JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN
PROFESSUR BWL – WIRTSCHAFTSINFORMATIK
UNIV.-PROF. DR. AXEL C. SCHWICKERT

Keller, Tobias; Schwickert, Axel C.

Branchenübergreifende Rechtsnormen zur IT-Sicherheit in Deutschland

ARBEITSPAPIERE WIRTSCHAFTSINFORMATIK

Nr. 1 / 2008
ISSN 1613-6667

Arbeitspapiere WI Nr. 1 / 2008

Autoren: Keller, Tobias; Schwickert, Axel C.

Titel: Branchenübergreifende Rechtsnormen zur IT-Sicherheit in Deutschland

Zitation: Keller, Tobias; Schwickert; Axel C.: Branchenübergreifende Rechtsnormen zur IT-Sicherheit in Deutschland, in: Arbeitspapiere WI, Nr. 1/2008, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2008, 33 Seiten, ISSN 1613-6667.

Kurzfassung: Unternehmen sind heute in höchstem Maße von Informationstechnologie (IT) abhängig. Die meisten Geschäftsprozesse werden durch IT unterstützt und ganze Branchen wären ohne Informationstechnologie nicht handlungsfähig. Der potentielle Schaden durch IT-Fehlfunktionen kann selbst für etablierte Unternehmen den Ruin bedeuten. Somit ist die Gewährleistung der IT-Sicherheit (ITS) zwingende Voraussetzung für das Erreichen der Unternehmensziele. Aber nicht nur für das Unternehmen selbst ist die ITS wichtig. Insbesondere externe Anspruchsgruppen fordern die Sicherstellung des Betriebs und den Schutz der verarbeiteten Informationen. Um diesem Schutzinteresse Dritter gerecht zu werden, wird der Gesetzgeber aktiv und schreibt ein Mindestmaß an Sicherheitsvorkehrungen vor. Ziel der vorliegenden Arbeit ist es, einen systematischen Überblick über die wichtigsten, branchenübergreifenden Rechtsnormen zur IT-Sicherheit in Deutschland zu geben.

Schlüsselwörter: Informationstechnologie, IT, IT-Sicherheit, Sicherheit, ITS, Rechtsnormen, branchenübergreifende Rechtsnormen, Deutschland, Haftungsrisiken, Sorgfaltspflicht, Risikomanagement, Buchführung, Datenschutz, Fernmeldegeheimnis

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

AktG ..... Aktiengesetz
AO ..... Abgabenordnung
BaFin ..... Bundesanstalt für Finanzdienstleitungsaufsicht
BFS ..... Buchführungssystem
BilReG ..... Bilanzrechtsreformgesetz
BITKOM ..... Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BSI ..... Bundesamt für Sicherheit in der Informationstechnik
CEO ..... Chief Executive Officer
CFO ..... Chief Financial Officer
DV ..... Datenverarbeitung
ERP ..... Enterprise Resource Planning
GDPdU ..... Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GG ..... Grundgesetz
GmbHG ..... Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GoB ..... Grundsätze ordnungsmäßiger Buchführung
GoBS ..... Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
HGB ..... Handelsgesetzbuch
IDW ..... Institut der Wirtschaftsprüfer
IKS ..... Internes Kontrollsystem
ISO ..... International Organization for Standardization
IT ..... Informationstechnologie
ITS ..... IT-Sicherheit
KontraG ..... Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KWG ..... Kreditwesengesetz
MaRisk ..... Mindestanforderungen an das Risikomanagement
PS ..... Prüfungsstandard
SigG ..... Signaturgesetz
SolvV ..... Solvabilitätsverordnung
SOX ..... Sarbanes-Oxley-Act
TDDSG ..... Teledienstedatenschutzgesetz

TDG ..... Teledienstegesetz
TKG ..... Telekommunikationsgesetz
UMAG ..... Gesetz zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts
UStG ..... Umsatzsteuergesetz
WORM ..... write once read multiple

1 Problem, Ziel und Aufbau

Unternehmen sind heute in höchstem Maße von Informationstechnologie (IT) abhängig.[1] Die meisten Geschäftsprozesse werden durch IT unterstützt und ganze Branchen wären ohne Informationstechnologie nicht handlungsfähig.[2] Der potentielle Schaden durch IT-Fehlfunktionen kann selbst für etablierte Unternehmen den Ruin bedeuten.[3] Somit ist die Gewährleistung der IT-Sicherheit (ITS) zwingende Voraussetzung für das Erreichen der Unternehmensziele. Die IT-Abhängigkeit und die Relevanz der ITS werden sich in Zukunft noch weiter steigern, getrieben durch die zunehmende Vernetzung und die offeneren Unternehmensnetzwerke, die zunehmende Verbreitung der IT sowie die immer häufigeren Angriffe auf IT-Systeme.[4]

Aber nicht nur für das Unternehmen selbst ist die ITS wichtig. Insbesondere externe Anspruchsgruppen fordern die Sicherstellung des Betriebs und den Schutz der verarbeiteten Informationen. Um diesem Schutzinteresse Dritter gerecht zu werden, wird der Gesetzgeber aktiv und schreibt ein Mindestmaß an Sicherheitsvorkehrungen vor.[5]

Für die Unternehmen gilt es folglich, effektiv und effizient mit einer doppelt komplexen Situation umzugehen: Erstens mit der zunehmenden Komplexität der IT-Systeme und dem damit verbundenen hohen Gefährdungspotential und zweitens mit dem komplexen Geflecht externer Anforderungen an die ITS.

Ziel der vorliegenden Arbeit ist es, diese Komplexität zu reduzieren, indem ein systematischer Überblick über die wichtigsten, branchenübergreifenden Rechtsnormen zur IT-Sicherheit in Deutschland gegeben wird. Zu diesem Zweck soll in Abschnitt 2 zunächst ein gemeinsames Verständnis für zentrale Begriffe geschaffen werden. Anschließend wird für die Abgrenzung des Untersuchungsgegenstandes eine Systematisierung der externen Anforderungen an die IT-Sicherheit vorgenommen und die branchenübergreifenden Rechtsnormen entsprechend eingeordnet. In Abschnitt 3 werden die Anforderungen der untersuchten Rechtsnormen herausgearbeitet. Der zusammenfassende Abschnitt 4 wird Überschneidungen aufzeigen und auf die Konsequenzen eingehen, welche die Rechtsnormen in der Summe für die Unternehmen haben.

1 Vgl. Falk, Michael; Hofmann, Marc: Integration des IT-Sicherheitsmanagements in das Risikomanagement im Kontext bankaufsichtsrechtlicher Vorgaben, in: Arbeitspapiere WI, Nr. 6/2006, Hrsg: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2006, S. 6.

2 Vgl. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Grundschutz – Basis für IT-Sicherheit, Online im Internet: http://www.bsi.de/gshb/deutsch/baust/01001.htm, 26.4.2006.

3 Vgl. o. V.: Barings Debacle, Online im Internet: http://www.riskglossary.com/link/barings_debacle .htm, 01.05.2006.

4 Vgl. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Grundschutz – Basis für IT-Sicherheit, a. a. O.

5 Vgl. Schmidt, Klaus: Der IT Security Manager, München: Hanser Verlag 2006, S. 265.

2 Einordnung des Untersuchungsgegenstandes

2.1 Der Begriff IT-Sicherheit

Mit der Abkürzung IT ist in dieser Arbeit der Begriff *Informationstechnologie* gemeint. Im Gegensatz zur *Informationstechnik*, ist hier nicht etwa nur die technische Informationsinfrastruktur alleine, sondern darüber hinaus auch die Informationsverarbeitung miteinbezogen, welche die Systemumwelt und die Nutzer umfasst.[6] Als Konsequenz beinhaltet der Begriff *IT-Sicherheit* nicht nur eine infrastrukturell-technische Perspektive sondern auch bzw. insbesondere eine organisatorisch-personelle Komponente.

Da in komplexen Situationen das Risiko nicht gänzlich eliminiert werden kann, ist unter Sicherheit ein situationsabhängiger relativer Zustand der Gefahren- bzw. Risikofreiheit zu verstehen.[7] Entsprechend fordert das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine IT-Risikoreduktion auf ein tragbares Maß durch angemessene Maßnahmen. Dabei werden drei *Schutzziele* als „Grundwerte der IT-Sicherheit“ formuliert:

1) *Verfügbarkeit*: Dienste, Funktionen und Informationen eines IT-Systems stehen dem Nutzer stets wie gewünscht zur Verfügung.
2) *Integrität*: Die Korrektheit der Daten und der Funktionsweise ist gesichert.
3) *Vertraulichkeit*: Nur autorisierte Nutzer haben Zugang zu vertraulichen Informationen.

Zusätzlich können zwei weitere Schutzziele berücksichtigt werden:

4) *Authentizität*: Die Identität von Personen, IT-Komponenten oder Anwendungen ist sichergestellt.
5) *Nichtabstreitbarkeit*: Versand und Empfang von Daten und Informationen können nicht in Abrede gestellt werden.

Beide o. g. zusätzlichen Schutzziele können unter dem Ziel der *Verbindlichkeit* zusammengefasst werden. Diese fordert, dass ein Kommunikationspartner seine Identität bewiesen hat und der Empfang einer Nachricht nicht abgestritten werden kann.[8] Abb. 1 fasst die genannten Schutzziele noch einmal zusammen.

6 Vgl. Falk, Michael; Hofmann, Marc: Integration des IT-Sicherheitsmanagements in das Risikomanagement im Kontext bankaufsichtsrechtlicher Vorgaben, a. a. O., S. 10 bis 13.

7 Vgl. Falk, Michael; Hofmann, Marc: Integration des IT-Sicherheitsmanagements in das Risikomanagement im Kontext bankaufsichtsrechtlicher Vorgaben, a. a. O., S. 11.

8 Vgl. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Grundschutz-Kataloge - Glossar: Stand 2006, Online im Internet: http://www.bsi.de/gshb/deutsch/baust/04.htm, 21.04.2007.

