Dr. Florian Deusch

Rechtsanwalt und Fachanwalt für IT-Recht

IT – COMPLIANCE in der PRAXIS

Haftungsrisiken und Organisationspflichten im Unternehmen

Wann führen Mängel der IT-Compliance zur persönlichen Haftung im Unternehmen? Welche Maßnahmen sind notwendig, damit die Informationstechnologie (kurz: IT) im Unternehmen effizient genutzt wird und die erforderliche Kontrolle durch die Unternehmensleitung gewährleistet ist?
Die Vorteile der modernen IT sind aus dem Unternehmensalltag nicht mehr wegzudenken.[1] Weniger bekannt sind dagegen die Sorgfaltsanforderungen, die der IT-Einsatz für das Unternehmen und die Personen der Unternehmensleitung mit sich bringen.

Der nachfolgende Beitrag verschafft einen Überblick über grundlegende Anforderungen zur Betriebsorganisation und zur Haftungsvermeidung beim IT-Einsatz im Unternehmen. Zunächst wird dargestellt, in welchem Umfang IT in Unternehmen eingesetzt wird und welche Gefahren hierbei bestehen können (Abschnitt 1). Anschließend werden die rechtlichen Grundlagen der IT-Compliance behandelt und die Haftungsrisiken aufgezeigt, die sich für die Personen der Unternehmensleitung stellen, insbesondere für Vorstände, Geschäftsführer, Aufsichtsräte, Beiräte und Arbeitnehmer mit besonderen Funktionen im Unternehmen (Abschnitt 2). Schließlich werden konkrete Maßnahmen unternehmerischer IT-Compliance anhand exemplarischer Praxisfälle behandelt (Abschnitt 3) und die Erkenntnisse hieraus zusammengefasst (siehe Abschnitt 4).

[1] Bill Gates sieht die IT und den Berufsalltag als „untrennbar miteinander verbunden“ an: „Information technology and business are becoming inextricably interwoven. I don't think anybody can talk meaningfully about one without the talking about the other.“ Zitat entnommen aus http://www.billgatesmicrosoft.com/ 22.08.2011.

Inhaltsverzeichnis Seite

1. Einsatz und Gefahren der IT im Unternehmen

1.1 Motive und Arten des unternehmerischen IT-Einsatzes

Hauptgründe für den IT-Einsatz in Unternehmen sind die Erhaltung der Wettbewerbsfähigkeit und die Steigerung der Effizienz.[2] Die Grundkomponenten eines IT-Systems sind Hardware und Software. Als Hardware werden die physikalischen Bestandteile eines Computersystems bezeichnet sowie alle peripheren Einrichtungen wie Monitor, Drucker, Tastatur und alle Geräte zur Kommunikation und Speicherung. Software dagegen erfasst die Gesamtheit aller Computerprogramme und Daten, die auf einem Computer eingesetzt bzw. gespeichert werden können.[3]

1.1.1 Hardware

Rund 85 % aller deutschen Unternehmen setzen Computer zur Bewältigung ihrer Aufgaben ein; in Unternehmen mit mehr als 10 Beschäftigten sind dies sogar 97 %.[4] Der Hardware-Einsatz erfasst Serverrechner[5], die Netzwerke steuern und Arbeitsplatzrechner, die in Netze integriert sind; eingesetzt werden weiter externe und interne Speicher, Universal-Serial-Bus-(USB)-Sticks, Laptops, Netbooks, Smartphones[6] und Multifunktionsgeräte, die verschiedene Funktionen ausführen können (zum Beispiel drucken, scannen, kopieren, faxen usw.).[7] Europaweit arbeiten 51 % aller Beschäftigten am PC; in Deutschland sind dies sogar 61 %.[8] Im Jahr 2010 waren ca. 26,5 Mio. Arbeitsplatzcomputer in den deutschen Unternehmen im Einsatz. Die Hälfte hiervon waren Desktop-PCs, gefolgt von Notebooks (41%), Thin Clients (8%) und Mini-PCs (1%). Bis zum Jahr 2020 wird mit bis zu 37,5 Mio. Arbeitsplatzcomputern in Deutschland gerechnet.[9] Erwartet wird die Verstärkung des Trends, mehr und mehr neuartige und mobile Endgeräte einzusetzen wie zum Beispiel Laptops, Tablet-PCs und Mobilfunktelefone. Dementsprechend wurden im Jahr 2010 weltweit ca. 80 Mio. Smartphones verkauft.[10] Für die IT-Compliance ist beim Hardware-Einsatz unter anderem der physische Schutz der Systeme und deren ordnungsgemäßer Einsatz relevant.

