit verteilter Datenhaltung, Verarbeitung und Austausch digitaler Dokumente (DMS), offene und komplex integrierte, geschäftsbasierte Anwendungen.

Die aufgezeigten Techniken gelten als Sinnbild moderner Informationsverarbeitung und damit als Schlüsselfaktor zum Überleben im globalen Wettbewerb. Dementsprechend werden sie bedenkenlos umfassend oder zumindest in organisatorischen Teilbereichen der Betriebe umgesetzt. Nicht selten fügen sich so – ohne begleitende Strategie und Abstimmung – alle denkbaren Spielarten der Datenverarbeitung, von der terminalgesteuerten Grossrechnerapplikation bis zum modernen NetComputing in einem Unternehmen zusammen.

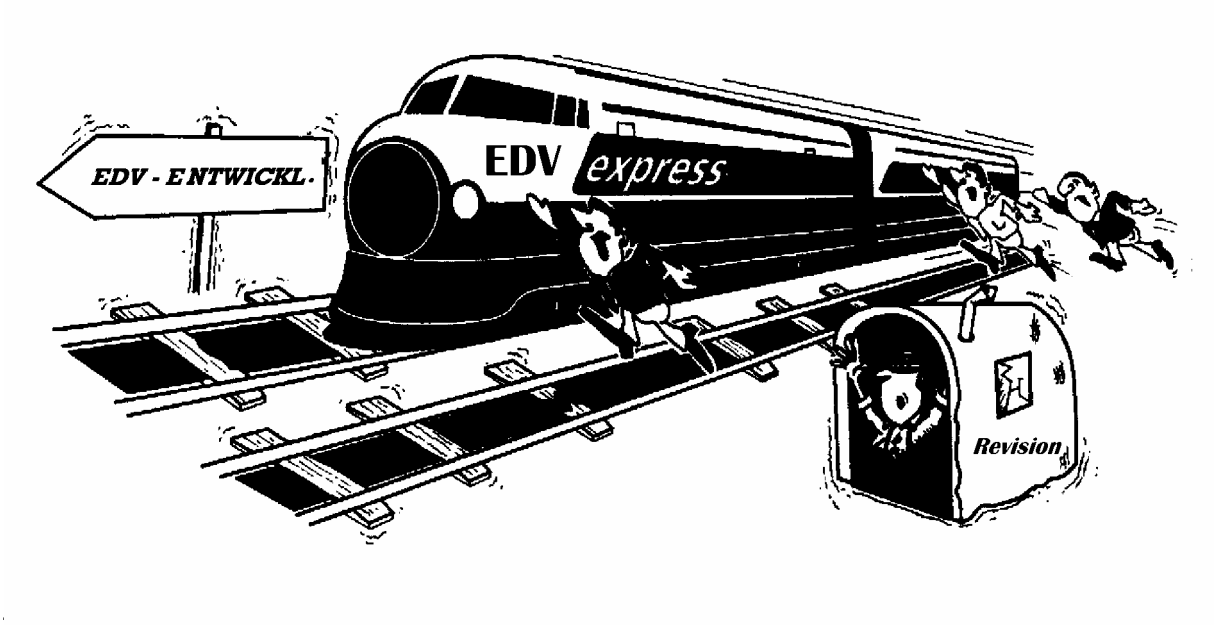

Abbildung 2 Prüfung vor dem Hintergrund aktueller EDV-Entwicklungen

Seitens der Abschlussprüfer und Interner Revision ist es notwendig, diese Entwicklung kritisch zu begleiten. Vielfach wird – wie der Prüfungsalltag zeigt – der *Einführung neuer Technologien*, wie z.B. das DownSizing in eine Client-/Serverumgebung und die Installation umfassender sogenannter ERP-Software von *nicht unerheblichen Risiken für den Fortbestand des Unternehmens*, seine Beziehungen zum Markt, zu den Kunden, die abzuwickelnden Geschäftsprozesse sowie die hieraus resultierenden Informationen für die Unternehmenssteuerung und die Sekundärdaten des Rechnungswesens begleitet.

3.2 Eigenschaften aktueller EDV-Technik

Risiken für die Unternehmen, die dort ablaufenden Geschäftsprozesse sowie die aufbereiteten und verwalteten Daten ergeben sich durch die nachfolgenden Eigenschaften moderner EDV-Technik:

❏ Offenheit der Anwendungen

Im Gegensatz zu priorietären, aus einer Hand erstellten EDV-Lösungen ermöglichen heutige Anwendungen eine *schrankenlose, plattformübergreifende Verarbeitung von Daten*. Der wechselseitige Austausch von Informationen zwischen einer auf dem Grossrechner geführten Produktionssteuerung, der netzwerkbasierten Lagerwirtschaft sowie der Finanzbuchhaltung und der Tabellenkalkulation auf dem Anwender-Personalcomputer wird als selbstverständlich angesehen.