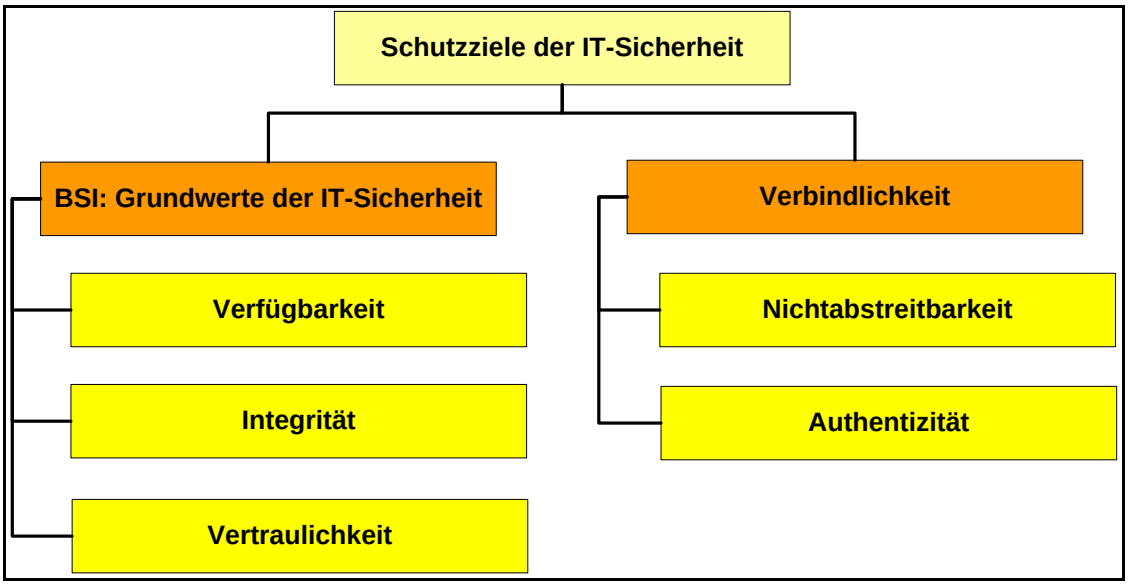

Abb. 1: Schutzziele der IT-Sicherheit

Die Risiken einer Beeinträchtigung dieser Schutzziele können durch technische, bauliche, organisatorische und personelle Maßnahmen gesenkt werden.[9]

2.2 Systematisierung der externen Anforderungen

Unternehmen sehen sich einer Vielzahl von Anspruchsgruppen gegenüber, die bzgl. der ITS Anforderungen stellen. Zu diesen *Stakeholdern* werden im Allgemeinen Eigen- und Fremdkapitalgeber, Management, Arbeitnehmer, Kunden, Lieferanten und die allgemeine Öffentlichkeit gezählt[10] Bspw. fordern Arbeitnehmer, Kunden sowie Lieferanten einen vertraulichen Umgang mit ihren Daten. Die Öffentlichkeit hat u. a. bei wichtigen technischen Infrastrukturen ein Interesse an ITS (z. B. Stromversorger).

Heute sind die Unternehmen durch die Wettbewerbssituation meist gezwungen, ein ausreichendes IT-Sicherheitsniveau zu signalisieren. Dazu wurden von der Industrie verschiedene Standards und Normen entwickelt. Eine unabhängige Prüfstelle zertifiziert jeweils deren Einhaltung. International etabliert ist die Zertifizierung nach ISO 27001. In Deutschland bietet das BSI eine IT-Grundschutz-Zertifizierung an, die für kleine und mittelständische Unternehmen wegen ihres geringeren Aufwands interessanter sein kann.

9 Vgl. Schaumüller-Bichl, Ingrid: Sicherheitsmanagement: Risikobewältigung in informationstechnologischen Systemen, Mannheim; Leipzig; Wien; Zürich: BI-Wissenschaftsverlag 1992, S. 17.

10 Vgl. Wöhe, Günther: Einführung in die Allgemeine Betriebswirtschaftslehre, München: Verlag Vahlen 2002, S. 77.

Auch der Gesetzgeber hat die Relevanz der ITS erkannt. Die erlassenen Rechtsnormen greifen schutzwürdige Belange der oben genannten Interessengruppen auf und formulieren entsprechende Mindestanforderungen, die in erster Linie durch das Management zu erfüllen sind. Obwohl bisher nur relativ wenige Gesetze mit explizitem IT-Bezug existieren,[11] gibt es mittlerweile eine unüberschaubare Vielzahl von Gesetzen, Verordnungen und Verwaltungsvorschriften, die Anforderungen an die ITS zumindest implizieren.

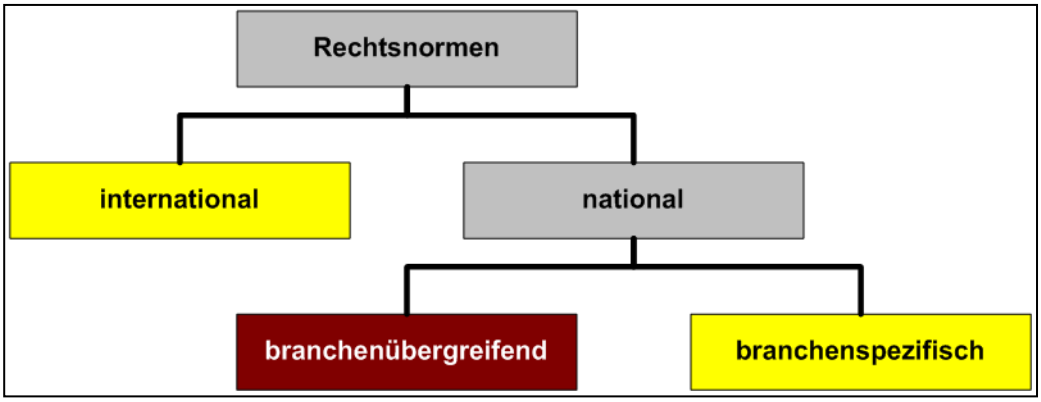

Abb. 2: Systematisierung der Rechtsnormen

Die Systematisierung dieser Rechtsnormen soll anhand von Abb. 2 erläutert werden. Zum einen kann man *internationale* und *nationale Rechtsnormen* unterscheiden. Internationale Rechtsnormen betreffen teilweise auch deutsche Unternehmen, die im Ausland aktiv sind. Relevant ist hier v. a. der Sarbanes-Oxley-Act. Zum anderen gibt es auf nationaler Ebene sowohl *branchenübergreifende* als auch *branchenspezifische* Rechtsnormen. Besonders für die Telekommunikations- sowie für die Bankenbranche wurden Anforderungen an IT-Systeme gesetzlich formuliert. In dieser Arbeit soll auf die deutschen branchenübergreifenden Rechtsnormen zur ITS eingegangen werden. Es werden jedoch auch die jeweiligen branchenspezifischen Regelungen erwähnt, sofern sie Auswirkungen über die Branche hinaus haben und in Abschnitt 3.3 werden auch die Grundzüge des Sarbanes-Oxley-Act erläutert.

3 Branchenübergreifende Rechtsnormen zur ITS in Deutschland

3.1 Systematisierung der branchenübergreifenden Rechtsnormen

Anhand von Abb. 3 soll der Aufbau von Abschnitt 3 erklärt werden. Branchenübergreifend ist die Unternehmensleitung aufgrund ihrer *Sorgfaltspflicht* für die Erfüllung der rechtlichen Pflichten des Unternehmens verantwortlich. Dazu gehören die Pflicht zum

11 Vgl. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Gutachten zur rechtlichen Analyse des Regelungsumfangs zur IT-Sicherheit in kritischen Infrastrukturen, Online im Internet: http://www.bsi.bund.de/fachthem/kritis/Regelungsumfang_ITSich_KRITIS.pdf, 05.05.2005, S. xiii.

Risikomanagement, die *Buchführungspflicht* und die Pflicht zum *Schutz personenbezogener Daten*.

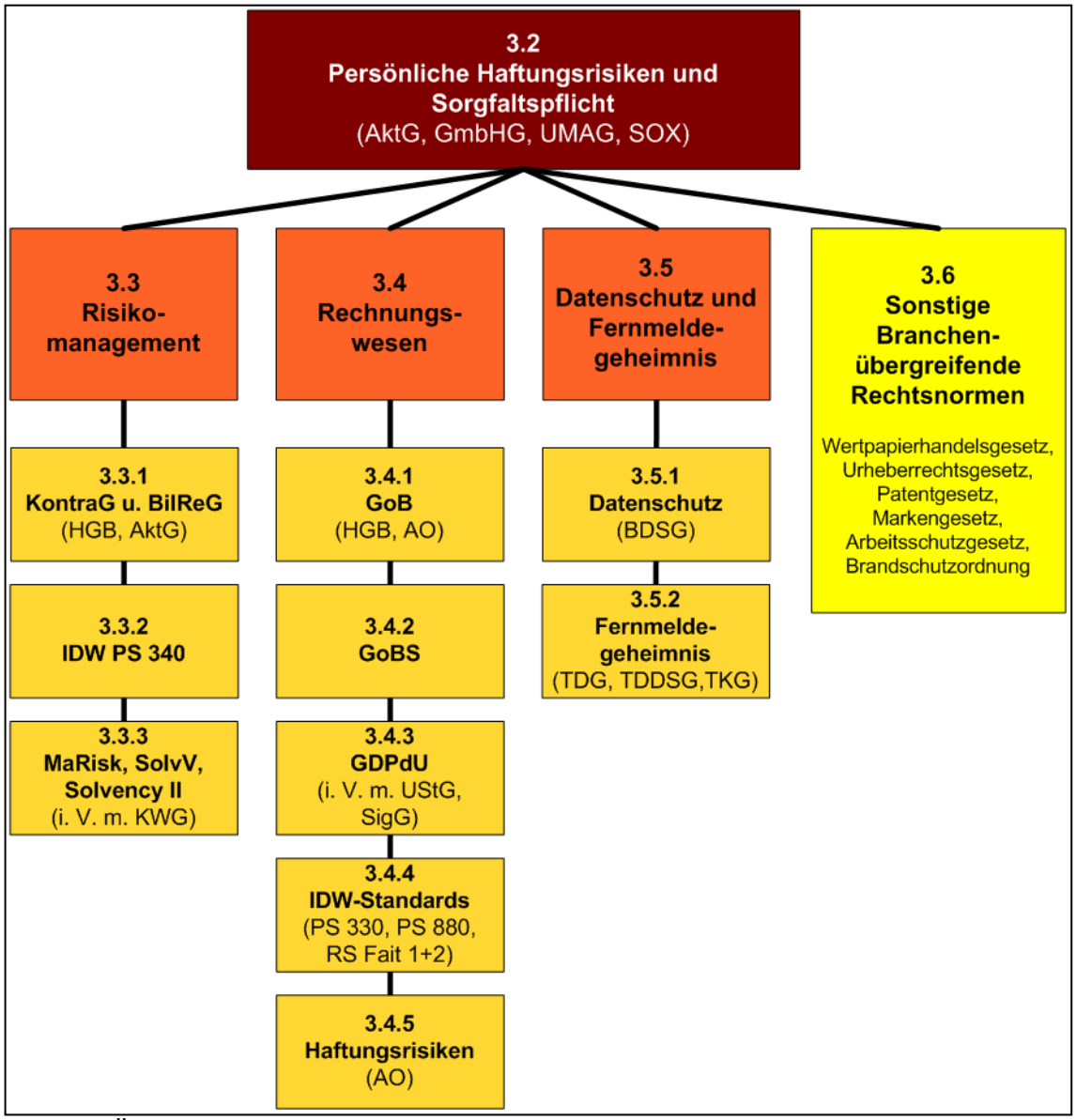

Abb. 3: Übersicht der untersuchten Rechtsnormen

Diese Pflichten haben jeweils explizit oder implizit einen Bezug zur ITS. In Abschnitt 3.2 soll zunächst auf die Sorgfaltspflicht und die haftungsrechtlichen Konsequenzen eingegangen werden. Anschließend sollen die Pflichten zum Risikomanagement (Abschnitt 3.3), zur Buchführung (Abschnitt 3.4) und zum Datenschutz (Abschnitt 3.5) erläutert werden. Darüber hinaus gibt es weitere rechtlich festgelegte Pflichten zur ITS, die in Abschnitt 3.6 kurz genannt werden.

3.2 Persönliche Haftungsrisiken und Sorgfaltspflicht

Sowohl die Geschäftsführer einer GmbH als auch die Vorstandsmitglieder einer Aktiengesellschaft sind durch den Gesetzgeber nach § 43 GmbHG[12] bzw. § 93 AktG[13] zur Sorgfalt eines ordentlichen Geschäftsmannes verpflichtet. Bei Pflichtverletzung haften sie für den entstandenen Schaden. Auch der Aufsichtsrat ist bei Verletzung seiner Kontrollpflichten nach § 116 AktG haftbar.