1.1.2 Softwareeinsatz

Sogenannte Systemsoftware dient dazu, der Hardware die Befehle für die erforderlichen Rechenarbeiten zu erteilen. Daneben werden sogenannte Anwendungsprogramme eingesetzt, die jeweils konkret definierte Aufgaben lösen. Anwendungsprogramme betreffen sowohl herkömmliche Textverarbeitung und Tabellenkalkulation (zum Beispiel Word und Excel), aber auch komplexere Software wie zum Beispiel Programme zum Enter-

[2] BSI-Lagebericht 2009, Seite 13.
[3] Kilian / Heussen, Computerrechtshandbuch, Kapitel 300, Stichworte Hard- und Software; Lehmann / Meents, Handbuch FA IT-Recht, Kapitel 1 Rn 3.
[4] Destatis, IKT in Unternehmen, S. 10.
[5] Ein Server ist ein Zentralrechner, der in einem Computersystem Dienste und / oder Ressourcen zur Verfügung stellt (Kilian / Heussen, Computerrechtshandbuch, Kapitel 300, Stichwort „Server“).
[6] Ein Smartphone ist ein Mobiltelefon mit besonders leistungsfähigem Prozessor, welcher den Funktionsumfang eines Mobiltelefons entsprechend erweitert.
[7] Lehmann / Meents, Handbuch FA IT-Recht, Kapitel 1 Rn 2 ff.
[8] BITKOM-Pressemeldung „Computerausstattung in Unternehmen“, www.bitkom.org/de/markt_statistik/64050_38546.aspx 10.08.2011.
[9] Fichter / Clausen / Hintermann, Roadmap „Ressourceneffiziente Arbeitsplatz-Computerlösungen“, Seiten 3 f.
[10] Hogben / Dekker, ENISA Quarterly Review Vol. 6. No. 4, December 2010, p.8.

prise Ressource-Planning (ERP) und zum Customer Relationship Managment (CRM).[11]
ERP-Programme wurden im Jahr 2010 von ca. 32 % aller Unternehmen in Deutschland eingesetzt; hierbei handelt es sich um Software, die zur Steuerung bestimmter Vorgänge im Unternehmen verwendet werden kann, um Ressourcen effizient zu nutzen. Unternehmen mit mehr als 50 Beschäftigte nutzen zu 51 % ERP-Software, ab 250 Beschäftigte sind es sogar 74 %.[12]
Sogenannte Customer-Relationship-Management-Programme dienen dazu, Bestellungen und sonstige Daten von Kunden im Unternehmen zentral, systematisch und effizient zu speichern und zu nutzen. Fast die Hälfte (46 %) aller Unternehmen in Deutschland mit mehr als 10 Mitarbeitern hat im Jahr 2010 solche Softwarelösungen eingesetzt.[13]
Zentrale Compliance-Themen bei der Softwarenutzung sind insbesondere ein striktes Lizenzmanagement, eine klare Definition der Zugriffsrechte und der Schutz des Datenbestands vor Verlust und Manipulation.

