CASTON

SINCE 1988 · INTERNATIONAL LAW & BUSINESS INFORMATION · WWW.CASTON.INFO COMPACT

IT-Compliance im Unternehmen

Monika Sekara, Rechtsanwältin in Hannover

No. 263 – 07/2008

Eines der wesentlichen Qualitätsmerkmale eines innovativen Unternehmens ist sein IT-System. Die IT-Infrastruktur verbindet das Unternehmen mit der Außenwelt und gewährleistet zudem eine effiziente Kommunikation unter den Mitarbeitern innerhalb des Betriebs. In Datenbanken lagern erhebliche Unternehmenswerte: das eigene Know how, Kunden- und Lieferantenadressen und unter Umständen Rezepturen und Formeln, die zusammen den Erfolg des Unternehmens im Wettbewerb sicherstellen.

Der Zugriff Unbefugter auf die IT-Systeme kann für Unternehmen daher zur existenziellen Bedrohung werden. Eine sichere IT zählt nicht nur zu den existenziellen Verpflichtungen eines jeden Unternehmens, sie ist auch Motor eines gesunden Wachstums und der problemfreien Anbindung von Standorten im Ausland.

IT-Compliance bedeutet die Einhaltung und Umsetzung von gesetzlichen Vorgaben, Verordnungen, Richtlinien und Verhaltensmaßgaben durch Unternehmen mit dem Ziel eines verantwortungsvollen Umgangs mit allen Aspekten der Informationstechnik.

Compliance-Vorschriften

KonTraG

Beim Risikomanagement geht es um die systematische Erfassung, Bewertung und Steuerung unterschiedlichster Risiken. Der Gesetzgeber hat unterschiedliche Regelungen geschaffen, die Unternehmen zur Einführung eines effizienten Risikomanagements auch im IT-Bereich verpflichten. Vorstände und Geschäftsführer von Unternehmen sind insbesondere seit der Einführung des KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich) verschärften Haftungsbedingungen ausgesetzt.

Das 1998 in Kraft getretene KonTraG hatte weitere Gesetzesänderungen im Bereich Corporate Governance zur Folge. Heute ist die Unternehmensleitung von Gesetzes wegen gezwungen (§§ 91 Abs. 2, 116 AktG bzw. § 43 Abs. 1 GmbHG), ein unternehmensweites Risikofrüherkennungssystem vorzuhalten. Dies gilt gleichermaßen für Aktiengesellschaften und für Unternehmen anderer Rechtsformen. Durch angemessene Informations-, Vorsorge- und Notfallmaßnahmen müssen Unternehmen die Sicherheit der verwendeten IT-Systeme gewährleisten. Jedes Unternehmen ist zudem verpflichtet, Aussagen zu Risiken und zur Risikostruktur zu treffen und diese im Jahresabschlussbericht der Gesellschaft zu veröffentlichen. Unternehmen müssen ihren Jahresabschlussbericht im elektronischen Bundesanzeiger im Internet hinterlegen (www.ebundesanzeiger.de).

Weitere Compliance-Anforderungen ergeben sich aus dem Bundesdatenschutzgesetz (BDSG), den Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), den Grundsätzen ordnungsgemäßer DV-gestützter Buchführung (GoBS), nach Basel II, aus dem Sarbanes-Oxley Act (SOX), vertraglichen Verpflichtungen mit Geschäftspartnern und den Grundrechten.

Das Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz verpflichtet Unternehmen, durch technische und organisatorische

Maßnahmen einen ausreichenden Schutz personenbezogener Daten zu gewährleisten. Insbesondere Zutritts-, Zugangs- und Zugriffskontrollen müssen verhindert, dass Unbefugte personenbezogene Daten einsehen können. Dasselbe gilt für die Speicherung oder Weitergabe solcher Daten.

Basel II

Anforderungen an die IT-Sicherheit ergeben sich auch aus dem Wirtschaftsverwaltungsrecht. Der Baseler Ausschuss für Bankenaufsicht hat Richtlinien zur Sicherung einer angemessenen Eigenkapitalausstattung im internationalen Bankwesen – kurz Basel II – aufgestellt. Seit Anfang 2007 müssen Banken bei der Bewilligung von Krediten eine differenzierte Risikobemessung vornehmen. Die Bonitätsprüfung erfolgt in Form eines Ratings, das das individuelle Ausfallrisiko des Kreditnehmers bestimmbar machen soll.

Bei der Entscheidung über die Fremdfinanzierung müssen die Banken vor allem das Risikomanagementsystem eines Kreditnehmers bewerten. Dazu gehört die Gefahr von Verlusten, die infolge des Versagens von internen Verfahren, Menschen und Systemen oder infolge externer Ereignisse eintreten können. Banken und Rating-Agenturen betrachten die Nutzung von IT-Systemen als operationelles Risiko. An das Risikomanagement und die Sicherheit von IT-Systemen stellen sie hohe Anforderungen.