Offenheit entwickelt sich auch nach aussen, im Rahmen eines weitgehend papierlosen Datenaustausches mit entfernt liegenden Betriebsteilen, mit Kunden oder Lieferanten oder bzw. mit Zugang zum weltumspannenden Internet und E-Commerce-Aktivitäten.

❏ Modularität der Systeme

Hinter dem Modularisierungskonzept steht der Wunsch nach *Flexibilität und Skalierbarkeit* sowohl der EDV-Prozesse als auch der zugehörigen Hardware. Ist eine Client-/Server-basierte Unternehmenssoftware angesichts neu hinzugekommener Nutzer bzw. eines ansteigenden Datenvolumens ihrer Aufgabe nicht mehr gewachsen, so werden z.B. für eine EDV- Finanzbuchhaltung *zusätzliche Serverlaufwerke an frei wählbarer Stelle* in das Netzwerk integriert und Datenverarbeitungsprozesse oder Datenbanken auf die hinzugenommenen Rechner *standortübergreifend* verteilt.

❏ Systemunabhängigkeit der Anwendungen

Moderner EDV-Systeme verdanken ihren Erfolg u.a. der *Unabhängigkeit* von einer bestimmten *herstellereigenen Hard- oder Softwareplattform*. Gleiche Applikationen laufen auf allen gängigen Rechnern mit verschiedenen Betriebssystemen und die Datenverwaltung erfolgt mit Hilfe standardisierter Schnittstellen in verschiedensten relationalen Datenbanken.

❏ Daten- und Prozessintegration

Die *Umsetzung des Integrationsgedankens* spielt sich innerhalb moderner *Anwendungssoftware an zwei Stellen* wieder. Formal ist diese funktional im Hinblick auf bestimmte betriebliche Anwendungsgebiete (Finanzbuchhaltung, Materialwirtschaft, etc.) aufgebaut, interne *Schnittstellen werden* bei der Bewegung und Aufbereitung von Daten jedoch *weitgehend vermieden*. So löst die Erfassung von Geschäftsvorfällen Buchungsvorgänge in einer Nebenbuchhaltung und begleitend, durch sogenanntes Mitbuchen, im Hauptbuch aus, führt gleichzeitig zur Aktualisierung der Kostenrechnung sowie zusätzlich zur Fortschreibung der für die Vertriebssteuerung notwendigen statistischen Informationen und sonstiger betrieblicher Auswertungen für die Führungsebene.

Neben dieser dialogorientierten, integrativen Fortschreibung von Zahlen rücken *komplexe Betriebspozesse* in den Blickpunkt solcher Systeme. Mittels Workflow-Management werden *strukturierte Arbeitsvorgänge durch ein System hindurch gereicht* und sorgen – je nach Ausgestaltung – weitgehend automatisch für die Abfrage oder Einspielung der hiermit verbundenen Informationen, Dialoge, Kontrollen, Buchungsvorgänge und die Ablage. Anstoss für einen derart automatisierten Betriebsprozess können alternativ die Handlungen eines Mitarbeiters oder eines automatisch von aussen in das System eingespieltes Dokument (Lieferschein, Rechnung, etc.) sein. *Der in der EDV abgebildete Geschäftsvorgang determiniert in diesen Fällen den realen Material- und Wertefluss.*

3.3 Risiken moderner EDV-Verfahren

Durch die dargestellten Merkmale sind die Gefahren für die *Entwicklung bestandsgefährdender Risiken bei der Abwicklung geschäftlicher Transaktionen* sowie für den Schutz, die Sicherheit, Integrität und Ordnungsmässigkeit der verwalteten Datenbestände extrem gewachsen. Konnte ein Prüfer vor einigen Jahren in einer zentral geführten, örtlich gesicherten und mit RACF abgeschotteten Grossrechnerumgebung *innerhalb eines vertretbaren Zeitrahmens eine kompetente Aussage über den Sicherheitsstandard eines EDV-Systems* und die Zuverlässigkeit der Verarbeitung treffen, so *ist dies heute nicht mehr möglich*, da sich die Gefahrenquellen potenziert haben.

Der *EDV-Betrieb*, ehedem einem elitären Kreis von RZ-Mitarbeitern vorbehalten, hat sich mit der Verbreitung des Personalcomputers und standardisierter Software *demokratisiert. Die Anwender sehen sich als ausreichend sachverständig*, um individuelle Datenverarbeitung auf dem Personalcomputer durchzuführen. Sowohl die Rechnereinheiten, als auch Betriebssysteme und Datenbanken, mit deren Hilfe geschäftskritische Anwendungen abgewickelt werden, sind ihnen vertraut. In Verbindung mit der bereits beschriebenen Offenheit der Systeme und dem einfachen Datenaustausch wird *jede in ein Netzwerk eingebundene Server- und Arbeitsplatzstation zum Gefahrenpotential*. Diese reicht weit über die allseits diskutierte Virenproblematik hinaus und geht von fehlerhaften eigenentwickelten „Makro"-Programmen über die Einspielung unautorisierter Programmstände, die Manipulation kritischer Systemparameter bis zur möglichen Ausspähung und Ausschleusung vertraulicher Informationen über Disketten oder Telefonleitungen.