Das am 01.11.2005 in Kraft getretene Gesetz zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts (UMAG)[14] erleichtert es Gesellschaftern bzw. Aktionären, Schadenersatzklagen gegen Vorstand und Aufsichtsrat durchzusetzen.[15]

Die Sorgfaltspflicht beinhaltet auch die Sicherstellung des sicheren und rechtskonformen Einsatzes von IT, denn durch einen Systemausfall oder durch die Verletzung von Rechtsnormen können Unternehmensverluste und Imageschäden entstehen.[16] Somit haftet die Unternehmensführung persönlich für die Einhaltung der im Folgenden dargestellten Rechtsnormen. Teilweise sind auch in den einzelnen Gesetzen Haftungsregelungen getroffen worden, auf welche an geeigneter Stelle eingegangen wird.

Darüber hinaus sieht sich das Management von Unternehmen, die an einer amerikanischen Börse notiert sind, erweiterten Haftungsrisiken gegenüber. Der Sarbanes-Oxley-Act, der am 30. Juli 2002 in Kraft getreten ist, verlangt vom CEO und vom CFO eine eidesstattliche Beglaubigung der Angaben in der Finanzberichterstattung sowie die Einrichtung und Durchführung eines internen Kontrollsystems um die Verlässlichkeit und Ordnungsmäßigkeit der veröffentlichten Unternehmensdaten und den Schutz des vorhandenen Vermögens zu gewährleisten.[17] Ferner muss dies durch den Abschlussprüfer bestätigt werden. Verstöße können zivil- und strafrechtliche Folgen haben.[18]

12 Die folgenden Ausführungen beziehen sich auf das GmbHG in der im BGB Teil III, Gliederungsnummer 4123-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch das Gesetz vom 10.11.2006, BGBl. I S. 2553.

13 Die folgenden Ausführungen beziehen sich auf das Aktiengesetz (AktG) vom 6. September 1965, BGBl. I S. 1089, zuletzt geändert durch Artikel 13 des Gesetzes vom 5. Januar 2007, BGBl. I S. 10.

14 Die folgenden Ausführungen beziehen sich auf das Gesetz zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts (UMAG) vom 22.09.2005, BGB1. I Nr. 60, S. 2802 ff.

15 Vgl. Harder, Bernd H.: IT-Sicherheit: Haftungsrisiko für alle Führungskräfte, Online im Internet: http://www.harder-rechtsanwaelte.de/edv-recht/haftungsrisiko-bbb_0106.html, 24.04.2007.

16 Vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) (Hrsg.): Matrix der Haftungsrisiken – IT-Sicherheit – Pflichten und Risiken, Online im Internet: http://www.bitkom.org/files/documents/BITKOM_Leitfaden_Matrix_der_Haftungsrisiken-V1.1f.pdf, 27.04.2007, S. 8.

17 Vgl. Falk, Michael; Hofmann, Marc: Integration des IT-Sicherheitsmanagements in das Risikomanagement im Kontext bankaufsichtsrechtlicher Vorgaben, a. a. O., S. 26.

18 Vgl. Fischer, Norbert; Rotter, Norbert: Sarbanes-Oxley Act und die Final Rule Section 404: Management Assessment of Internal Controls, in: USA-Mitteilungen Oktober 2003, Hrsg.: KPMG Deutsche

Nicht nur die Unternehmensführung ist Haftungsrisiken ausgesetzt, sondern auch die Arbeitnehmer sind bei schuldhaft begangenen Pflichtverletzungen dem Arbeitgeber und ggf. auch gegenüber Dritten zum Schadensersatz verpflichtet.[19]

Unternehmensführung, IT-Leiter, Datenschutzbeauftragte und Mitarbeiter sehen sich also einer Vielzahl rechtlicher und mit persönlicher Haftung gekoppelten Pflichten im Zusammenhang mit ITS gegenüber, die nun dargestellt werden sollen.

3.3 Risikomanagement

3.3.1 Risikomanagementanforderungen nach KontraG und BilReG

In Reaktion auf einige Aufsehen erregende, durch Missmanagement verursachte, Unternehmenskrisen[20] wurden 1998 durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) Veränderungen am Aktiengesetz (AktG) sowie am Handelsgesetzbuch (HGB) vorgenommen.[21] Anwendung findet das KonTraG bei Aktiengesellschaften sowie mittelgroßen Kapitalgesellschaften gemäß § 267 HGB.[22]

Durch das KonTraG ist die Pflicht der Unternehmensführung zu einem Risikomanagement gesetzlich verankert.[23] So heißt es in § 91 Abs. 2 AktG: „Der Vorstand hat […] ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.“ Zu den bestandsgefährdenden Risiken „[…] gehören insbesondere risikobehaftete Geschäfte, Unrichtigkeiten der Rechnungslegung und Verstöße gegen gesetzliche Vorschriften, die sich auf die Vermögens-, Finanz- und Ertragslage […] wesentlich auswirken.“[24] Wegen der Bedeutung der IT für die Vermögens-, Finanz- und Ertragslage sowie den Fortbestand des Unternehmens sind implizit auch IT-Sicherheitsrisiken in das Überwachungssystem einzubeziehen.[25]

Die konkrete Ausgestaltung eines Risikomanagementsystems hat der Gesetzgeber nicht bestimmt. Gemäß der Gesetzesbegründung müssen jedoch ein Frühwarnsystem und ein

Treuhand-Gesellschaft Aktiengesellschaft Wirtschaftsprüfungsgesellschaft, Online im Internet: http://www.kpmg.de/library/pdf/031014_USA_Mitteilungen_Oktober2003_de.pdf, 24.04.2007.

19 Vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) (Hrsg.): Matrix der Haftungsrisiken – IT-Sicherheit – Pflichten und Risiken, a. a. O., S. 15.

20 Vgl. Pollanz, Manfred: Offene Fragen der Prüfung von Risikomanagementsystemen nach KonTraG , in: Der Betrieb, Heft 25 vom 22.6.2001, S. 1317.

21 Die folgenden Ausführungen beziehen sich auf das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KontraG) vom 27.04.1998, BGB1. I Nr. 24, S. 786 ff.

22 Vgl. Heinrich, Robert; Lang, Franz-Josef: DV und Recht/Risikobewertung und Frühwarnsysteme – Ein neues Gesetz macht die IT-Sicherheit zur Pflicht, in: Computerwoche, 24/1999, S. 71.

23 Vgl. Eckert, Claudia: IT-Sicherheit, München; Wien: Oldenbourg Verlag 2006, S. 176.

24 Deutscher Bundestag (Hrsg.): Bundestag-Drucksache 13/9712, Anlage 1, Entwurf eines Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), S. 15.

25 Vgl. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Gutachten zur rechtlichen Analyse des Regelungsumfangs zur IT-Sicherheit in kritischen Infrastrukturen, a. a. O., S. 12.

internes Überwachungssystem inklusive Revision und Controlling enthalten sein.[26] Durch das Frühwarnsystem sollen rechtzeitige Gegenmaßnahmen ermöglicht werden.

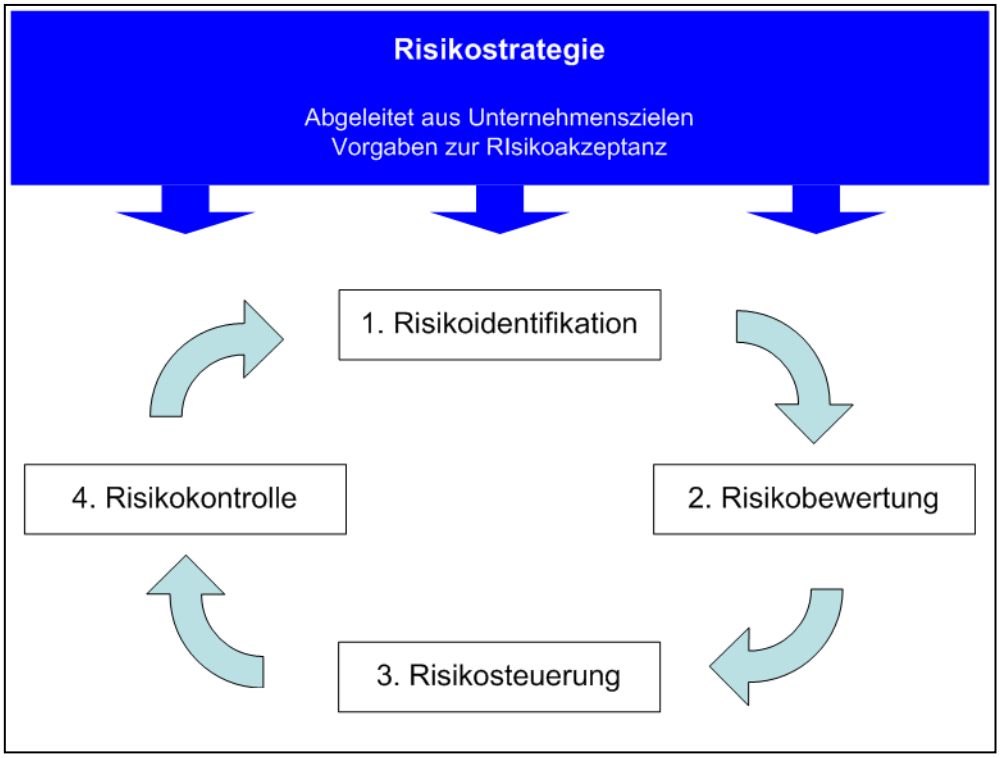

Abb. 4: Der Risikomanagement-Kreislauf[27]

Ein dementsprechender Risikomanagementprozess kann in einen Kreislauf, wie in Abb. 4 dargestellt, aus vier Phasen aufgeteilt werden. Diesem ist eine Risikostrategie übergeordnet, die aus den Unternehmenszielen abgeleitet wird und die Risikoakzeptanz sowie den Umgang mit Risiken im Unternehmen festschreibt. In Phase Eins werden die Risiken identifiziert und anschließend in Phase Zwei bewertet. In der dritten Phase, der Risikosteuerung, werden die Risiken entweder vermieden, verringert, überwälzt (z. B. an Versicherungen) oder selbst getragen bzw. akzeptiert.[28] Durch IT-Sicherheitsmaßnahmen können IT-Risiken verringert werden, der Umfang der nötigen Maßnahmen hängt jedoch von der branchen- und unternehmensspezifischen Risikosituation sowie von der jeweiligen Risikoakzeptanz ab. Die Risikokontrolle bildet die vierte Phase des Kreislaufs und vereinigt Risiko-Controlling und Revision. Der Erfolg der übrigen Phasen soll hier überwacht werden und ggf. Anpassungen der Maßnahmen, Methoden sowie der Risikostrategie angestoßen werden.[29]

26 Vgl. Eckert, Claudia: IT-Sicherheit, München; Wien: Oldenbourg Verlag 2006, S. 176.

27 Falk, Michael; Hofmann, Marc: Integration des IT-Sicherheitsmanagements in das Risikomanagement im Kontext bankaufsichtsrechtlicher Vorgaben, a. a. O., S. 58

28 Vgl. Krystek, Ulrich; Fiege, Stefanie: Risikomanagement, in: Gabler Wirtschaftslexikon, 16. vollständig aktualisierte und überarbeitete Auflage, Wiesbaden: Gabler 2004, S. 2558.