1.1.3 Virtualisierung und Vernetzung von Systemen

Neben den klassischen Softwarefunktionen der Betriebs- und Anwendungssysteme werden mithilfe von Computerprogrammen vermehrt Hard- und Softwarefunktionen virtualisiert. Bei der Hardwarevirtualisierung wird auf einem physisch vorhandenen Server mithilfe von Software ein zweiter Server simuliert und virtuell genutzt. Auf diese Weise können die Ressourcen eines IT-Systems effizienter ausgenutzt werden.[14]
Vermehrt wird aber auch Softwarevirtualisierung betrieben; hierbei werden die einzelnen Softwareanwendungen durch eine Abstraktionsschicht im Rechner voneinander getrennt. Diese Technik beugt unter anderem möglichen Problemen bei der technischen Verträglichkeit mehrerer Anwendungsprogramme vor. Der Hard- bzw. Softwarevirtualisierung wurden im Zeitraum 2008 bis 2012 Wachstumspotentiale bis zu 22% (Hardware) bzw. sogar 36 % (Software) bescheinigt.[15]
Das Phänomen der Virtualisierung löst die klassische Trennung zwischen Hard- und Software zunehmend auf. Teilweise werden Hard- und Software-Ressourcen mithilfe der Virtualisierungstechnik bedarfsorientiert auch von externen Servern als internetbasierte Dienste unter den Stichworten „Cloud Computing“ bzw. „Software as a Service“ bezogen.[16]
Wenn mehrere Computer miteinander verbunden („vernetzt“) sind, können sie je nach Konfiguration der Zugriffsrechte auf die Daten und Anwendungen der anderen vernetzten Computer zugreifen. Dies steigert die Effizienz des IT-Einsatzes. 83 % aller deutschen Unternehmen mit mehr als 10 Mitarbeitern haben ihre Computer betriebsintern miteinander vernetzt. In 48% der betriebsintern vernetzten Unternehmen werden drahtlose Netze eingesetzt.[17]
Der vermehrte Einsatz mobiler Endgeräte und die zunehmende Vernetzung der IT-Systeme führen dazu, dass die Grenzen zwischen Arbeits- und Privatleben zunehmend verschwimmen. Neun von zehn Berufstätige sind außerhalb ihrer Arbeitszeit für Vorgesetzte, Kollegen und Kunden (insbesondere per E-Mail) erreichbar; mehr als ein Drittel der Handybesitzer nutzt sein privates Mobiltelefon auch zu beruflichen Zwecken. Andererseits nutzt fast die Hälfte aller Beschäftigten in Deutschland den Internet-Zugang im Unternehmen auch zu privaten Zwecken; hauptsächlich zum Abruf eingegangener E-Mails.[18]
Die Virtualisierung und Vernetzung der IT wirft für die Compliance vor allem Probleme bei der System-Verfügbarkeit und beim Datenschutz auf.

1.2 Gefahren des IT-Einsatzes

Risiken beim IT-Einsatz ergeben sich, wenn die Funktionsfähigkeit der Systeme angegriffen bzw. nicht gewährleistet wird. Zentrale Elemente der IT-Sicherheit sind hierbei die Verfügbarkeit, Unversehrtheit und Vertraulichkeit der IT-Systeme (siehe auch § 2 Absatz (2) BSIG[19]). Hierbei wächst das Gefahrenpotential für die Unternehmen mit ihrer fortschreitenden Technisierung. Da der IT-Einsatz in Wechselwirkung mit zahlreichen anderweitigen Vorgängen im Unternehmen steht, ist die Abhängigkeit von einer reibungslosen IT-Nutzung nicht zu unterschätzen.[20]
Bedrohungen für IT-Systeme ergeben sich vor allem aus sogenannten Schadprogrammen (Malware). Dies sind gemäß § 2 Absatz (5) BSIG Computerprogramme, die unbefugt Daten nutzen, löschen oder in sonstiger Weise unbefugt auf informationstechnische Abläufe einwirken. Arten von Schadprogrammen sind zum Beispiel folgende:[21]

- Computerviren sind solche Programme, die sich selbst vermehren. Im Gegensatz zu einem Wurm setzt die Funktion eines Computervirus erst ein, wenn das Programm den Befehl zur Ausführung erhalten hat. Meist führen Computerviren gleichzeitig Schadfunktionen anderer Malware-Arten aus.
- Würmer nutzen die vorhandene Netzwerkinfrastruktur des befallenen Rechners (zum Beispiel E-Mail-Dienste), um sich selbständig zu verbreiten. Sie belasten damit die Ressourcen