Die *Modularität* verleiht der EDV-Umgebung eine ungeheure Dynamik. Eine kompetente Aussage darüber, *welche Rechner ein komplettes EDV-System abbilden ist nur für den Augenblick und nur unter Vorbehalten möglich*. Eine Applikation kann nicht mehr eindeutig ohne weiteres einem oder mehreren Serverlaufwerken zugeordnet werden. Das Netz als Ganzes, einschliesslich der darin eingebundenen Rechner, UNIX-, Windows- und sonstiger Server sowie der zugehörigen Arbeitsplatzstationen, Fernverbindungen und Verknüpfungen mit Fremdsystemen bilden ein sich tagtäglich änderndes Geschäfts- und Prüfungsumfeld.

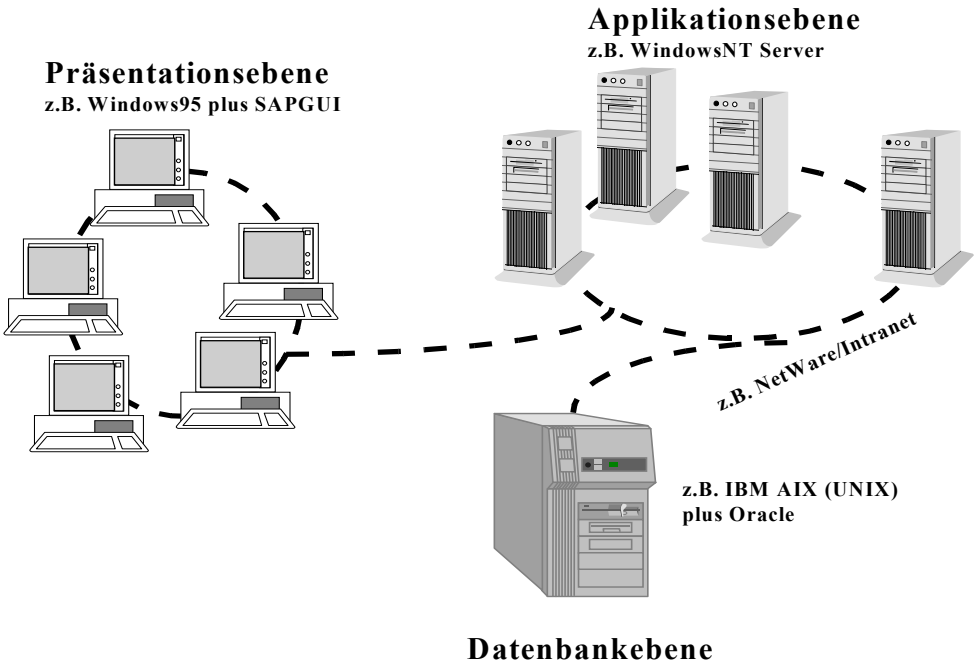

Abbildung 3 Modularer Aufbau einer modernen EDV-Umgebung

Der betriebswirtschaftlich nachvollziehbare Wunsch nach *Systemunabhängigkeit* der Anwendungen *birgt ebenfalls nicht unerhebliche Risiken*. Schutz und Sicherheit der EDV-Daten werden von jedem Hersteller naturgemäss nur für die von ihm zu verantwortenden Komponenten optimiert, d.h., vom Hersteller der geschäftsabwickelnden Software nur für sein Programm, vom Hersteller des hierzu notwendigen (fremden) Datenbanksystems nur für seine Datenbank, von den Lieferanten der Hardware sowie des jeweiligen Betriebssystems nur für diese Komponenten. Da *für alle aufgeführten Schichten differente, jedoch gleichermassen komplexe, häufig objektorientierte Berechtigungskonzepte* zur Verfügung gestellt werden, ist eine Beurteilung der Gesamtsicherheit unter Berücksichtigung der Interdependenzen zwischen diesen verschiedenen EDV-Komponenten, für den EDV-Revisor ausserordentlich zeitaufwändig und schwierig.