29 Vgl. Falk, Michael; Hofmann, Marc: Integration des IT-Sicherheitsmanagements in das Risikomanagement im Kontext bankaufsichtsrechtlicher Vorgaben, a. a. O., S. 63 f.

Durch das KonTraG werden auch die Wirtschaftsprüfer stärker in die Pflicht genommen. § 317 HGB verlangt, dass der Abschlussprüfer dem Vorstand börsennotierter Aktiengesellschaften attestiert, ein geeignetes Überwachungssystem eingerichtet zu haben. Nach § 321 HGB soll im Prüfungsbericht darauf eingegangen werden, ob Verbesserungsmaßnahmen nötig sind. Darüber hinaus ist auch zu prüfen, ob im Lagebericht gemäß § 289 HGB angemessen auf die Risiken der zukünftigen Entwicklung eingegangen wurde. Analog gilt § 315 HGB für den Konzernlagebericht.

Aufgrund des Bilanzrechtsreformgesetzes (BilReG) vom 4.12.2004[30] haben sich zusätzliche Änderungen am HGB ergeben: im Lagebericht sollen zusätzlich die Risikomanagementziele und -methoden dargestellt werden.

3.3.2 Risikomanagementanforderungen des IDW

Die Ansprüche an das Risikomanagement prüfungspflichtiger Unternehmen wurden durch das Institut der Wirtschaftsprüfer (IDW) im Prüfungsstandard 340 (die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB) konkretisiert.[31] An dieser Stelle sollen nur einige wichtige Anforderungen daraus genannt werden. Das Risikomanagement soll an die operativen Prozesse angebunden und die Verantwortlichkeit dafür organisatorisch verankert sein. Ferner werden die Dokumentation der verwendeten Risikomodelle und des Risikomanagementprozesses sowie die Kommunikation nicht bewältigter Risiken geprüft.[32] Eine Nichtbeachtung der Anforderungen kann zur Versagung des Bestätigungsvermerks führen. Ein solcher Vorfall hat erhebliche Imageschäden zur Folge und kann sogar zur Insolvenz führen, wenn die Kapitalgeber dem Unternehmen das Vertrauen entziehen.

3.3.3 MaRisk, SolvV und Solvency II

Zusätzlich existieren branchenspezifische Vorschriften für die Einrichtung eines Risikomanagementsystems. Betroffen ist hier vor allem der Finanzdienstleistungssektor, der von der Bundesanstalt für Finanzdienstleitungsaufsicht (BaFin) überwacht wird.

Die BaFin verlangt in den Mindestanforderungen an das Risikomanagement (MaRisk), auch IT-Risiken zu betrachten. So müssen die Finanzdienstleister über eine angemessene technisch-organisatorische Ausstattung verfügen, um die Schutzziele der Integrität,

30 Die folgenden Ausführungen beziehen sich auf das Gesetz zur Einführung internationaler Rechnungslegungsstandards und zur Sicherung der Qualität der Abschlussprüfung (Bilanzrechtsreformgesetz – BilReG) vom 9.12.2004, BGB1. I. Nr. 65, S. 3166 ff.

31 Vgl. IDW (Hrsg.): Die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB (IDW PS 340), in: WPg 1999, Heft-Nr. 16/1999, S. 658 ff.

32 Vgl. Schmidt, Klaus: Der IT Security Manager, München: Hanser Verlag 2006, S. 267.

Vertraulichkeit, Verfügbarkeit und Authentizität bezüglich der Daten zu gewährleisten. Ein regelmäßig zu testendes Notfallkonzept soll potentielle Schäden bei Systemausfällen verringern, indem Geschäftsfortführungs- und Wiederanlaufpläne erstellt werden.[33]

Im Rahmen der Solvabilitätsverordnung (SolvV), welche die §§ 10 und 10a des Kreditwesengesetzes (KWG)[34] konkretisiert, fordert die BaFin eine angemessene Risikounterlegung mit Eigenkapital.[35] Dies hat weit reichende Folgen über die Finanzdienstleistungsbranche hinaus. Denn bei der Kreditvergabe müssen die Banken nun ein Rating des Kreditnehmers vornehmen. Je höher das Ausfallrisiko zu bewerten ist, desto mehr Eigenkapital müssen sie hinterlegen und die steigenden Opportunitätskosten könnten sie in Form höherer Zinsen weitergeben. In die Risikobewertung fließen laut SolvV auch die operationellen Risiken ein. Diese umfassen auch IT-Risiken und rechtliche Risiken.[36] Sofern das jeweilige Ausfallrisiko in die Kreditbepreisung einfließt, können Unternehmen durch geeignete Sicherheitsmaßnahmen ihr operationelles Risiko verringern und so durch geringere Kreditzinsen ihre Kapitalkosten senken.

Voraussichtlich im Jahr 2010 soll die europäische Eigenmittelausstattungsverordnung Solvency II der Europäischen Kommission in Kraft treten. Diese stellt an die Versicherungsbranche risikoorientierte Anforderungen zur Eigenkapitalunterlegung von Risiken.[37] Die branchenübergreifenden Auswirkungen dieser Verordnung sind analog zur SolvV zu sehen. ITS hat dann Auswirkungen auf die Versicherungskosten und dadurch auch auf das Risikomanagement in den Unternehmen. Denn die ITS wirkt in diesem Zusammenhang auch auf die Risikoüberwälzungsmöglichkeiten und somit auf die Risikosteuerung im Allgemeinen über die IT-spezifischen Risiken hinaus.

IT-Risikomanagement und Risikosteuerung als Bestandteile des Risikomanagements implizieren Maßnahmen zur Abwälzung, Vermeidung und Reduzierung sowie zum Tragen von IT-Risiken. Ebenso gilt es, um rechtliche Risiken zu reduzieren, die übrigen Rechtsnormen zur ITS zu berücksichtigen. Somit thematisiert die Fülle der Anforderun-

33 Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (Hrsg.): Rundschreiben 18/2005: Mindestanforderungen an das Risikomanagement, Online im Internet: http://www.bafin.de/rundschreiben/89_2005/051220.htm, 20.12.2005.

34 Die folgenden Ausführungen beziehen sich auf das Gesetz über das Kreditwesen (Kreditwesengesetz - KWG) vom 9.9.1998, BGBl. I S. 2776, zuletzt geändert durch Art. 8 des Gesetzes vom 5.1.2007, BGBl. I S. 10.

35 Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (Hrsg.): Rundschreiben 18/2005: Mindestanforderungen an das Risikomanagement, a. a. O.

36 Vgl. Hirschmann, Stefan; Romeike, Frank: IT-Sicherheit als Rating-Faktor, in: RATINGaktuell, 01/2004, S. 13.

37 Vgl. Romeike, Frank; Müller-Reichart, Matthias; Hein, Thorsten: Die Assekuranz am Scheideweg - Ergebnisse der ersten Benchmark-Studie zu Solvency II, in: Zeitschrift für Versicherungswesen, 10/2006, S. 316.

gen an das Risikomanagement implizit alle Schutzziele der ITS, da aus deren Beeinträchtigung erhebliche Risiken erwachsen können.

3.4 Buchführung

3.4.1 Buchführungspflicht und GoB

Die Unternehmen sind nach § 238 HGB[38] bzw. § 141 Abgabenordnung (AO)[39] verpflichtet, ihre Bücher nach den Grundsätzen ordnungsgemäßer Buchführung (GoB) zu führen.[40] Vom Gesetzgeber wird keine bestimmte Form der Buchführung vorgegeben, es werden vielmehr Mindestanforderungen normiert, für deren Einhaltung die gesetzlichen Vertreter der Unternehmen verantwortlich sind, selbst wenn die Buchführung von einem Dritten, z. B. einem Steuerberater, übernommen wird.[41] Von den GoB, die teilweise in den §§ 145 bis 147 AO sowie den §§ 238, 239 und 257 HGB kodifiziert wurden, sind auch die Schutzziele der ITS betroffen, denn heutzutage wird die Buchführung in der Regel „elektronisch“ unter Zuhilfenahme entsprechender IT-Anwendungen durchgeführt. Außerdem beziehen sich die Anforderungen auch auf IT-Systeme außerhalb der Buchführung, weil diese meist auch buchführungsrelevante Daten verarbeiten und zudem technisch mit dem Buchführungssystem verbunden sind. Bspw. lassen sich Buchführungs- und übrige Systeme im Rahmen von ERP-Systemen kaum noch voneinander abgrenzen.[42]

§ 239 HGB bzw. § 146 AO erlauben die Buchführung auf Datenträgern, fordern aber eine vollständige, richtige, zeitgerechte und geordnete Aufzeichnung. Diese Forderung betrifft v. a. die Schutzziele der Verfügbarkeit und Integrität. Auch die Verbindlichkeit wird nach § 239 HGB miteinbezogen, denn die Aufzeichnungen dürfen „nicht in einer Weise verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist. Auch solche Veränderungen dürfen nicht vorgenommen werden, deren Beschaffenheit es ungewiss lässt, ob sie ursprünglich oder erst später gemacht worden sind.“

38 Die folgenden Ausführungen beziehen sich auf das Handelsgesetzbuch in der im Bundesgesetzblatt Teil III, Gliederungsnummer 4100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 5 des Gesetzes vom 5. Januar 2007, BGBl. I S. 10.

39 Die folgenden Ausführungen beziehen sich auf die Abgabenordnung in der Fassung der Bekanntmachung vom 1. Oktober 2002, BGBl. I S. 3866; 2003 I S. 61, zuletzt geändert durch Artikel 10 des Gesetzes vom 13. Dezember 2006, BGBl. I S. 2878.

40 Vgl. Witt, Bernhard C.: IT-Sicherheit kompakt und verständlich, Neu-Ulm: Vieweg Verlag 2006, S. 5.

41 Vgl. Henn, Martin: Anforderungen an die Ordnungsmäßigkeit der EDV-Buchführung, in: Buchführung, Bilanzierung, Kostenrechnung (BBK), Nr. 4 vom 17.2.2006, S. 1188.

42 Vgl. Henn, Martin: Anforderungen an die Ordnungsmäßigkeit der EDV-Buchführung, a. a. O., S. 1190.

Die Verfügbarkeit wird zusätzlich betont: die Daten müssen während der Aufbewahrungsfrist jederzeit verfügbar und in angemessener Frist lesbar gemacht werden können. Laut §§ 257 HGB sind buchführungsrelevante Unterlagen für sechs bzw. zehn Jahre aufzubewahren. Im Steuerrecht gelten nach § 147 AO weitgehend deckungsgleiche Anforderungen, allerdings zusätzlich auch für sonstige steuerlich relevante Unterlagen.[43] Konkret bedeutet dies, dass z. B. Angebote, Auftragsbestätigungen, Lieferscheine sowie Reklamationsschreiben und -E-Mails, nicht jedoch Werbeschreiben und Prospekte aufbewahrt werden müssen.[44] Werden Unterlagen auf Bild- oder Datenträgern aufbewahrt, so müssen sie bildlich und inhaltlich mit den Originalen übereinstimmen. Auch um eigene Ansprüche nachweisen zu können, empfiehlt sich die Aufbewahrung wichtiger geschäftlicher Unterlagen ggf. über die gesetzlichen Fristen hinaus.

Allein schon durch die Buchführungspflicht an sich ist implizit auch die Vertraulichkeit erforderlich, denn regelmäßig werden hier sensible Unternehmensdaten verarbeitet. Somit umfassen Rechtsnormen zur Buchführung alle betrachteten Schutzziele der ITS.