Handels- und steuerrechtliche Vorgaben

Die IT-gestützte Buchführung und Rechnungslegung ist an hohe handelsrechtliche und steuerrechtliche Vorgaben gebunden. Bei Verstößen drohen eine Verwerfung der handelsrechtlichen Rechnungslegung und eine Schätzung der Besteuerungsgrundlage durch die Finanzverwaltung.

Buchführungs- und Rechnungslegungsverfahren müssen vom ursprünglichen Beleg bis zur zum Jahresabschluss nachvollziehbar sein (§ 238 Abs. 1 S. 2 HGB). Für die Erfassung, Verarbeitung, Ausgabe und Aufbewahrung aller rechnungsrelevanten Daten über Geschäftsvorgänge gelten nach GoBS die Kriterien der Vollständigkeit, Richtigkeit, Zeitgerechtheit, Ordnung, Nachvollziehbarkeit und Unveränderlichkeit.

Im Rahmen der steuerrechtlichen Außenprüfung ist es der Finanzverwaltung gestattet, die steuerrelevanten Unterlagen eines Unternehmens über einen digitalen Datenzugriff zu kontrollieren. Seit Anfang 2002 besteht die Verpflichtung, Buchführungsunterlagen elektronisch zu archivieren. Die Archivierung muss auf maschinell lesbaren und auswertbaren Datenträgern erfolgen. Der Steuerpflichtige muss dafür sorgen, dass die archivierten Unterlagen jederzeit innerhalb des gesamten Zeitraums der Aufbewahrungspflicht am Bildschirm lesbar sind. Die Dokumente sind unveränderbar und fälschungssicher aufzubewahren.

Internationale Standards: SOX und EURO-SOX

Nach gravierenden Bilanzskandalen einiger US-Firmen veranlassten die Senatoren Paul S. Sarbanes und Michael Oxley den US-amerikanischen Gesetzgeber zum Erlass des Sarbanes-Oxley-Acts (SOX oder SOA). Seit Mitte 2002 regelt dieses Gesetz umfassende Bilanzierungs-, Prüfungs- und Haftungspflichten für Unternehmen, die am US-Kapitalmarkt notiert sind und gegenüber der SEC (Securities and Exchange Commission) zur Publizität verpflichtet sind. Die SOX-Anforderungen sind auch von wesentlichen US-Tochtergesellschaften im Ausland (significant subsidiary) und von in den USA notierten ausländischen Gesellschaften (Foreign Private Issuer) zu erfüllen.

Das Gesetz macht CEO und CFO persönlich haftbar für fehlerhafte oder falsche finanzielle Angaben und Berichte. Es verlangt ein umfassendes und funktionsfähiges internes Kontrollsystem, das die Zuverlässigkeit der Rechnungslegung und der hieraus resultierenden Jahresabschlüsse gewährleistet. Im Falle eines Verstoßes ist das Management zur Rückzahlung erfolgsabhängiger Vergütungen verpflichtet. Gleichzeitig gilt ein Verbot der Darlehensgewährung an die Unternehmensleitung. Wirtschaftsprüfern ist es verboten, in der Zeit von Abschlussprüfungen weitere Beratungsleistungen zu erbringen.

Die Grundsätze des SOX haben EU-weite Reformen des Wirtschaftsprüfungsrechts nach sich gezogen. Mit der so genannten Abschlussprüferrichtlinie (RL 2006/43/EG, auch: EURO-SOX) haben das Europäische Parlament und der Rat internationale Prüfungsstandards zum Maßstab für eine europaweite Harmonisierung der Anforderungen an die Abschlussprüfung gemacht. Diese Richtlinie hat der Bundestag über eine Novelle des Wirtschaftsprüferrechts bereits Anfang September 2007 umgesetzt.

Die Novelle stellt sicher, dass Abschlussprüfer und Prüfungsgesellschaften bei der Durchführung von Abschlussprüfungen unabhängig bleiben und nicht

an den internen Entscheidungsprozessen der geprüften Unternehmen mitwirken. Die Erbringung zusätzlicher prüfungsfremder Leistungen, die die Unabhängigkeit gefährden könnten, ist während einer Jahresabschlussprüfung untersagt. Die Einrichtung von Prüfungsausschüssen und wirksamen internen Kontrollsystemen soll Risikomanagement und Rechnungslegung in Unternehmen verbessern. Unternehmen müssen ihre IT-Infrastruktur und deren Sicherheit künftig ordentlich dokumentieren.