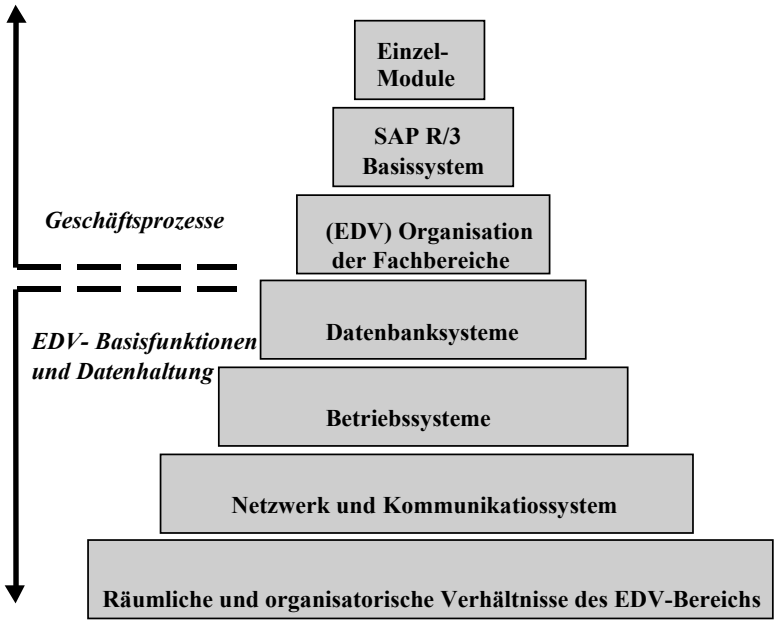

Abbildung 4 Schichten einer komplexen EDV-Applikation am Beispiel von SAP R/3

Die bereits beschriebene *Daten- und insbesondere Prozessintegration* kann sich, je nach Gestaltung, zum *Fluch oder Segen für das betreibende Unternehmen und den Abschlussprüfer entwickeln*. Sie verlangt, dass ein im Standard ausgeliefertes EDV-System richtig an die Gegebenheiten eines spezifischen Unternehmens eingestellt und angepasst wird. Jede Inkonsistenz zwischen den innerhalb der Programme abgebildeten Betriebsprozessen und der realen Abwicklung hat – wie nachfolgend an einigen Beispielen dargestellt wird – schwerwiegende Konsequenzen sowohl für die geschäftliche Entwicklung als auch für die sich hieraus ergebenden und zu prüfenden Zahlen. Die dazu notwendigen Parameter müssen überschaubar und in ihrer gegenseitigen Abhängigkeit transparent sein, mit angemessenen und wirksamen Kontrollen. Nur dann tragen sie zu einem funktionierenden internen Kontrollsystem bei. Allerdings – wer könnte z.B. in einem sich fortentwickelnden SAP R/3-System mit seiner Vielzahl von Tabellen und Programmen dafür einstehen?

Zuletzt sei an dieser Stelle auf die mit der *Miniaturisierung der Hardware verbundenen Risiken* hingewiesen. Der Kostenanteil für die aus Prüfersicht angemessene Absicherung der Systemumgebung und nachfolgender Kontrollen steigt – gemessen an den originären Ausgaben für das EDV-System – überproportional. *Das hierfür notwendige Bewusstsein und die Akzeptanz der Kostenverantwortlichen entwickelt sich leider nicht in gleichem Umfang.*

Man muss kein Pessimist sein, um zu erkennen, dass der *Sicherheitsstandard der EDV-Verarbeitung sowie die Zuverlässigkeit der hiermit abgewickelten Geschäftsvorgänge mit der fortschreitenden Technik nicht Schritt hält*. In einer wirtschaftlichen Situation, in der die Existenz eines Unternehmens von einem funktionsfähigen und sicheren EDV-Umfeld abhängt, sieht sich der erfahrene Prüfer *sicherheitstechnisch einem Rückschritt von 10 – 15 Jahren* gegenüber.

Häufig befinden sich Datenserver in frei zugänglichen Räumen ohne Sicherheitsschleuse und nur selten ist eine mit RACF vergleichbare Abschottung der Anwender von den Netz-Betriebssystemen und den einzelnen Applikationen feststellbar. Vertrauliche Daten, bis hin zu Kontenständen werden unverschlüsselt über lokale Modemstationen und ungesicherte Netze ausgetauscht. *Vorschnell und mit unzureichender Beratung eingeführte, komplexe Programmsysteme behindern nachhaltig wesentliche Unternehmensfunktionen*, wie z.B. die Auslieferung von Produkten bzw. die Erstellung von Rechnungen oder legen diese für Wochen völlig lahm. Fehlerhaft eingestellte Software und Anwender mit unzureichenden Kenntnissen der ineinander greifenden (EDV-)Geschäftsprozesse führen zu einem vollkommen falschen, kaum mehr abstimmbaren Zahlenwerk.