3.4.2 GoBS

Die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) wurden 1995 durch das Bundesministerium der Finanzen veröffentlicht. Sie konkretisieren die nötigen Maßnahmen, Regelungen und Kontrollen um den GoB bei elektronischer Buchführung gerecht zu werden. Es werden keine konkreten Lösungen vorschlagen, die vorgenommenen Maßnahmen sollen sich aber nach dem jeweiligen Stand der Technik richten.[45]

Nach § 238 HGB sollen die Geschäftsvorfälle für einen sachverständigen Dritten nachvollziehbar sein. Dafür soll das Buchführungssystem (BFS) drei Funktionen erfüllen, die (1) Belegfunktion, die (2) Journalfunktion und die (3) Kontenfunktion. Die betroffenen Schutzziele werden im Folgenden in Klammern hinter den jeweiligen Anforderungen genannt.[46]

Die Belegfunktion ist die Voraussetzung für die Beweiskraft der Buchführung. Elektronische wie Papier-(Ur-)Belege sollen dem Aussteller zurechenbar und unabänderlich sein. Änderungen der Buchungen dürfen nur mit Berichtigungsbuchungen durch einen

43 Vgl. Haiges, Ingo: Aspekte der Daten- und Dokumentensicherheit - Verfügbar, lesbar, dennoch sicher, in: Beschaffung aktuell, 07.07.2005, S. 34.

44 Vgl. Anduleit, Manfred: Datenarchivierung - ganz nach Vorschrift, in: Computerwoche, 01.02.2007, Online im Internet: http://www.computerwoche.de/it_strategien/it_management/586945/, 15.02.2007.

45 Vgl. Bittner, Klaus: Grundsätze ordungsmäßiger DV-gestützter Buchführungssysteme (GoBS), in: Buchführung, Bilanzierung, Kostenrechnung (BBK), Nr. 24 vom 20.12.1995, S. 989.

46 Vgl. Bittner, Klaus: Grundsätze ordungsmäßiger DV-gestützter Buchführungssysteme (GoBS), a. a. O., S. 990.

per Zugriffsschutz autorisierten Mitarbeiter erfolgen (betr. Verbindlichkeit, Integrität, Vertraulichkeit). Dies wird auch für die Journalfunktion gefordert. Für die Kontenfunktion müssen Erfassungskontrollen die formale Richtigkeit der Buchungen und die Übereinstimmung mit den Buchungsjournalen sicherstellen (betr. Integrität).[47] Das jeweilige Archivierungssystem soll nachweisbar die Integrität und Authentizität der auf Datenträgern geführten Unterlagen gewährleisten.[48]

Die GoBS verlangen die Einrichtung eines *internen Kontrollsystems* (IKS), welches die folgenden vier Ziele erfüllen soll:

1) Schutz von Vermögen und Informationen,
2) Vollständigkeit, Genauigkeit, Aussagefähigkeit und Zeitnähe der Aufzeichnungen,
3) Auswertung und Kontrolle der Aufzeichnungen und
4) Unterstützung der Geschäftspolitik.

Sicherheitsrelevante Handlungsbedarfe bestehen für die IT-Systeme v. a. im Nachweis der korrekten Funktionsweise verwendeter BFS (insbesondere bei Eigenentwicklungen, betr. Integrität) und im Erfordernis von Zugriffsbeschränkungen (betr. Vertraulichkeit).

Eine zentrale Forderung der GoBS ist die nach einem umfassenden, detailliert dokumentierten *Datensicherheitskonzept*. Die Daten sollen vor Verlust (betr. Verfügbarkeit und teilweise Vertraulichkeit) und gegen unberechtigte Veränderung und Kenntnisnahme geschützt sein (betr. Verbindlichkeit, Integrität, Vertraulichkeit). Explizit beziehen die GoBS nicht bloß die Buchführungsdaten sondern auch die übrigen für das Unternehmen wichtigen Daten mit ein. Allerdings ist nur die Sicherheit der Buchführungsdaten, mindestens für die Dauer der Aufbewahrungsfristen obligatorisch.

In dieser Frist müssen sie *vor Verlust geschützt* sein *und jederzeit lesbar* gemacht werden können. Deshalb muss die notwendige Hard- und Software zum Lesen der Sicherungsdatenträger stets funktionsfähig vorhanden sein. Dies stellt wegen des rasanten technischen Fortschritts ein Problem dar, denn veraltete Ausstattung kann dann bei Defekten oft nicht mehr bezogen bzw. repariert werden. Die Sicherungssoftware und die Sicherungshardware muss also vorausschauend ausgewählt werden. Ggf. sollten mehrere Verfahren parallel eingesetzt werden. Des Weiteren ist die Verantwortung für die Durchführung von Datensicherungen organisatorisch zu verankern. Neben periodischen

47 Vgl. Bittner, Klaus: Grundsätze ordungsmäßiger DV-gestützter Buchführungssysteme (GoBS), a. a. O., S. 991.

48 Vgl. o. V.: Grundsätze ordungsmäßiger DV-gestützter Buchführungssysteme (GoBS) vom 07.11.1995, Online im Internet: http://www.elektronische-steuerpruefung.de/rechtsgrund/gobs.pdf, 23.04.2007.

Sicherungen sollten weitere Sicherungen vorgenommen werden, wenn zwischen zwei regelmäßigen Sicherungszeitpunkten viele Daten verändert wurden. Die GoBS empfehlen auch die Aufbewahrung der Sicherungsmedien an mehreren Orten. Um die jederzeitige Auffindbarkeit der Datenbestände zu sichern, soll ein ausführliches Datenträgerverzeichnis angelegt werden. Die letztgenannten Maßnahmen zielen in erster Linie auf das Schutzziel der Verfügbarkeit ab.

Die folgenden Maßnahmen sollen zusätzlich die Integrität der Daten gewährleisten. Das Risiko einer Vernichtung oder Beeinträchtigung der Datenträger soll durch Schutzmaßnahmen gegen Feuer, Temperatur, Feuchtigkeit und Magnetfelder in „erforderlichem Maße“ reduziert werden. Darüber hinaus soll bei Langzeitspeicherung die Lesbarkeit der Sicherungsmedien in regelmäßigen Abständen geprüft werden, da z. B. ein Magnetband mit der Zeit entmagnetisiert und die Integrität und Verfügbarkeit der Daten dadurch eingeschränkt sein kann. Die Zeitintervalle hängen hierbei von der Lebensdauer der verwendeten Medien ab. [49]

Die geforderte Aufbewahrung der Datenträger in einbruchssicheren Räumen bzw. Tresoren soll das Diebstahlrisiko senken (betr. Verfügbarkeit, Vertraulichkeit) und dient sowohl zum Schutz der Daten vor Verlust als auch zur *Sicherung gegen unberechtigte Veränderung und Kenntnisnahme*. Für letzteres sind gemäß GoBS außerdem Zugriffskontrollen einzurichten, die gewährleisten, dass nur berechtigte Personen entsprechend ihrem Aufgabenbereich Zugriff auf Programme und Daten erhalten. Zum anderen werden Zugangskontrollen zu den Räumen gefordert, in denen die Datenträger aufbewahrt werden.[50] Zugriffs- u. Zugangskontrollen zielen auf die Vertraulichkeit, Integrität, Verbindlichkeit und Verfügbarkeit ab, da das Risiko einer unberechtigten Veränderung, Löschung, Vernichtung oder Kenntnisnahme der Daten verringert wird.

Um die Ordnungsmäßigkeit des BFS sicherzustellen, verlangen die GoBS eine detaillierte *Verfahrensdokumentation* bezüglich der Erfüllung der Beleg-, Journal- und Kontenfunktion, des IKS und des Datensicherheitskonzeptes. Der erforderliche Umfang der Dokumentation richtet sich nach der Komplexität des BFS.[51] Die Verfahrensdokumentation ist 10 Jahre aufzubewahren.[52]

49 Vgl. o. V.: Grundsätze ordungsmäßiger DV-gestützter Buchführungssysteme (GoBS) vom 07.11.1995, a. a. O.

50 Vgl. o. V.: Grundsätze ordungsmäßiger DV-gestützter Buchführungssysteme (GoBS) vom 07.11.1995, a. a. O.

51 Vgl. Bittner, Klaus: Grundsätze ordungsmäßiger DV-gestützter Buchführungssysteme (GoBS), a. a. O., S. 990 f.

52 Vgl. o. V.: Grundsätze ordungsmäßiger DV-gestützter Buchführungssysteme (GoBS) vom 07.11.1995, a. a. O.

Die GoBS decken als Konkretisierung der GoB ebenfalls sämtliche Schutzziele der ITS ab und fordern v. a. im Hinblick auf die Sicherstellung der Verfügbarkeit und Integrität umfangreiche Maßnahmen von den buchführungspflichtigen Unternehmen.

3.4.3 GDPdU

Die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) vom 16.07.2001 konkretisieren die Anforderungen der Finanzbehörde an Buchführungssysteme und nehmen dabei Bezug auf die GoBS.

Im ersten Abschnitt wird das Recht der Finanzbehörde behandelt, die IT-gestützte Buchführung des Steuerpflichtigen durch Datenzugriff auf steuerlich relevante Daten zu prüfen. Das BFS muss der Finanzbehörde die geforderten Daten jederzeit zur Verfügung stellen können (betr. Verfügbarkeit). Diese hat das Recht auf unmittelbaren Lesezugriff über das BFS des Steuerpflichtigen, mittelbaren Lesezugriff durch maschinelle Auswertungen und Überlassung der Daten auf maschinell verwertbaren Datenträgern.[53]

Für den unmittelbaren Datenzugriff müssen dem Steuerprüfer die Zugriffsrechte auf alle steuerlich relevanten Daten des Steuerpflichtigen eingerichtet werden – und zwar nur hierauf. Dies hat Implikationen für das Schutzziel der Vertraulichkeit: ein Steuerberater könnte z. B. versehentlich auch Buchführungsdaten anderer Mandanten freigeben. Analog sind jeweils nur die erforderlichen Daten für den „mittelbaren Datenzugriff“ und im Rahmen der „Datenträgerüberlassung“ bereit zu stellen. Darüber hinaus ist die Unveränderlichkeit des Datenbestandes zu gewährleisten (betr. Integrität).[54]

Der zweite Abschnitt der GDPdU stellt Anforderungen an die Prüfbarkeit der Unterlagen. Nach § 14 Umsatzsteuergesetz (UStG)[55] darf die Vorsteuer nur abgezogen werden, wenn Echtheit und inhaltliche Unversehrtheit der Rechnung gewährleistet sind. Gemäß § 15 Abs. 1 Signaturgesetz (SigG)[56] brauchen diese Rechnungen dazu eine qualifizierte Signatur mit Anbieterakkreditierung.[57] Die GDPdU fordern die Speicherung der Daten auf nicht mehr änderbaren Datenträgern. Werden änderbare Datenträger eingesetzt, muss von Seiten des Datenverarbeitungssystems die Unabänderlichkeit sichergestellt

53 Vgl. o. V.: Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), Online im Internet: http://www.aufbewahrungspflicht.de/pdfs/gdpdu.pdf, 16.07.2001, Abschnitt I.

54 Vgl. o. V.: Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), a. a. O., Abschnitt I.

55 Die folgenden Ausführungen beziehen sich auf das Umsatzsteuergesetz in der Fassung der Bekanntmachung vom 21.02.2005, BGBl. I S. 386, zuletzt geändert durch Artikel 7 des Gesetzes vom 13.12.2006, BGBl. I S. 2878.

