**IBM Deutschland**
September 2008

# IT-Sicherheit im Unternehmen

*Risikomanagement als IT-Compliance*

Autorin:
Monika Sekara, Herfurth & Partner Rechtsanwälte GBR

*Inhaltsverzeichnis*



## Einleitung

Das wesentliche Asset eines innovativen Unternehmens ist heutzutage sein IT-System. Die IT-Infrastruktur verbindet das Unternehmen mit der Außenwelt und gewährleistet eine effiziente Kommunikation unter den Mitarbeitern innerhalb des Betriebs. In Datenbanken lagern die Schätze des Unternehmens: das eigene Know-how, Kunden- und Lieferanten-adressen und geheime Rezepturen, die zusammen den Erfolg des Unternehmens im Wettbewerb sicherstellen.

Der Zugriff Unbefugter auf die IT-Systeme kann für Unternehmen 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.

## Compliance

Unternehmen, die im Ausland tätig sind, sehen sich aktuell inbesondere Gefährdungen durch Schadprogramme oder Datenausspähungen ausgesetzt. Häufig begünstigt die Nachlässigkeit der eigenen Mitarbeiter eine solche Situation. Studien bestätigen diese Einschätzung. Bereits in 2004 hat eine Umfrage im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ergeben, dass 89 % der IT-Verantwortlichen die Wirtschaft durch mangelnde IT-Sicherheit gefährdet sehen. Nach einer Studie von PWC zur Wirtschaftskriminalität kommt die Hälfte aller Täter aus dem eigenen Unternehmen. Pro betroffenem Unternehmen in Deutschland belaufe sich der Schaden auf ca. 3,4 Mio. EUR, schätzte PWC in 2005. Aktuellere Studien zeigen, dass selbst große Unternehmen in Deutschland ein nur mangelhaftes Risikomanagement betreiben. Gute Ergebnisse erzielten nur Unternehmen der Chemie-und Elektrobranche. Bei über 60 % der großen und mittelständischen Unternehmen war das Risikomanagement dagegen mangelhaft. Kleine Unternehmen sahen teilweise überhaupt kein Risikomanagement vor. Als Ursache hierfür gaben die Unternehmen eine fehlende Kompetenz im Compliance-Bereich an. Nach betriebswirtschaftlicher Betrachtung ist das Ziel eines effektiven Risikomanagements, den Wert des Eigenkapitals durch Optimierung des Risikoprofils zu maximieren. In rechtlicher Hinsicht ist ein optimales Risikomanagement darauf ausgerichtet, die gesetzlichen Comliance-Anforderungen umzusetzen bzw. hierdurch Haftung zu vermeiden. 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.

## 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).

***Inhalt***

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 verhindern, 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 Risiko-management 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 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, Nachvollzieh-barkeit 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: EUROSOX) 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.

*Inhalt*

*Compliance Vorschriften*

### 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.

*Folgen mangelnder IT-Sicherheit*

### Spionage und Datenverlust

Nach der Rechtsprechung ist eine Risikofrüherkennung entsprechend zu dokumentieren. Im Unternehmen muss es unmissverständliche Zuständigkeiten, ein enges Berichtswesen und eine Dokumentation über das Risikomanagement geben. Unterbleibt eine solche Dokumentation, stellt dies einen wesentlichen Gesetzesverstoß dar. Gerichte verlangen, sicherzustellen, dass vom verantwortlichen Sachbearbeiter über die jeweiligen Hierarchieebenen bis hin zur Unternehmensleitung sämtliche relevanten Stellen von vorhandenen Risiken Kenntnis erlagen, um die entsprechenden Maßnahmen zur Beherrschung dieser Risiken einleiten zu können. Eine mangelnde IT-Sicherheit kann einschneidende Folgen haben. Werden Betriebsgeheimnisse ausgespäht, drohen erhebliche wirtschaftliche Schäden. Datenverluste können Ausfälle in der Produktion und Schadensersatzforderungen auslösen. In einem solchen Fall verteuern sich nicht nur die Unternehmenskredite. Vielmehr drohen Über-prüfungen durch Datenschützer, die Bußgelder oder gar den Entzug der gewerblichen Zuverlässigkeit nach sich ziehen können. Oft fehlen in gerichtlichen Verfahren mangels verwertbarer Datensätze die entscheidenden Entlastungsbeweise.

### Geschäftsleitung in der Verantwortung

Rechtlich verantwortlich für die IT-Sicherheit im Unternehmen ist die Unternehmensleitung, etwa die Geschäftsführung oder der Vorstand. Die Mitglieder der Geschäftsleitung eines Unternehmens sind nach dem Gesetz verpflichtet, bei ihrer Tätigkeit die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Bei Pflichtverletzungen haften Geschäftsführer oder Vorstand im Innenverhältnis gegenüber ihrer Gesellschaft für den entstandenen Schaden. Diese Schadensersatzpflicht verjährt in fünf Jahren. Ein effizientes Risikomanagement muss sicherstellen, dass aktuelle und potenzielle Risiken kalkulierbar und kontrollierbar sind. Die Unternehmensleitung hat die Aufgabe, diese Risiken zu identifizieren, ihre Ursachen zu analysieren und ihr Ausmaß zu bewerten. Auf der Grundlage derartiger Informationen muss die Unternehmensleitung dann entscheiden, welche Maßnahmen der Risikosteuerung nach dem Gesamtziel des Unternehmens geeignet sind. Aus diesen Regelungen folgt die Pflicht der Unternehmensleitung zur Organisation von Zuständigkeiten, insbesondere zur sorgfältigen Auswahl und Aufsicht eines fachlich geeigneten IT-Leiters, IT-Sicherheitsbeauftragten und eines betrieblichen Datenschutzbeauftragten. Fehlen  unternehmenseigene Fachleute, muss die Unternehmensleitung externe Berater mit den Aufgaben betrauen.