Die in gemeinsamer Arbeit von Abschlussprüfern und Interner Revision entwickelten *Grundsätze für eine funktionssichere und ordnungsgemässe Datenverarbeitung werden zunehmend nicht berücksichtigt*. Für den *Abschlussprüfer* haben diese Umstände *nachteilige Konsequenzen*. Er sieht sich – wenn er nicht von Anfang an in die Gestaltung und den Betrieb neuer Informationstechniken einbezogen wurde bzw. sich nicht selbst einbringt – mit der Situation konfrontiert, dass Schutz, Sicherheit und Ordnungsmässigkeit der einzelnen, auch buchungsrelevanten EDV-Prozesse, einschliesslich der daraus resultierenden Zahlen, für ihn nicht mehr oder nur mit erheblichem Aufwand prüfbar sind.

Es sei an dieser Stelle noch einmal darauf hingewiesen, dass es sich keinesfalls um eine Problematik handelt, mit der sich ausschliesslich der „EDV-Revisor“ auseinandersetzen muss. *Ohne enge Zusammenarbeit zwischen fachlichem- und technisch ausgerichtetem Prüfer ist es unmöglich, die inhärenten Risiken der Geschäftsvorgänge festzustellen und zu beurteilen.* Die Richtigkeit und Zuverlässigkeit, z.B. in einer Bilanz eingestellter, halbfertiger Produkte, kann nur beurteilt werden, wenn das Verständnis der Bewertungsvorschriften sowie der hierzu notwendigen Arbeitsgänge mit den in der EDV abgebildeten, automatisierten Prozessen zusammengeführt wird.

3.4 Beispiele für bestandsgefährdende Risiken im EDV-Umfeld

Es gibt unzählige Beispiele für wesentliche Risiken, die sich aus der Einführung neuer Programme und deren Betrieb ergeben. So musste sich die Firma Whirlpool zwei Monate nach der Inbetriebnahme einer R/3-Installation mit dem *Verlust einer Reihe von Kundenaufträgen* und einem *Umsatzrückgang von bis zu 15%* auseinandersetzen, da den Kunden keine oder falsche Ware geliefert wurde.[3]

Nach Ausführungen eines Sachverständigen sind diese Schwierigkeiten kein Einzelfall. Mehr als 30% aller R/3-Projekte erfüllten die Erwartungen der Anwender nicht. Schuld daran sei u.a. die starke Integration der Software. Sie erfordere eine sehr aufwändige Abstimmung zwischen allen Beteiligten innerhalb und ausserhalb der Unternehmen, die nicht immer gelinge.

[3] Beispiele aus Computerwoche 49 bis 52, Dezember 1999

Gleichfalls von Lieferschwierigkeiten betroffen war ein grosser US-Süsswarenhersteller. So waren gerade *in der umsatzstärksten Weihnachtszeit keine Auslieferungen möglich, ohne dass klar zu sein schien, welcher Teil des EDV-Gesamtsystems nicht funktionierte*.

„Hat Andersen Consulting die SAP-Einführung vermasselt?“ – Modifiziertes R/3 legt VW-Ersatzteillager lahm“ lautete eine Schlagzeile, unter der nachfolgend ausgeführt wurde, dass Kunden und Händler, die bisher ein bis zwei Tage auf ein benötigtes *Ersatzteil* warten mussten, sich nach einer Softwareumstellung *wochenlang zu gedulden* hatten.

Gerade in der Einführungsphase komplexer Softwareprogramme sind die Risiken evident. So hat die Lego-Group sich vor kurzem entschlossen, ihre bereits in Produktion befindliche R/3-Applikationen durch neue Software auszutauschen, obwohl erst kürzlich eine grössere Summe in die Finanz- und Vertriebsmodule investiert wurde. Nach Auskunft des EDV-Verantwortlichen *war man ausserstande, die realen Geschäftsprozesse soweit zu standardisieren, dass eine spiegelbildliche Abbildung innerhalb der SAP R/3-Software möglich gewesen wäre*. Weitere Anstrengungen und Frustrationserlebnisse seien den Mitarbeitern nicht zuzumuten. Der Wechsel auf eine neue Lösung stehe deshalb in enger Verbindung mit der Motivation der Lego-Mitarbeiter.

Diesen veröffentlichten Beispielen können zahlreiche Erfahrungen aus eigener Prüfungspraxis beigesteuert werden:

- gravierende *Rechenfehler bei der Verbrauchsabrechnung* eines Energieversorgungsunternehmens für Anwender mit mehr als einem Verbrauchsobjekt,

- hunderte *„verschwundener“ Buchungen* in der Finanzbuchhaltung eines grossen Handelsunternehmens in Folge eines technischen Reparaturmechanismus der Datenbank,

- *zwei Monate Geschäftsstillstand* eines Textilhandelsunternehmens nach Einführung einer kleinen Auftragsabwicklung mit falscher Tabelleneinstellung,

- *drei Monate ohne Rechnungsstellung* bei einem Produktionsunternehmen nach fehlerhafter Einführung und Anpassung einer Vertriebssoftware,

- Beeinträchtigung wesentlicher Betriebsprozesse mit
  - fehlender Abstimmungsmöglichkeiten von Haupt- und Nebenbuchhaltung
  - fehlenden Mahnverfahren,
  - fehlender ordnungsgemässer Patientenabrechnung,
  - gravierenden Unrichtigkeiten in der Materialbuchhaltung

  Monate nach der Softwareumstellung in einem Krankenhaus,

- wochenlange erheblich *verzögerte (manuelle) Schadensbearbeitung* in einem Versicherungsunternehmen, nach dem das DMS-System mit den digitalisierten Schadensakten ausgefallen und nicht hinreichend schnell wiederhergestellt werden konnte.