Verträge mit Geschäftspartnern

Eine rechtliche Pflicht, die IT-Sicherheit im Unternehmen regelmäßig zu überwachen und weiterzuentwickeln, folgt mittelbar auch aus bestehenden Geschäftsbeziehungen. Verträge unter Geschäftspartnern enthalten z. B. häufig so genannte Vertraulichkeitsvereinbarungen. In diesen verpflichten sich die Unternehmen gegenseitig, die Geschäfts- und Betriebsgeheimnisse des jeweils anderen zu wahren. Für den Fall einer Verletzung wird eine erhebliche Vertragsstrafenzahlung vorgesehen. Eine mangelhafte IT-Sicherheit kann eine schuldhafte Verletzung vertraglicher Schutzpflichten und damit die Verwirkung von Vertragsstrafen oder Schadensersatzansprüchen zur Folge haben.

Das „neue" IT-Grundrecht

Im Februar 2008 hat das Bundesverfassungsgericht aus dem Grundgesetz ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme abgeleitet. Zwar erging das Urteil im Zusammenhang mit geplanten „Online-Durchsuchungen und –Überwachungen" der Verfassungsschutzbehörden in Nordrhein-Westfalen. Der Schutz dieses Grundrechts steht jedoch auch jedem Mitarbeiter zu, dem eine private Nutzung der Kommunikationsmittel am Arbeitsplatz gestattet ist. Die Rechtswissenschaft bezeichnet dies als so genannte „mittelbare Drittwirkung des Grundrechts" auf das Privatrecht. Damit hat das Urteil eine unmittelbare Auswirkungen auf die Wirtschaft: Unternehmen müssen ihre bisherige Politik zur Nutzung von IT-Systemen am Arbeitsplatz überdenken.

Der Schutz vor Eingriffen in die informationstechnischen Systeme sei eine Ausprägung des allgemeinen Persönlichkeitsrechts, entschieden die Verfassungsrichter. Die Möglichkeit, im Arbeitsspeicher und in Speichermedien hinterlegte personenbezogene Daten zu erheben und bis hin zur Erstellung eines Persönlichkeitsprofils auszuwerten, berge nach Ansicht der Richter eine neue Persönlichkeitsgefährdung. Hieraus folge ein grundrechtlich erhebliches Schutzbedürfnis des Einzelnen, auch am Arbeitsplatz. Eingriffe seien ausnahmsweise allenfalls dann erlaubt, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestünden. Ob dies der Fall ist, bleibt allein der richterlichen Einschätzung vorbehalten.

Für Unternehmen ergibt sich folgende Konsequenz: Ist es den Mitarbeitern gestattet, Kommunikationsmittel auch zu privaten Zwecken zu nutzen, dürfen automatisierte Überwachungsmaßnahmen oder Hardware-Durchsuchungen nur mit Einwilligung der betroffenen Mitarbeiter erfolgen. Dies erschwert einige Prozesse im Betrieb erheblich; beispielsweise müsste vor jeder automatisierten Kontrolle von E-Mail, Internetkommunikation, Softwarelizenzen oder dem Einsatz von Spam-Filtern und Firewalls grundsätzlich das Einverständnis der Mitarbeiter eingeholt werden.

Umgang mit Kommunikationsmitteln im Betrieb

Der Schutz des Fernmeldegeheimnisses umfasst nicht nur die Inhalte einer Kommunikation, sondern auch ihre Umstände. Zu ihnen gehört insbesondere, ob, wann, wie oft und zwischen welchen Personen oder Telekommunikationseinrichtungen eine Telekommunikation stattgefunden hat oder versucht worden ist. Diese Schutzwirkungen des Fernmeldegeheimnisses erstrecken sich ebenso auf den Informations- und Datenverarbeitungsprozess und die Kommunikationsdienste des Internets (z. B. E-Mail). Das hat das Bundesverfassungsgericht bereits 2005 in einem höchstrichterlichen Urteil klargestellt (BVerfG, Urt. v. 27.07.2005 – 1 BvR 668/04).

Der Schutz des Fernmeldegeheimnisses greift jedoch lediglich während eines laufenden Telekommunikationsvorgangs im Rechnernetz. Es ist grundsätzlich nicht betroffen bei Maßnahmen zur Überwachung oder Durchsuchung von Daten, die ein Teilnehmer nach Abschluss eines Telekommunikationsvorgangs auf seinen IT-Systemen gespeichert hat. Diese Schutzlücke hat das Grundrecht auf Integrität der IT-Systeme nunmehr geschlossen. Es verbietet jede Überwachung der auf einem PC abgelegten Daten, die ohne Einwilligung des Betroffenen erfolgt. Ist es Mitarbeitern im Betrieb gestattet, vom Arbeitgeber zur Verfügung gestellte PC, Notebooks, Email, Internet, Telefone, Mobiltelefone und andere Kommunikationsmittel eigenverantwortlich auch außerhalb der betrieblichen Belange privat zu nutzen, ist eine Ü-

berwachung nur mit vorheriger Einwilligung der Mitarbeiter möglich. Eine Ausnahme gilt nur für den Fall des Verdachts auf eine schwerwiegende Straftat. Selbst dann muss eine Überwachungsmaßnahme durch ein Gericht angeordnet sein.