56 Die folgenden Ausführungen beziehen sich auf das Signaturgesetz vom 16.02.2001, BGBl. I S. 876, zuletzt geändert durch Artikel 4 des Gesetzes vom 26.02.2007, BGBl. I S. 179.

57 Vgl. Hofmann, Kathrin: Dokumente rechtssicher speichern, in: IT-Business News, 26.02.2007.

werden.[58] Es kann somit ratsam sein, sog. „write once read multiple"-Medien (WORM) einzusetzen. Nicht wiederbeschreibbare optische Medien wie CD-R, DVD-R und DVD+R sind hier zu nennen, aber mittlerweile gibt es auch WORM-fähige Magnetbandlösungen.[59] Darüber hinaus müssen originär digitale Unterlagen in elektronisch auswertbarer, strukturierter Form vorgehalten werden. Die alleinige Verwendung der unstrukturierten Papier-, Mikrofilm- oder PDF-Formate ist nicht erlaubt. Etwaige verwendete Signatur- und Kryptographieschlüssel müssen aufbewahrt werden.[60]

Während im ersten Abschnitt der GDPdU die Schutzziele der Verfügbarkeit, Integrität und Vertraulichkeit im Mittelpunkt stehen, werden im zweiten Abschnitt die Verbindlichkeit und die Integrität betont. Insgesamt decken die GDPdU also ebenfalls alle Schutzziele der ITS ab.

3.4.4. IDW-Standards und -Verlautbarungen

Auch das IDW hat verschiedene Standards veröffentlicht, in denen die Anforderungen an die elektronische Buchführung konkretisiert werden.

IDW PS 330 (Abschlussprüfung bei Einsatz von Informationstechnologie) behandelt einen Teilbereich der Prüfung des IKS (siehe auch GoBS). Folgende Voraussetzungen für ITS werden in diesem PS explizit genannt: Vertraulichkeit, Verfügbarkeit, Authentizität, Autorisierung,[61] Verbindlichkeit und Integrität.[62]

Der Prüfer soll Sicherheitsmaßnahmen wie Zugriffs- und Zutrittskontrollen sowie Datensicherungsverfahren beurteilen. Die verwendeten Programme sollen auf korrekte Funktion getestet werden (betr. Integrität).

Standardsoftware wird schon beim Softwarehersteller gemäß IDW PS 880 (Erteilung und Verwendung von Softwarebescheinigungen) geprüft.[63]

In IDW RS FAIT 1 werden die gleichen Schutzziele formuliert.[64] Hinsichtlich dieser Ziele werden Anforderungen in sechs Bereichen gestellt:

---

58 Vgl. o. V.: Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), a. a. O., Abschnitt II.

59 Vgl. Wirz, Erik: Vorschriften und Lösungsansätze - Langzeitarchivierung digitaler Daten, Online im Internet: http://www.lanline.de/article.html?thes=&art=/articles/2005008/30451905_ha_LL.html, 01.09.2005.

60 Vgl. o. V.: Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), a. a. O., Abschnitt II.

61 Autorisierung fordert, dass nur berechtigte Nutzer die Daten lesen, ändern oder löschen können. Dies wird allerdings durch die Vertraulichkeit, die Integrität und die Verfügbarkeit abgedeckt.

62 Vgl. Institut der Wirtschaftsprüfer (Hrsg.): IDW-Prüfungsstandard: Abschlussprüfung bei Einsatz von Informationstechnologie (IDW PS 330), WPg 2002, Heft Nr. 21/2002, S. 1167 ff.

63 Vgl. Müller, Klaus-Rainer: Handbuch Unternehmenssicherheit - umfassendes Sicherheits-, Kontinuitäts- und Risikomanagement mit System, 1. Auflage, Wiesbaden: Vieweg Verlag 2005, S. 93 f.

1) IT-Umfeld und IT-Organisation,
2) IT-Infrastruktur,
3) IT-Anwendungen,
4) IT-gestützte Geschäftsprozesse,
5) Überwachung des IT-Kontrollsystems und
6) IT-Outsourcing.[65]

IDW RS FAIT 2 geht näher auf die Risiken beim Einsatz von E-Commerce-Systemen ein.[66]

Die IDW-Standards und -Verlautbarungen erfassen alle untersuchten Schutzziele der ITS. Es sind jeweils nur die rechnungslegungsrelevanten IT-Systeme zu prüfen, aber in Abschnitt 3.4.1 wurde bereits dargelegt, dass auch Systeme außerhalb des BFS rechnungslegungsrelevante Daten verarbeiten oder erzeugen. Eine Nichtbeachtung der Anforderungen kann zur Versagung oder Einschränkung des Bestätigungsvermerks führen. Im Abschnitt 3.4.2 wurde bereits auf die Prüfung des Risikomanagements eingegangen. Durch den risikoorientierten Prüfungsansatz bewirken größere IT-Risiken einen größeren Umfang der Prüfungshandlungen und somit höhere Prüfungshonorare. Zusätzlich steigt aus Unternehmenssicht das Entdeckungsrisiko bzgl. wesentlicher Fehler in der Buchführung, die bei niedrigerem IT-Sicherheitsniveau ohnehin wahrscheinlicher sind.

3.4.5. Haftungsrisiken im Zusammenhang mit der Buchführungspflicht

Verletzt das Unternehmen die Buchführungspflicht, kann dies strenge Strafen von Seiten der Finanzbehörden nach sich ziehen. Bei nicht ordnungsgemäßer Buchführung kann die Finanzbehörde laut § 162 AO eine Steuerschätzung auf Basis der bekannten Besteuerungsgrundlagen vornehmen. Bei Verletzung der Aufbewahrungspflichten kann sie ein Zwangsgeld verhängen (§ 328 AO), den Vorwurf der Steuerhinterziehung (§ 370 AO) oder der leichtfertigen Steuerverkürzung (§ 378 AO) erheben. Dies kann zu Geld- oder Freiheitsstrafen von bis zu fünf Jahren führen. Werden die Anforderungen der GDPdU nicht erfüllt, ist mit einem Bußgeld von 5000 Euro wegen Steuergefährdung (§ 379 AO) oder 50.000 Euro wegen Steuerordnungswidrigkeit (§ 377 AO) zu rechnen.

64 Vgl. Institut der Wirtschaftsprüfer (Hrsg.): IDW-Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1), WPg 2002, Heft-Nr. 21/2002, S. 1157, Tz. 23.

65 Vgl. Institut der Wirtschaftsprüfer (Hrsg.): IDW-Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1), a. a. O., Kapitel 4.

66 Vgl. Müller, Klaus-Rainer: Handbuch Unternehmenssicherheit - umfassendes Sicherheits-, Kontinuitäts- und Risikomanagement mit System, a. a. O., S. 93 f.

Auch ein Zwangsgeld in Höhe von bis zu 25.000 Euro kann nach § 328 AO verhängt werden.[67] Darüber hinaus erfasst die Sorgfaltspflicht, wie oben bereits dargestellt, auch die Buchführungspflicht und dies hat ebenfalls haftungsrechtliche Auswirkungen.

3.5 Datenschutz und Fernmeldegeheimnis

3.5.1 Datenschutz

Sofern in IT-Systemen personenbezogene Daten verarbeitet werden, sind bezüglich der ITS zusätzliche Anforderungen zu beachten. Hier sind für die meisten Unternehmen in erster Linie das Bundesdatenschutzgesetz (BDSG) und das Teledienstedatenschutzgesetz (TDDSG) einschlägig.[68]

Der erhöhte Schutzbedarf personenbezogener Daten ergibt sich aus dem grundgesetzlichen Persönlichkeitsrecht, welches nach dem Volkszählungsurteil des Bundesverfassungsgerichts von 1983 auch das Recht auf informationelle Selbstbestimmung umfasst. Die Betroffenen dürfen demnach grundsätzlich selbst über die Erhebung, Verwendung und Weitergabe ihrer persönlichen Daten entscheiden. Nur auf der Basis einer Rechtsgrundlage (gesetzliche Vorschrift, Vertragsverhältnis, vertragsähnliches Vertrauensverhältnis oder Einwilligung des Betroffenen) darf in dieses Recht eingegriffen werden.[69]

Entsprechend dürfen Unternehmen nach § 4 BDSG[70] personenbezogene Daten ihrer Kunden nur unter enger Zweckbindung an das zugrunde liegende Vertragsverhältnis, für per Gesetz erlaubte Zwecke (siehe hierzu insbesondere § 28 BDSG), oder aufgrund einer ausdrücklichen Einwilligung erheben, verarbeiten oder nutzen (z. B. weiterleiten).[71] Personenbezogene Daten werden in § 3 Abs. 1 BDSG wie folgt definiert: „Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).“ Grundsätzlich sind die entsprechenden IT-Systeme gemäß § 3 a BDSG auf Datenvermeidung und Datensparsamkeit auszurichten. Nach § 9 BDSG die folgenden acht technischen und organisatorischen Kontrollmaßnahmen zu treffen, die in der Anlage zu § 9 Satz 1 BDSG genannt werden, sofern sie wirtschaftlich sind:

67 Vgl. o. V.: Datenarchivierung - ganz nach Vorschrift, in: Computerwoche, 01.02.2007.

68 Vgl. Müller, Klaus-Rainer: Handbuch Unternehmenssicherheit - umfassendes Sicherheits-, Kontinuitäts- und Risikomanagement mit System, a. a. O., S. 95.

69 Vgl. Witt, Bernhard C.: Rechtliche Anforderungen an die Informations-Sicherheit, in: <kes> Die Zeitschrift für Informations-Sicherheit, 1/2006, S. 95.

70 Die folgenden Ausführungen beziehen sich auf das Bundesdatenschutzgesetz (BDSG) vom 14.01.2003, BGBl. I S. 66, zuletzt geändert durch das Gesetz vom 22.08.2006, BGBl. I S. 1970.

71 Vgl. Faust, Harald: Datenschutz und Arbeitsplatzrechner, Oldenburg: Oldenbourg Verlag 1991, S. 14.

Maßnahme	Beschreibung	Betroffene Schutzziele
Zutritts-kontrolle	Unbefugte sollen physisch keinen Zutritt zu IT-Systemen haben. Die entsprechenden Räumlichkeiten sind also gegen unbefugtes Eindringen zu sichern.	Vertraulichkeit
Zugangs-kontrolle	Unbefugte dürfen die IT-Systeme nicht nutzen können.	Vertraulichkeit
Zugriffs-kontrolle	Die Nutzer der IT-Systeme sollen jeweils nur im Rahmen ihrer Zugriffsberechtigungen auf die Daten zugreifen können, die sie zur Erledigung ihrer Aufgaben benötigen.	Vertraulichkeit
Weitergabe-kontrolle	Bei der elektronischen Übertragung oder der Speicherung der Daten soll verhindert werden, dass Unbefugte die Daten zur Kenntnis nehmen oder verändern können.	Integrität, Vertraulichkeit
Eingabe-kontrolle	Es soll nachträglich, z. B. anhand eines Protokolls, festgestellt werden können, ob und von wem personenbezogene Daten in IT-Systeme eingegeben, verändert oder entfernt worden sind.	Integrität, Verbindlichkeit
Auftrags-kontrolle	Im Auftrag zu verarbeitende Daten sind nur entsprechend den Weisungen des Auftraggebers zu verarbeiten.	Vertraulichkeit
Verfügbar-keitskontrolle	Die Daten sollen gegen Zerstörung und Verlust geschützt sein.	Verfügbarkeit
Trennungs-gebot	Daten die zu unterschiedlichen Zwecken erhoben werden, sollen auch nur getrennt verarbeitet werden können. Dies erfordert jedoch keine räumliche Trennung der Datenbestände und dieses Gebot greift nicht, wenn eine Zusammenführung der Daten vorgesehen ist.	Vertraulichkeit

Tab. 1: Maßnahmen gemäß der Anlage zu § 9 BDSG[72]

Zwar werden im Rahmen dieser Anforderungen alle Schutzziele erfasst, der Fokus liegt beim BDSG jedoch auf der Vertraulichkeit. Ab einer gewissen Größe sind Unternehmen nach § 4 f BDSG verpflichtet, einen Datenschutzbeauftragten mit umfassendem Kontrollrecht zur Einhaltung der Datenschutzbestimmungen zu bestimmen. Zusätzlich kontrolliert eine Aufsichtsbehörde die Ausführung des BDSG und kann gemäß § 38 Abs. 5 BDSG bei gravierenden Missständen sogar die Datenverarbeitung untersagen.[73]

72 Vgl. Gola, Peter; Schomerus, Rudolf: Bundesdatenschutzgesetz – Kommentar, 7. völlig neu bearbeitete Auflage, München: C.H. Beck 2002, S. 316 ff.