[11] Lehmann / Meents, Handbuch FA IT-Recht, Kapitel 1 Rn 16.
[12] Destatis, IKT in Unternehmen, Seite 29.
[13] Destatis, IKT in Unternehmen, Seite 30; Rapp, Customer Relationship Management, Seiten 40 ff.
[14] Grützmacher, ITRB 2011, 193.
[15] Runge / Sturm / Wisskirchen / Ebel / Groh / Höller / Mewes, VMware Infrastructure, S. 50, 63; Groll, Lizenzmanagement, Seite 272 f.
[16] Buxmann / Lehmann / Draisbach / Koll / Diefenbach / Ackermann: Cloud Computing und Software as a Service in: Leible / Sosnitza (Hrsg.): Onlinerecht 2.0: Alte Fragen - neue Antworten, Seite 22; Backu, ITRB 2011, 184; Bierekoven, ITRB 2010, 42.
[17] Destatis, ITK in Unternehmen, Seiten 12 f.
[18] BITKOM, Netzgesellschaft, Seiten 46 ff.
[19] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik.
[20] Schmidl in: Hauschka, Corporate Compliance, § 29 Rn 1; ders., NJW 2010, 477; BSI Leitfaden Informationssicherheit, Seite 11; Keitsch, Risikomanagement, Seiten 119 ff.
[21] Spindler, Verantwortlichkeit von IT-Herstellern, Nutzern und Intermediären, Seite 28 f.

eines IT-Systems. Wenn sie gleichzeitig andere Schadfunktionen ausführen, werden diese über das angegriffene IT-System durch den Wurm verbreitet.
- Trojaner sind Programme, die mit nützlichen Funktionen getarnt sind, aber gleichzeitig ohne Wissen des Anwenders schädliche Aktionen ausführen.
- Als Spyware werden Programme bezeichnet, die ohne Wissen des Benutzers Informationen über das IT-System des Opfers sammeln (zum Beispiel Anmeldedaten oder Passwörter) und an Dritte weitergeben. Die gestohlenen Daten werden in sogenannten „Dropzones“[22] zum Verkauf angeboten.[23]

Meist sind in einem Schadprogramm mehrere Schadfunktionen kombiniert.[24]

Nach den Erhebungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) nimmt die Anzahl der Schadprogramme weiter zu: alle ein bis zwei Sekunden entsteht ein neues Schadprogramm. Zudem setzen die kriminellen Täter Schadprogramme gezielter und individueller ein als noch vor einigen Jahren. Sogenannte Exploit-Kits (Baukästen für Schadprogramme) können im Internet von jedermann erworben und eingesetzt werden.[25] Folgende Ursachen und Zusammenhänge sind für die Verbreitung von Schadprogrammen insbesondere relevant:

- Sicherheitslücken und fehlende Updates
  Schadsoftware nutzt Sicherheitslücken und Schwachstellen in Standardprogrammen (Betriebssysteme und Anwendungssoftware), um Datenmanipulationen vorzunehmen. Aus diesem Grund veröffentlichen die Softwarehersteller in regelmäßigen Abständen kostenlose Updates, die die Sicherheitslücken schließen. Daher stellt es ein IT-Sicherheitsrisiko dar, wenn die Installation der jeweils aktuellen Sicherheitsupdates im Unternehmen nicht systematisch geregelt ist.[26]

- Mangelhafte Systemkonfiguration und fehlende Sicherheitskonzepte
  Oftmals sind vorhandene Sicherheitsfunktionen der Standardprogramme in IT-Systemen nicht aktiviert. Zudem stellt es ein Sicherheitsrisiko dar, wenn die Zugriffsrechte auf das IT-System nicht systematisch vergeben werden, sondern wenn allen Nutzern das gesamte IT-System mit allen Funktionen und Installationsmöglichkeiten offen steht.[27]
  Insbesondere beim Einsatz mobiler Endgeräte (Smartphones, Laptops, Netbooks usw.) ergeben sich bei einem fehlenden Sicherheitskonzept erhebliche Risiken. Erhebungen zufolge gehen mehr als 40 % aller Schadensfälle im Bereich IT-Sicherheit auf den Diebstahl mobiler Endgeräte zurück. Ohne den Schutz des Geräts durch entsprechende Sicherheitsmaßnahmen hat der Dieb eines gestohlenen Geräts leichtes Spiel, an unternehmensinterne Daten auf dem Gerät zu gelangen oder sich sogar in das unternehmensinterne Netzwerk einzuloggen. Zudem sind auf zahlreichen mobilen Geräten weder aktuelle Sicherheitsupdates noch entsprechende Programme zum Schutz vor Malware installiert.[28]