Die Aufzählung ließe sich endlos fortführen. Unternehmen, deren *Geschäftsergebnis im Zwanzig-Minuten-Rhythmus* in Folge von Softwarefehlern um *mehrere Millionen-DM variiert* wären ebenso zu nennen, wie solche, für die *keine Umsatzsteuerverprobung* möglich ist oder *wöchentliche körperliche Bestandsaufnahmen notwendig* sind, um einen Überblick über die EDV-geführten Bestände zu erhalten.

Auf die nahezu „normale“ Situation, dass in einer Vielzahl von Systemen *unkomplizierte Eindringversuche* mit Zugriff auf sensible Daten erfolgreich sind, dass vorgefundene Berechtigungsverfahren den Anwendern beliebige Möglichkeiten eröffnet kritischste Funktionen zu bedienen oder spurlos rechnungsrelevante Informationen zu verändern, soll an dieser Stelle nicht weiter eingegangen werden.

3.5 Kennzeichen einer revisionsfreundlichen EDV-Umgebung

3.5.1 Mindestanforderungen der Abschlussprüfer

Interne Revision und Abschlußprüfer dürfen angesichts der aufgezeigten Situation nicht resignieren. Sie können einen wesentlichen Beitrag dazu leisten, die jeweiligen EDV-Verfahren „revisionsfähig“ zu gestalten. Hierzu genügt es, dass sie – ohne tiefgreifendes technisches Verständnis – ihre berechtigten Forderungen an Dokumentation und Prüfbarkeit sowohl der EDV-Einführung, als auch des Systembetriebs anmelden. Hierbei gibt kein anerkanntes Gütesiegel für eine revisionsfreundliche Informationsverarbeitung. Da jedoch nahezu alle mit EDV-Hilfe abgewickelten Betriebsprozesse zu Sekundärdaten eines EDV-geführten Rechnungswesens führen, muss der EDV-Betrieb ganz allgemein die Erfüllung der aus Gesetz und Rechtsprechung abgeleiteten *GoBS* oder - spezieller - der *GoDV* sicherstellen (vgl. IDW, FAMA-Richtlinie; IIR, DV-Revision Leitfaden; Schuppenhauer, GoDV[4]). Hinzu kommen die *Bestimmungen des Datenschutzes* und aus unternehmerischem Eigeninteresse formulierte *Sicherheits- und Schutzanforderungen* an die EDV.

Im Rahmen dieser Vorgaben muss die EDV für den (Abschluss-) Prüfer nachvollziehbar, sicher und kontrollierbar sein. Dazu zählen u.a. die:

- Dokumentation und Prüfbarkeit der in einer EDV-Umgebung vorhandenen *Hardware*,
- Dokumentation und Prüfbarkeit der verwendeten *Software*,
- Dokumentation und Prüfbarkeit des *Systembetriebes*,
- Dokumentation und Prüfbarkeit der mit der EDV-Anwendung verbundenen *organisatorischen und technischen Gegebenheiten*,
- Dokumentation und Prüfbarkeit eines *Softwareeinführungsprojektes*.

Auf diese Punkte wird im folgenden näher eingegangen.

3.5.2 Dokumentation und Prüfbarkeit der in einer EDV-Umgebung vorhandenen Hard- und Software

3.5.2.1 Übersicht über die Hardware

Kennzeichen für eine moderne EDV-Umgebung sind die für verschiedene Aufgaben in ein *Netzwerk integrierten Serverlaufwerke* sowie die dezentral angebundenen *PC-Arbeitsstationen* der einzelnen Anwender.

Ausstattung und Konfiguration dieser Rechner können sowohl die *Arbeit auf den Arbeitsplatzstationen selbst*, als auch den *sicheren Zugang und die Arbeit auf die Netzwerkserver beeinflussen*. Sehr schnell sind beispielsweise Speicherbausteine entfernt, ist die teure Bildschirmkarte gegen ein billiges Produkt aus dem privaten Computer ausgewechselt oder eine ISDN-Karte für den Internet-Zugang installiert, ohne dass man es dem jeweiligen Rechner ansieht. Darüber hinaus *gehen unberechtigte Zugriffsversuche* auf EDV-Anwendungen oft von schlecht abgesicherten Arbeitsplatzstationen aus. Dieses macht laufende Prüfungen in diesem Bereich notwendig.