73 Vgl. Witt, Bernhard C.: IT-Sicherheit kompakt und verständlich, a. a. O., S. 8.

Nach § 43 BDSG kann eine Nichtbeachtung zu Geldbußen bis zu 250.000 Euro führen, laut § 44 BDSG sogar mit Freiheitsstrafe bis zu zwei Jahren geahndet werden.

Die Europäische Union hat den Datenschutz ebenfalls in der EU-Datenschutzrichtlinie von 1995 thematisiert. Insbesondere für die Weitergabe personenbezogener Daten in Nicht-EU-Länder sind Maßnahmen zur Gewährleistung der Vertraulichkeit zu treffen.[74]

3.5.2 Fernmeldegeheimnis

Der Datenschutz ist eng mit der Gewährleistung des Fernmeldegeheimnisses nach Art. 10 Abs. 1 GG verknüpft. In vielen Unternehmen ist die private Nutzung elektronischer Kommunikationsmedien gestattet und der Arbeitgeber wird dadurch zum Teledienste-anbieter und Provider. Die Vorschriften des Telekommunikationsgesetzes (TKG), des Teledienstegesetzes (TDG) und des TDDSG müssen in diesem Fall neben dem BDSG beachtet werden. Insbesondere hat das Unternehmen die nach § 4 TDDSG[75] erforderlichen technischen und organisatorischen Vorkehrungen zu treffen, die auch Anforderungen hinsichtlich der IT-Sicherheitsschutzziele beinhalten. Der Betrieb von Telekommunikationsanlagen verpflichtet Unternehmen laut den §§ 100 Abs. 1 und 107 Abs. 2 TKG[76] zu geeigneten Maßnahmen zur Vermeidung von Störungen, Fehlübermittlungen und unbefugtem Offenbaren. Dies betrifft die Verfügbarkeit, die Vertraulichkeit und die Integrität. Zwar bestimmt das Unternehmen über den Einsatz seiner Arbeitsmittel und kann zur Kostenkontrolle die Nutzung überwachen, dennoch ist eine vollständige Überwachung und Aufzeichnung nicht zulässig. Das Unternehmen darf virenverseuchte E-Mails unter Rückgriff auf § 109 Abs. 1 Nr. 2 TKG aber ausfiltern.[77]

Ebenso wie beim BDSG werden hier alle IT-Sicherheitsschutzziele berührt, das Ziel der Vertraulichkeit steht aber im Mittelpunkt.

3.6 Sonstige branchenübergreifende Rechtsnormen

Als weitere Rechtsnormen zur IT-Sicherheit sind u. a. das Wertpapierhandelsgesetz, das Urheberrechtsgesetz, das Patentgesetz, das Markengesetz, das Arbeitsschutz- sowie das Arbeitssicherheitsgesetz, die Brandschutzordnung und berufsgenossenschaftliche Vorschriften zu nennen. Diese sollen an dieser Stelle jedoch nicht weiter untersucht werden.

74 Vgl. Müller, Klaus-Rainer: Handbuch Unternehmenssicherheit - umfassendes Sicherheits-, Kontinuitäts- und Risikomanagement mit System, a. a. O., S. 95.

75 Die folgenden Ausführungen beziehen sich auf das TDDSG vom 22.07.1997, BGBl. I, S. 1870, geändert durch das Elektronische Geschäftsverkehr-Gesetz (EGG) vom 14.12.2001, BGBl. I, S. 3721.

76 Die folgenden Ausführungen beziehen sich auf das TDG vom 22.07.1997, BGBl. I, S. 1870, geändert durch das Elektronische Geschäftsverkehr-Gesetz (EGG) vom 14.12.2001, BGBl. I, S. 3721.

77 Vgl. Witt, Bernhard C.: IT-Sicherheit kompakt und verständlich, a. a. O., S. 10.

4 Zusammenfassende Darstellung und Fazit

Ziel dieser Arbeit war es, einen Überblick über die branchenübergreifenden Rechtsnormen zu liefern, die für die ITS relevant sind. Es wurde gezeigt, dass insbesondere in den Bereichen Risikomanagement, Buchführung und Datenschutz IT-Sicherheitsmaßnahmen erforderlich bzw. gesetzlich vorgeschrieben sind.

Die dort vorhandenen einzelnen Vorschriften weisen deutliche Überschneidungen auf. Dies gilt im Besonderen für die Buchführung, wo die GoB durch die GoBS konkretisiert werden, welche wiederum von den GDPdU aufgegriffen werden. Das IDW nimmt auf alle genannten Grundsätze Bezug. Auch beim Datenschutz und beim Risikomanagement sind die Anforderungen der einzelnen Rechtsnormen teilweise redundant.

Zwischen den drei Bereichen ergeben sich ebenfalls Überschneidungen, da jeweils die genannten Schutzziele – zumindest implizit – vollständig abgedeckt werden. Da dies für Buchführung und Datenschutz am deutlichsten erkennbar ist, sollen hier beispielhaft einige Überschneidungen genannt werden. Dazu gehören die Forderungen nach einem Datensicherheitskonzept, nach Zugriffs-, Zutritts- und Zugangsschutz, sowie nach Erfassungskontrollen.

Allerdings werden in den Bereichen jeweils bestimmte Schutzziele priorisiert. So steht beim Datenschutz eher die Vertraulichkeit, im Bereich der Buchführung die Verfügbarkeit, Integrität und Verbindlichkeit eher im Fokus. So wird z. B. für den Schutz personenbezogener Daten ggf. ein umfassenderer Vertraulichkeitsschutz nötig sein. Die Pflicht zum Risikomanagement erfordert nur implizit die Einhaltung der Schutzziele zur Senkung des IT-Risikos sowie des rechtlichen Risikos. Infolgedessen hängt die Priorität vom jeweiligen Unternehmen ab. Es kommt darauf an, bei welchem Schutzziel der größte Schaden entstehen könnte, wenn es beeinträchtigt würde.

Die Redundanzen ermöglichen es den Unternehmen häufig, sich jeweils auf die strengsten für das jeweilige IT-System geltenden Anforderungen zu konzentrieren und damit auch die übrigen Rechtsnormen zu erfüllen. Werden in einem IT-System z. B. personenbezogene Daten verarbeitet und gleichzeitig steuerrelevante Daten erzeugt, so kann man sich in vielen Fällen bezüglich der Vertraulichkeit an den Datenschutzanforderungen, bezüglich der Verfügbarkeit an den Buchführungsanforderungen orientieren.

In den untersuchten Rechtsnormen dominieren allgemeine Formulierungen gegenüber konkreten Pflichtmaßnahmen. Zwar wird es dadurch möglich, Bedrohungen unabhängig von der jeweiligen technischen Ausgestaltung – und damit unabhängig von der rasanten technischen Entwicklung – zu erfassen, jedoch ergibt sich auch ein Auslegungsspiel-

raum für die Kontrollinstanzen.[78] Dies erhöht die Unsicherheit bezüglich der Gesetzeskonformität der konkreten Maßnahmenausgestaltung.

Es zeigt sich, dass sich die Unternehmen einer unüberschaubaren Vielzahl rechtlicher Anforderungen gegenüber sehen. Die Unternehmensleitung ist persönlich haftbar für die Einhaltung der oben genannten Rechtsnormen. Auch den einzelnen Mitarbeiter treffen im Einzelfall Haftungsrisiken.[79] Dadurch wird eine gewisse Sensibilisierung für ITS vom Gesetzgeber erzwungen. Letztlich lässt sich ITS nicht durch bessere, konkretere Gesetze erreichen, sondern nur dadurch, dass die Unternehmen selbst erkennen, wie erfolgskritisch sie ist. Es ist insbesondere erforderlich, dass sich die Unternehmensleitung für ITS einsetzt. Nur sie kann die Einführung eines IT-Sicherheitsprozesses anstoßen und die erforderlichen Ressourcen bereitstellen. Aber auch innerhalb des Unternehmens haben Sicherheitsrichtlinien und Handlungsanweisungen nur dann einen Sinn, wenn Sie von den Mitarbeitern auch verinnerlicht werden, denn das längste Passwort ist nicht sicher, wenn es nicht geheim gehalten wird. Ein ausgeprägtes Sicherheitsbewusstsein in den Unternehmen ist wegen der oben dargestellten zunehmenden Relevanz der IT-Sicherheit besonders wichtig.

78 Vgl. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Gutachten zur rechtlichen Analyse des Regelungsumfangs zur IT-Sicherheit in kritischen Infrastrukturen, a. a. O., S. xiv.

79 Vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) (Hrsg.): Matrix der Haftungsrisiken – IT-Sicherheit – Pflichten und Risiken, a. a. O., S. 4 ff.