- Drive-by-Downloads und Zero-Day Exploits
  Als eine Hauptursache für die Verbreitung von Schadsoftware werden sogenannte Drive-by-Downloads bzw. Drive-by-Exploits angesehen. Wenn der Anwender eine mit Schadsoftware versehene Webseite betrachtet, wird dessen IT-System unbemerkt nach Sicherheitslücken gescannt und gegebenenfalls ohne dessen Wissen mit Schadsoftware infiziert. Besonders oft wurde festgestellt, dass Schwachstellen in webbasierter Software (beispielsweise Adobe, Java, Internet-Explorer usw.) ausgenutzt wurden, weil die längst vorhandenen Sicherheitsupdates nicht installiert waren. Von einem „Zero-Day-Exploit“ spricht man, wenn eine Sicherheitslücke in Standardprogrammen ausgenutzt wird, für die es noch kein Sicherheitsupdate des Herstellers gibt.[29]

- Botnetze, DDoS-Angriffe
  Bei einem Botnetz handelt es sich um eine Verbindung mehrerer Computer, die mit Schadsoftware infiziert sind und ohne Kenntnis der Computer-Nutzer von einem Angreifer ferngesteuert werden. Aufgrund der Vielzahl der Computer, die in einem Botnetz verfügbar sind, werden diese unter anderem für sogenannte DDoS[30]-Angriffe und für Spams missbraucht. Bei einem DDoS-Angriff übermitteln die in einem Botnetz verbundenen Computer an das angegriffene IT-System eine Vielzahl von Anfragen, um dessen Ressourcen zu überlasten und auf diese Weise einen Systemzusammenbruch herbeizuführen. Kriminelle bieten Botnetze im Internet frei zugänglich zur Miete an.[31]

- Spams und Social Engineering
  Zwar ist ein Rückgang der Anzahl an Spams (unerwünschte E-Mails) zu verzeichnen, die Zielgenauigkeit der Spams nimmt jedoch zu. Indem die Kriminellen beim sogenannten Social Engineering zunächst Kontakt mit dem Opfer aufnehmen oder ihre E-Mail so gestalten, dass sie für das konkrete Opfer scheinbar einen relevanten Inhalt aufweist, erhöht sich

[22] Das sind Server, auf denen die gestohlenen Daten gespeichert sind.
[23] BSI-Lagebericht 2011, Seite 22: Im Jahr 2010 wurden vom BSI ca. 86.000 Online-Banking-Daten in Dropzones gefunden.
[24] Spindler, Verantwortlichkeit von IT-Herstellern, Nutzern und Intermediären, Seite 34.
[25] Der Preis für ein Exploit-Kit beträgt zwischen US-Dollar 400 bis 2.000, BSI-Lagebericht 2011, Seiten 12, 25 ff.; ENISA Country Reports Overview Document, Seite 10.
[26] Spindler, Verantwortlichkeit von IT-Herstellern, Nutzern und Intermediären, Seite 35; BSI-Lagebericht 2011, Seiten 9 f.
[27] BSI Leitfaden IT-Sicherheit, Seite 24.
[28] Hogben / Dekkers, ENISA Quarterly Review Vol. 6. No. 4, December 2010, p.8.; BSI-Lagebericht 2011, Seite 27.
[29] BSI-Lagebericht 2011, Seiten 12 f.; Spindler, Verantwortlichkeit von IT-Herstellern, Nutzern und Intermediären, Seite 37.
[30] Distributed Denial of Service.
[31] https://www.botfrei.de/technik.html, 24.08.2011; Walter, Kompendium der Web-Programmierung, Seite 24; BSI-Lagebericht 2011, Seiten 14 ff.; Spindler, Verantwortlichkeit von IT-Herstellern, Nutzern und Intermediären, Seite 39.