[4] Vgl. Schuppenhauer, WpG 3/2000, S. 128 ff.

Revisionsfreundlich ist eine EDV-Umgebung, deren einzelne Rechner und Netzwerk-Komponenten sowohl in Papier- als auch in Dateiform dokumentiert sind. Diese, als *Hardwareinventarisierung* bezeichnete Zusammenstellung erleichtert dem Systemverantwortlichen zudem die Unterstützung der Anwender, die Fehlerdiagnose und ist für den Prüfer eine wichtige Grundlage für die Beurteilung der mit der EDV verbundenen Risiken.

3.5.2.2 Übersicht über die Software

Neben der Hardware sind die in einer EDV-Umgebung eingesetzten Programme Prüfobjekte für den Revisor. Dies gilt besonders in einer Netzwerkumgebung. Die grundsätzlich bestehende Gefahr, dass einzelne Anwender und Abteilungen *unautorisierte Programme* auf ihren PC-Arbeitsstationen verwenden ist durch regelmässige Kontrollen zu verringern. Hierdurch mögliche Schäden sind für die betroffenen Unternehmen nicht unerheblich und gehen weit über das im Vordergrund stehende Virenproblem hinaus. Unsauber programmierte Software führt u.U. zu Systemabstürzen im Netz. Nicht definierte Schnittstellen und fehlerhafte Software kann zu Datenverlusten und falschen Ergebnissen führen. Die Anwendung nicht lizensierter Programme schadet dem Ruf eines Unternehmens und zieht ggf. Schadensersatzansprüche nach sich.

Revisionsfreundlich ist eine EDV-Umgebung, welche mit einer *aktuellen und detaillierten Aufzeichnung* der für den Betrieb autorisierten und *lizensierten Programme* in Schrift- und Dateiform betrieben wird.

3.5.3 Dokumentation und Prüfbarkeit des Systembetriebes

Die Sicherheit und Integrität der Datenbestände in einer heterogenen EDV-Umgebung können durch vielfältige Einflüsse, wie bspw.:

- Stromausfall,
- fehlerhafte Installation,
- fehlerhafte programmierte Software,
- schadhafte Leitungen,
- Hardwarefehler
- oder Programmanipulationen,

beeinträchtigt werden. Die Revision muss sich deshalb davon überzeugen können, ob die einzelnen *Schichten einer EDV-Umgebung mit Hardware, Betriebs- und Kommunikationssystem sowie Datenbank und die hierauf aufbauenden Programme stabil ablaufen*, auftretende Fehler umgehend beseitigt werden und - nach einem Systemausfall - eine schnelle, unkomplizierte Wiederinbetriebnahme einschliesslich einer Rekonstruktion beschädigter Datenbestände möglich ist.

Dieses bedingt zum einen, das *schriftlich fixierte Datensicherungs- und Notfallkonzepte* vorliegen. Darüber hinaus bieten alle Betriebssysteme spezielle Funktionen, die den laufenden Systembetrieb, einschliesslich dabei auftretender Fehler, automatisch in *Logdateien* erfassen, vorausgesetzt, diese Funktionen wurden aktiviert. *Eine revisionsfreundliche Gestaltung des EDV-Betriebes schreibt diese Aktivierung zwingend* vor und stellt dem EDV-Revisor neben den hieraus resultierenden *Protokollen* eine Übersicht zur Verfügung, in der die Bedeutung und Auswirkung der einzelnen, häufig vorkommenden Fehlermeldungen hinsichtlich Datenschutz und -sicherheit detailliert erläutert werden.

Die laufende Kontrolle und Interpretation der Fehlermeldungen sowie die Analyse des Sicherheitsstatus von Betriebs- und Datenbanksystemen wird durch Zusatzprogramme, wie sie speziell für die Revision angeboten werden (z.B. das SAP AIS-System), wesentlich vereinfacht. Sie müssen jedoch ebenfalls installiert und aktiviert werden.

Eng verbunden mit der Dokumentation und Prüfbarkeit des Systembetriebs sowie der daraus resultierenden Risiken ist das *Vorliegen eines* auf die jeweilige Software zugeschnittenen *Berechtigungskonzeptes*. Dieses muss ein klares, verständliches Bild von der Aufbauorganisation, den Aufgaben der einzelnen Mitarbeiter und der Systematik der hierzu zugeordneten Berechtigungen vermitteln. Dieses schriftlich formulierte Konzept und dessen entsprechende Umsetzung innerhalb des EDV-Systems ist eines der *wesentlichen Grundlagen für die Beurteilung eines funktionierenden internen Kontrollsystems*.