Literaturverzeichnis

1. **Abgabenordnung** in der Fassung der Bekanntmachung vom 1. Oktober 2002, BGBl. I S. 3866; 2003 I S. 61, zuletzt geändert durch Artikel 10 des Gesetzes vom 13. Dezember 2006, BGBl. I S. 2878.
2. **Aktiengesetz (AktG)** vom 6. September 1965, BGBl. I S. 1089, zuletzt geändert durch Artikel 13 des Gesetzes vom 5. Januar 2007, BGBl. I S. 10.
3. **Anduleit, Manfred:** Datenarchivierung - ganz nach Vorschrift, erschienen in: Computerwoche, 01.02.2007, Online im Internet: http://www.computerwoche.de/it_strategien/it_management/586945/, 15.02.2007.
4. **Bittner, Kaus:** Grundsätze ordungsmäßiger DV-gestützter Buchführungssysteme (GoBS), in: Buchführung, Bilanzierung, Kostenrechnung (BBK), Nr. 24 vom 20.12.1995, S. 989 – 998.
5. **Bundesamt für Sicherheit in der Informationstechnik (Hrsg.):** Gutachten zur rechtlichen Analyse des Regelungsumfangs zur IT-Sicherheit in kritischen Infrastrukturen, Online im Internet: http://www.bsi.bund.de/fachthem/kritis/Regelungsumfang_ITSich_KRITIS.pdf, 05.05.2005.
6. **Bundesamt für Sicherheit in der Informationstechnik (Hrsg.):** IT-Grundschutz – Basis für IT-Sicherheit, Online im Internet: http://www.bsi.de/gshb/deutsch/baust/01001.htm, 26.4.2006.
7. **Bundesamt für Sicherheit in der Informationstechnik (Hrsg.):** IT-Grundschutz-Kataloge - Glossar: Stand 2006, Online im Internet: http://www.bsi.de/gshb/deutsch/baust/04.htm, 21.04.2007.
8. **Bundesanstalt für Finanzdienstleistungsaufsicht (Hrsg.):** Rundschreiben 18/2005: Mindestanforderungen an das Risikomanagement, Online im Internet: http://www.bafin.de/rundschreiben/89_2005/051220.htm, 20.12.2005.
9. **Bundesdatenschutzgesetz (BDSG)** in der Fassung der Bekanntmachung vom 14.01.2003, BGBl. I S. 66, zuletzt geändert durch Artikel 1 des Gesetzes vom 22.08.2006, BGBl. I S. 1970.
10. **Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) (Hrsg.):** Matrix der Haftungsrisiken – IT-Sicherheit – Pflichten und Risiken, Online im Internet: http://www.bitkom.org/files/documents/BITKOM_Leitfaden_Matrix_der_Haftungsrisiken-V1.1f.pdf, 27.04.2007.
11. **Deutscher Bundestag (Hrsg.):** Entwurf eines Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), Bundestag-Drucksache 13/9712, Anlage 1.
12. **Eckert, Claudia:** IT-Sicherheit, München; Wien: Oldenbourg Verlag 2006.
13. **Falk, Michael; Hofmann, Marc:** Integration des IT-Sicherheitsmanagements in das Risikomanagement im Kontext bankaufsichtsrechtlicher Vorgaben, in: Arbeitspapiere WI, Nr. 6/2006, Hrsg: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2006.

14. **Faust, Harald:** Datenschutz und Arbeitsplatzrechner, München: Oldenbourg Verlag 1991.

15. **Fischer, Norbert; Rotter, Norbert:** Sarbanes-Oxley Act und die Final Rule Section 404: Management Assessment of Internal Controls, in: USA-Mitteilungen Oktober 2003, Hrsg.: KPMG Deutsche Treuhand-Gesellschaft Aktiengesellschaft Wirtschaftsprüfungsgesellschaft, Online im Internet: http://www.kpmg.de/library/pdf/031014_USA_Mitteilungen_Oktober2003_de.pdf, 24.04.2007.

16. **Gesetz betreffend die Gesellschaften mit beschränkter Haftung (GmbHG)** in der im Bundesgesetzblatt Teil III, Gliederungsnummer 4123-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 10 des Gesetzes vom 10. November 2006, BGBl. I S. 2553.

17. **Gesetz über das Kreditwesen (Kreditwesengesetz - KWG)** in der Neufassung der Bekanntmachung vom 9. September 1998, BGBl. I S. 2776, zuletzt geändert durch Art. 8 des Gesetzes vom 5. Januar 2007, BGBl. I S. 10.

18. **Gesetz zur Einführung internationaler Rechnungslegungsstandards und zur Sicherung der Qualität der Abschlussprüfung (Bilanzrechtsreformgesetz – BilReG)** vom 9.12.2004, BGB1. I. Nr. 65, S. 3166 ff.

19. **Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KontraG)** vom 27.04.1998, BGB1. I Nr. 24, S. 786 ff.

20. **Gesetz zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts (UMAG)** vom 22.09.2005, BGB1. I Nr. 60, S. 2802 ff.

21. **Gola, Peter; Schomerus, Rudolf:** Bundesdatenschutzgesetz – Kommentar, 7. völlig neu bearbeitete Auflage, München: C.H. Beck 2002, S. 316 ff.

22. **Haiges, Ingo:** Aspekte der Daten- und Dokumentensicherheit - Verfügbar, lesbar, dennoch sicher, in: Beschaffung aktuell, 07.07.2005.

23. **Handelsgesetzbuch** in der im Bundesgesetzblatt Teil III, Gliederungsnummer 4100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 5 des Gesetzes vom 5. Januar 2007, BGBl. I S. 10.

24. **Harder, Bernd H.:** IT-Sicherheit: Haftungsrisiko für alle Führungskräfte, Online im Internet: http://www.harder-rechtsanwaelte.de/edv-recht/haftungsrisiko-bbb_0106.html, 24.04.2007.

25. **Heinrich, Robert; Lang, Franz-Josef:** DV und Recht/Risikobewertung und Frühwarnsysteme – Ein neues Gesetz macht die IT-Sicherheit zur Pflicht, in: Computerwoche, 24/1999.

26. **Henn, Martin:** Anforderungen an die Ordnungsmäßigkeit der EDV-Buchführung, in: Buchführung, Bilanzierung, Kostenrechnung (BBK), Nr. 4 vom 17.2.2006, S. 1185 – 1198.

27. **Hirschmann, Stefan; Romeike, Frank:** IT-Sicherheit als Rating-Faktor, in: RATINGaktuell, 01/2004.

28. **Hofmann, Kathrin:** Dokumente rechtssicher speichern, in: IT-Business News, 26.02.2007.

29. **Institut der Wirtschaftsprüfer (Hrsg.):** Die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB (IDW PS 340), in: WPg 1999, Heft-Nr. 16/1999, S. 658 ff.

30. **Institut der Wirtschaftsprüfer (Hrsg.):** IDW-Prüfungsstandard: Abschlussprüfung bei Einsatz von Informationstechnologie (IDW PS 330), WPg 2002, Heft Nr. 21/2002, S. 1167 ff.

31. **Institut der Wirtschaftsprüfer (Hrsg.):** IDW-Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1), WPg 2002, Heft-Nr. 21/2002, S. 1157.

32. **Krystek, Ulrich; Fiege, Stefanie:** Risikomanagement, in: Gabler Wirtschaftslexikon, 16. vollständig aktualisierte und überarbeitete Auflage, Wiesbaden: Gabler 2004, S. 2558.

33. **Müller, Klaus-Rainer:** Handbuch Unternehmenssicherheit - umfassendes Sicherheits-, Kontinuitäts- und Risikomanagement mit System, 1. Auflage, Wiesbaden: Vieweg Verlag 2005.

34. **o. V.:** Barings Debacle, Online im Internet: http://www.riskglossary.com/link/barings_debacle .htm, 01.05.2006

35. **o. V.:** Grundsätze ordungsmäßiger DV-gestützter Buchführungssysteme (GoBS) vom 07.11.1995, Online im Internet: http://www.elektronische-steuerpruefung.de/rechtsgrund/gobs.pdf, 23.04.2007.

36. **o. V.:** Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), Online im Internet: http://www.aufbewahrungspflicht.de/pdfs/gdpdu.pdf, 16.07.2001.

37. **Pollanz, Manfred:** Offene Fragen der Prüfung von Risikomanagementsystemen nach KonTraG , in: Der Betrieb, Heft 25 vom 22.6.2001, S. 1317 ff.

38. **Romeike, Frank; Müller-Reichart, Matthias; Hein, Thorsten:** Die Assekuranz am Scheideweg - Ergebnisse der ersten Benchmark-Studie zu Solvency II, in: Zeitschrift für Versicherungswesen, 10/2006, S. 316 – 321.

39. **Schaumüller-Bichl, Ingrid:** Sicherheitsmanagement: Risikobewältigung in informationstechnologischen Systemen, Mannheim; Leipzig; Wien; Zürich: BI-Wissenschaftsverlag 1992.

40. **Schmidt, Klaus:** Der IT Security Manager, München: Hanser Verlag 2006.

41. **Signaturgesetz** vom 16.02.2001, BGBl. I S. 876, zuletzt geändert durch Artikel 4 des Gesetzes vom 26.02.2007, BGBl. I S. 179.

42. **TDDSG** vom 22.07.1997, BGBl. I, S. 1870, zuletzt geändert durch Artikel 1 des Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz - EGG) vom 14.12.2001, BGBl. I, S. 3721.

43. **TDG** vom 22.07.1997, BGBl. I, S. 1870, zuletzt geändert durch Artikel 1 des Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz - EGG) vom 14.12.2001, BGBl. I, S. 3721.

44. **Umsatzsteuergesetz** in der Fassung der Bekanntmachung vom 21.02.2005, BGBl. I S. 386, zuletzt geändert durch Artikel 7 des Gesetzes vom 13.12.2006, BGBl. I S. 2878.

45. **Wirz, Erik:** Vorschriften und Lösungsansätze - Langzeitarchivierung digitaler Daten, Online im Internet: http://www.lanline.de/article.html?thes=&art=/ articles/2005008/30451905_ha_LL.html, 01.09.2005.

46. **Witt, Bernhard C.:** Rechtliche Anforderungen an die Informations-Sicherheit, in: <kes> Die Zeitschrift für Informations-Sicherheit, 1/2006, S. 92 ff.

47. **Witt, Bernhard C.:** IT-Sicherheit kompakt und verständlich, Neu-Ulm: Vieweg Verlag 2006.

48. **Wöhe, Günther:** Einführung in die Allgemeine Betriebswirtschaftslehre, München: Verlag Vahlen 2002.

Impressum

Reihe: **Arbeitspapiere Wirtschaftsinformatik** (ISSN 1613-6667)

Bezug: http://wiwi.uni-giessen.de/home/Schwickert/arbeitspapiere/

Herausgeber: Prof. Dr. Axel C. Schwickert
Prof. Dr. Bernhard Ostheimer

c/o Professur BWL – Wirtschaftsinformatik
Justus-Liebig-Universität Gießen
Fachbereich Wirtschaftswissenschaften
Licher Straße 70
D – 35394 Gießen
Telefon (0 64 1) 99-22611
Telefax (0 64 1) 99-22619
eMail: Axel.Schwickert@wirtschaft.uni-giessen.de
http://wi.uni-giessen.de

Ziele: Die Arbeitspapiere dieser Reihe sollen konsistente Überblicke zu den Grundlagen der Wirtschaftsinformatik geben und sich mit speziellen Themenbereichen tiefergehend befassen. Ziel ist die verständliche Vermittlung theoretischer Grundlagen und deren Transfer in praxisorientiertes Wissen.

Zielgruppen: Als Zielgruppen sehen wir Forschende, Lehrende und Lernende in der Disziplin Wirtschaftsinformatik sowie das IT-Management und Praktiker in Unternehmen.

Quellen: Die Arbeitspapiere entstehen aus Forschungsarbeiten, Abschluss-, Studien- und Projektarbeiten sowie Begleitmaterialien zu Lehr- und Vortragsveranstaltungen der Professur BWL – Wirtschaftsinformatik, Univ. Prof. Dr. Axel C. Schwickert, Justus-Liebig-Universität Gießen sowie der Professur für Wirtschaftsinformatik, insbes. medienorientierte Wirtschaftsinformatik, Fachbereich Wirtschaft, Hochschule Mainz.

Hinweise: Wir nehmen Ihre Anregungen und Kritik zu den Arbeitspapieren aufmerksam zur Kenntnis und werden uns auf Wunsch mit Ihnen in Verbindung setzen.

Falls Sie selbst ein Arbeitspapier in der Reihe veröffentlichen möchten, nehmen Sie bitte mit dem Herausgeber unter obiger Adresse Kontakt auf.

Informationen über die bisher erschienenen Arbeitspapiere dieser Reihe erhalten Sie unter der Adresse http://wi.uni-giessen.de.