das Risiko, dass Spams geöffnet und damit Schadprogramme installiert werden.[32]

Die polizeilichen Kriminalstatistiken des Bundesinnenministeriums und des Landeskriminalamts Baden-Württemberg haben im Jahr 2010 jeweils eine erhebliche Zunahme der Straftaten in den Bereichen Computerkriminalität und IuK-Kriminalität (Straftaten im Bereich der Informations- und Kommunikationstechnik) verzeichnet. In den Teilbereichen der Datenveränderung und der Computersabotage ist die Aufklärungsquote im Jahr 2010 im Vergleich zum Vorjahr um ca. 5 % gesunken; das strafbare Ausspähen und Abfangen von Daten hat um mehr als 32 % zugenommen.[33] Der durchschnittliche Schaden für Unternehmen bei Straftaten im Bereich der Informations- und Telekommunikationstechnologie hat im Jahr 2010 ca. € 300.000,00 betragen; gleichwohl hat ein Drittel der deutschen Mittelständler keine organisatorischen Maßnahmen zur IT-Sicherheit und zum Datenschutz getroffen. Ein formell geregeltes IT-Sicherheitskonzept haben lediglich 26,41 % aller europäischen Unternehmen.[34]

2. Rechtsgrundlagen der IT-Compliance im Unternehmen

Im Kontext der Organisation eines Unternehmens („Corporate Governance") wird unter dem Begriff Compliance die Einhaltung von gesetzlichen und selbst definierten Anforderungen verstanden.[35] Der Teilbereich der IT-Compliance betrifft die Übereinstimmung des IT-Einsatzes im Unternehmen mit den gesetzlichen und unternehmensintern festgelegten Regelungen.[36]
Nachfolgend werden zunächst die Rechtsgrundlagen der IT-Compliance dargestellt und im Anschluss die Haftungsrisiken für die verantwortlichen Personen für den Fall von Compliance-Verstößen.

2.1 IT-Compliance als Element der Unternehmensorganisation[37]

2.1.1 Pflicht zur Legalität und sorgfältigen Geschäftsführung

Gemäß den §§ 93 Absatz (1) Satz 1 AktG[38], 43 Absatz (1) GmbHG[39], 34 Absatz (1) Satz 1 GenG[40] sind Vorstände und Geschäftsführer von Kapitalgesellschaften verpflichtet, die Geschäfte der Gesellschaft mit der Sorgfalt eines ordentlichen Kaufmanns zu führen. Bei Geschäftsführern von Personengesellschaften ergibt sich diese Verpflichtung auch ohne ausdrückliche Regelung aus dem Gesellschaftsvertrag (gilt für Gesellschafter-Geschäftsführer) bzw. aus dem Geschäftsführer-Dienstverhältnis gemäß den §§ 611 ff. BGB (gilt für Fremdgeschäftsführer).[41] Von dieser Pflicht zur sorgfältigen Geschäftsführung ist – unabhängig von der Gesellschaftsform – auch die sogenannte „allgemeine Legalitätspflicht" erfasst: Gesetzesverstöße sind zu vermeiden und Schäden vom Unternehmen abzuwenden.[42] Diese Verpflichtung der Unternehmensleitung erstreckt sich auf alle Bereiche des Unternehmens und somit auch auf den Einsatz von IT. Daher besteht eine Verpflichtung der Unternehmensleitung, den IT-Einsatz so zu organisieren, dass Gesetze eingehalten und Schäden vermieden werden.[43]