Wesentlich einfacher gestaltet sich die Rechtslage, wenn den Mitarbeitern eine private Nutzung der Kommunikationsmittel des Arbeitgebers untersagt ist. Hierbei haben die Interessen des Arbeitgebers am Schutz des IT-Systems und an einer Kosten- und Arbeitskontrolle Vorrang gegenüber den Persönlichkeitsrechten der Mitarbeiter. Zum einen darf der Arbeitgeber in diesem Fall die Verbindungsdaten einer Kommunikation erfassen, ohne das Fernmeldegeheimnis zu verletzen. Die Inhalte der Kommunikation bleiben allerdings tabu. Zum anderen darf der Arbeitgeber die auf seinen IT-Systemen nach Abschluss einer Kommunikation gespeicherten Daten kontrollieren und überwachen. Die Maßnahmen bedürfen hier nicht der vorherigen Zustimmung der Betroffenen. Es empfiehlt sich aber, die Kontrollen (auch technisch) so zu gestalten, dass Persönlichkeitsprofile von Mitarbeitern nicht erfassbar sind.

Um zu verhindern, dass das Grundrecht auf Integrität der IT-Systeme sich gegen die Interessen des Arbeitgebers durchsetzt, sollte von vornherein eine private Nutzung der betrieblichen IT-Systeme untersagt werden. Jedenfalls aber sollten Unternehmen den Umfang von Privatnutzung und Kontrollrechten des Arbeitgebers mit ihren Mitarbeitern arbeitsvertraglich Regeln.

Der Beitrag wird fortgesetzt.

HERAUSGEBER

HERFURTH & PARTNER,
Rechtsanwälte GBR - German & International Lawyers
Luisenstr. 5, D-30159 Hannover
Fon 0511-30756-O Fax 0511-30756-10
Mail info@herfurth.de, Web www.herfurth.de
Hannover · Göttingen · Brüssel · München
Member of the ALLIURIS GROUP, Brussels

REDAKTION / HANNOVER

Redaktion: Ulrich Herfurth, Rechtsanwalt, zugelassen in Hannover und Brüssel (verantw.), Sibyll Hollunder-Reese, M.B.L., Rechtsanwältin (D); Philipp Neddermeyer, Rechtsanwalt (D);

unter Mitarbeit von Kenneth S. Kilimnik, LL.M., M.IUR., Attorney at Law (USA); Angelika Herfurth, Rechtsanwältin (D); Jens-Uwe Heuer, Rechtsanwalt (D); Dr. jur. Konstadinos Massuras, Rechtsanwalt (D) und Dikigoros (GR); Thomas Gabriel, Rechtsanwalt (D); JUDr. Yvona Rampáková, Juristin (CR); Egbert Dittmar, Rechtsanwalt (D); Metin Demirkaya, Rechtsanwalt (D); Dr. Jona Aravind Dohrmann, Rechtsanwalt (D); Marc-André Delp, M.L.E., Rechtsanwalt (D); Tatiana Getman, Rechtsanwältin (D); Monika Sekara, Rechtsanwältin (D); Kornelia Winnicka, Rechtsanwältin (D); Dr. jur. Wolf Christian Böttcher, Rechtsanwalt (D); Adeline Maler Berger, Advocate and Solicitor(GB/ SG), Peh-Wen Lin, Rechtsanwältin (D); Maimiti Cohen-Solal, Avocat (France), Attorney at Law (USA), Alexia Calleja Cabeza, Abogada (ES).

KORRESPONDENTEN / AUSLAND

u.a. Amsterdam, Athen, Barcelona, Brüssel, Budapest, Bukarest, Helsinki, Kiew, Kopenhagen, Lissabon, London, Luxemburg, Mailand, Madrid, Oslo, Paris, Prag, Stockholm, Warschau, Wien, Zürich, New York, Moskau, Peking, Tokio, Bombay, Bangkok, Singapur, Sydney.

VERLAG

CASTON GmbH, Law & Business Information
Luisenstr. 5, D-30159 Hannover,
Fon 0511 - 30756-50, Fax 0511 - 30756-60
Mail info@caston.info; Web www.caston.info