3.5.4 Dokumentation und Prüfbarkeit der organisatorischen und baulichen Gegebenheiten

Modernen EDV-Verfahren ist zu eigen, dass EDV-administrative Tätigkeiten, die vormals der Arbeitsvorbereitung oder dem Operating vorbehalten waren, in die Fachabteilungen verlagert werden. Umgekehrt übernimmt der EDV-Bereich fachliche Aufgaben, wie z.B. die Einsteuerung von Abstimmprozessen, oder die Reorganisation von Buchhaltungsdaten, die grundsätzlich von betroffenen Fachabteilungen verantwortet werden müssen. Hinzu kommt, dass den zunehmenden kleiner werdenden Stäben der EDV-Basis-Betreuung vielfältige Arbeiten zugeordnet werden, die zwangsläufig zu Funktionshäufungen führen.

Revisionsfreundlich ist eine EDV-Umgebung, in der die *mit der EDV verbunden Abläufe und Zuständigkeiten* eindeutig geregelt sind. Dieses gilt ebenfalls für eine Aufzeichnung der mit dem EDV-Systembetrieb verbundenen *technischen und baulichen Gegebenheiten* einschliesslich einer *Darstellung der Netz-Infrastruktur*.

3.5.5 Dokumentation und Prüfbarkeit des Softwareeinführungsprojektes

Vielfach scheitern Softwareprojekte bereits bei ihrer Einführung mit kritischen Folgen für die betroffenen Unternehmen. Unzureichende gedankliche Vorüberlegungen und mangelhafte Übersichten über den jeweiligen Projektstand sind hierfür verantwortlich. Die Faustregel, dass *komplexe Softwareprojekte mindestens doppelt so teuer sind wie kalkuliert und bei Einhaltung des als notwendig erachteten Projektplans genau so viel länger* dauern ist erfahrungsgemäss zutreffend.

In einer solchen Situation werden mit Sicherheit die für die Qualität der Zahlen wichtigen Projektphasen, wie z.B. Testvorgänge, die Gestaltung eines funktionierenden Berechtigungswesens sowie die ausreichende Schulung der Anwender reduziert. Gleiches gilt für die zuverlässige Migration (einschliesslich deren Dokumentation) von Altdaten auf das neue System.

Ein Abschlußprüfer sollte sich – soweit er dieses beeinflussen kann – bereits in *einer sehr frühen Projektphase* mit seinen Anforderungen an eine *ordnungsgemässe, klare und ausreichende Projektdokumentation* äussern. Diese führt erfahrungsgemäß zwangsläufig zu einer besseren Projektqualität, nutzt damit dem Mandanten und erleichtert nachfolgende Prüfungen.

4 Zusammenfassung

Die EDV-Abwicklung stellt einen wesentlichen und wachsenden Risikofaktor innerhalb der Unternehmen dar. Sie ist nicht mehr lediglich unterstützender Teilbereich neben anderen Unternehmensfunktionen sondern deren zentrales Element und häufig sogar bestimmend für die Aufbau- und Ablauforganisation eines Unternehmens. Es ist deshalb unabdingbar notwendig, sich im Rahmen der Abschlussprüfung mit den EDV-Prozessen auseinanderzusetzen. Diese Aufgabe kann nicht ausschließlich der EDV-Revision übertragen werden. Hier muss sich der *fachlich bzw. kaufmännisch orientierte Prüfer ebenso einbringen, um mit seinen Anforderungen nach einem Mindestmaß an Transparenz und Prüfbarkeit das Risikopotential der EDV einschätzen zu können und so den erweiterten Anforderungen des KonTraG gerecht zu werden*. Für darüber hinausgehende detaillierte technische Untersuchungen können Spezialisten herangezogen werden, die jedoch in enger Kooperation mit dem jeweiligen fachlichen Kollegen agieren müssen.

Literaturverzeichnis

IDW Institut der Wirtschaftsprüfer,
Fachausschuß für moderne Abrechnungssysteme (FAMA);
Grundsätze ordnungsmäßiger Buchführung bei computergestützten Verfahren und deren Prüfung

IIR Deutsches Institut für interne Revision e.V.,
Arbeitskreis "Revision der Datenverarbeitung": DV REVISION,
Ergänzbarer Leitfaden zur Durchführung von Prüfungen der Informationsverarbeitung

Odenthal, Roger Die Prüfung von Netzwerken mit Hilfe einer Revisionssoftware, in ECU-Management, Ausgabe 1, Januar 1994

EDV-Revision in einer PC-Netzwerkumgebung, in Zeitschrift "Datensicherheits-Report", Ausgabe 7/1996

Schuppenhauer, Rainer Grundsätze für eine ordnungsmäßige Datenverarbeitung (GoDV), IDW-Verlag GmbH, Düsseldorf, 1992

Verschiedene Autoren LAN, Praxis, WEKA Fachverlag für EDV, Augsburg, 1994

Wißner, Bernd (Hrsg.) Sichere EDV, Loseblatt-Sammlung, Interest-Verlag, Augsburg, 1994