Auch für Einzelunternehmer sind die Rechtsgrundsätze der IT-Compliance relevant. Zwar gilt für Einzelunternehmer weder das Aktien-, noch das GmbH- oder das Genossenschaftsgesetz; allerdings können IT-Compliance-Versäumnisse für jede juristische oder natürliche Person im Schadensfall Ansprüche gegen Schädiger und Versicherungen ausschließen oder einschränken. Wenn in einem Schadensfall zum Beispiel (Geschäfts-) Daten verloren gehen, stellt eine fehlende Datensicherung ein derart gravierendes Mitverschulden dar, dass ein Schadensersatzanspruch des geschädigten Unternehmens gegen den Schädiger gemäß § 254 BGB[44] vollständig oder zu einem erheblichen Anteil ausgeschlossen ist. Auch der Verlust des Versicherungsschutzes kann die Folge mangelnder IT-Compliance sein.[45]

[32] BSI Lageberichte 2011, Seite 18 und 2009, Seite 78.
[33] Polizeiliche Kriminalstatistik des Bundesinnenministeriums 2010, Seiten 7 f. (246.607 Fälle mit dem Tatmittel Internet; ca. 85.000 Fälle zur Computerkriminalität); Jahresbericht 2010 IuK-Kriminalität des Landeskriminalamts Baden-Württemberg 2010, Seite 3 (32.249 Fälle der IuK-Kriminalität in Baden-Württemberg).
[34] BITKOM-Pressemeldung vom 29.03.2011, http://www.bitkom.org/68897_67471.aspx 10.08.2011; ENISA Country Reports Overview Document, Seite 15.
[35] Hauschka, Corporate Compliance, § 1 Rn 2; ders., NJW 2004, 257; Küting, DB 2009, 1364; Passarge, DStR 2010, 1675; siehe auch Ziffer 2 IDW PS 980. Mit dem Grünbuch „Europäischer Corporate Governance-Rahmen" hat die Kommission der Europäischen Union im April 2011 Eckpunkte definiert, die für einen einheitlichen europäischen Rechtsrahmen ordnungsgemäßer Unternehmensorganisation gelten könnten, siehe hierzu Jung, BB 2011, 1987 ff.
[36] Rath / Sponholz, IT-Compliance, Seite 25; Schneider, Handbuch des EDV-Rechts, Kapitel B Rn 1; Junker / Knigge / Pischel / Reinhart in: Büchting / Heussen, Beck´sches Rechtsanwaltshandbuch, § 48 Rn 106; Lensdorf, CR 2007, 413, Taeger, NJW 2007, 3330; Lensdorf / Steger, ITRB 2006, 206.
[37] Branchenspezifische Vorgaben wie zum Beispiel die §§ 25 a Kreditwesengesetz, 33 Wertpapierhandelsgesetz (Bankbranche) bleiben unberücksichtigt.
[38] Aktiengesetz.
[39] Gesetz betreffend die Gesellschaften mit beschränkter Haftung.
[40] Gesetz betreffend die Erwerbs- und Wirtschaftsgenossenschaften.
[41] KG Berlin, Urteil vom 24.02.2011, 19 U 83/10, BeckRS 2011, 05510; Oetker / Weitemeyer, HGB § 114 Rn 23.
[42] BGHZ 133, 370; BGH DB 2002, 473; Scholz / Uwe H. Schneider, GmbHG, § 43 Rn 74; Rodewald / Unger, BB 2006, 113; Nolte, BB Special 5.2008, 23; Meier-Greve, BB 2009, 2555; Heldmann, DB 2010, 1235; Wytibul, BB 2009, 2591; Wiederholt / Walter, BB 2011, 969.
[43] Rath / Sponholz, IT-Compliance, Seite 69; Lehmann / Meents, Handbuch des FA IT-Recht, Kapitel 21 Rn 21; Schmidl, NJW 2010, 478; Hauschka, AnwBl 2010, 631; Roth / Schneider ITRB 2005, 19.
[44] Bürgerliches Gesetzbuch.
[45] BGH NJW 2009, 1066; OLG Hamm, CR 2004, 654; OLG Koblenz, Urteil vom 04.08.2010, 1 U 1492/09, BeckRS 2010, 28603; OLG Karlsruhe, NJW-RR 1997, 554; OLG Karlsruhe NJW 1996, 200; LG Konstanz, NJW 1996, 2662; Lehmann / Meents, Handbuch des FA IT-Recht, Kapitel 21 Rn 2; Lensdorf / Steger, ITRB 2006, 209.