### Haftungsrisiken für IT-Leiter

Verursachen Mitarbeiter einen Schaden im Unternehmen, haften sie nur für grobe Fahrlässigkeit und Vorsatz persönlich. In der Regel stellt ein Arbeitgeber eigene Mitarbeiter von der Haftung für leichte Fahrlässigkeit frei. In Fällen mittlerer Fahrlässigkeit kann der Arbeitnehmer anteilig an der Haftung beteiligt werden. Dies geschieht meistens in Höhe des Selbstbehalts einer eingreifenden Versicherung. Trifft den Arbeitgeber ein Mitverschulden, haften Arbeitgeber und Arbeitnehmer anteilig nach Quoten. Die Quoten bestimmen sich nach den jeweiligen Verschuldens- anteilen. Der Grad des Verschuldens wird anhand der konkreten Umstände geschätzt. Fahrlässig handelt, wer die im Verkehr erforderliche Sorgfalt außer Acht lässt. D. h. aufgrund der im Arbeitsvertrag präzisierten Standards hätte der betroffene Mitarbeiter wissen können und müssen, dass eine bestimmte Handlung vorzunehmen war. Grob Fahrlässig handelt, wer die im Verkehr erforderliche Sorgfalt in besonders hohem Maße außer Acht und dasjenige unbeachtet lässt, was jedem in der gleichen Situation hätte einleuchten müssen. Mittlere Fahrlässigkeit liegt vor, wenn der rechtlich missbilligte Erfolg voraussehbar und vermeidbar gewesen ist. Die leichte Fahrlässigkeit bezieht sich auf Fälle des typischen Abirrens (z. B. Vergreifen, Versprechen, Vertun). Vorsätzlich handelt, wer die Pflichtverletzung und den Schaden als möglich voraussieht und ihn für den Fall des Eintritts billigend in Kauf nimmt.

### Der 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 statt-

gefunden 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 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 Überwachung 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.

### Datenschutz

Das unternehmenseigene Sicherungskonzept muss die Einhaltung des Bundesdatenschutzgesetzes (BDSG) gewährleisten und personenbezogene Daten vor einem Missbrauch bei ihrer Speicherung und Übermittlung oder durch Veränderung und Löschung schützen. Die Erhebung, Verarbeitung und Nutzung von Daten darf daher nur erfolgen darf, wenn dies gesetzlich erlaubt ist oder die Einwilligung des Betroffenen bzw. eine Betriebsvereinbarung vorliegt. Personenbezogene Daten sind alle Informationen über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person. Bestimmbar ist eine Person, wenn sie direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem

oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind. Vom Schutzumfang des BDSG umfasst sind demnach alle Angaben zu einer Einzelperson. Neben Namen und Anschrift gehören dazu u. a. personalisierte Emailadressen und IPAdressen. Das BDSG stellt damit Anforderungen an die Gestaltung von Internetauftritten, Verträgen mit Auftragnehmern und innerbetrieblichen Dokumentationsprozessen.

Der Aufbau effektiver IT-Sicherheitsstrukturen soll Missbrauch verhindern. Dabei haben die IT- und Kommunikationssysteme folgende Sicherheitsanforderungen zu erfüllen: Vertraulichkeit (Schutz sensibler Daten); Verfügbarkeit (Nutzer hat Zugriff); Integrität (Daten bleiben nach Verarbeitung unverändert), Authentizität (Echtheit) sowie die Zurechenbarkeit und Revisionsfähigkeit von Daten. Das BDSG sieht eine verschuldensunabhängige Haftung für Schäden vor, die Dritten durch unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten entstehen. Eine Exkulpation ist hier nur möglich, wenn die Integrität und die Vertraulichkeit der gespeicherten personenbezogenen Daten gewährleistet ist und dies auch nachgewiesen werden kann (z. B. durch eine Zertifizierung). Für Unternehmen besteht die gesetzliche Pflicht, binnen eines Monats seit Aufnahme der Tätigkeit schriftlich einen betrieblichen Datenschutzbeauftragten zu bestellen (§ 4 f BDSG). Diese Pflicht gilt grundsätzlich für alle rechtlich selbständigen Betriebe, die personenbezogene Daten sowie Personaldaten automatisiert verarbeiten. Ausgenommen sind nur Betriebe, die auf klassische Weise mit personenbezogenen Daten (z. B. über Akten, Karteikarten, Formulare, Videos) umgehen. Hier ist ein betrieblicher Datenschutzbeauftragter erst zu bestellen, wenn mindestens 20 Arbeitnehmer regelmäßig damit befasst sind.

Der betriebliche Datenschutzbeauftragte kann auch unternehmensfremd sein, muss aber die erforderliche Fachkunde und Zuverlässigkeit besitzen. Die erforderliche Fachkunde ist gegeben bei vorhandenem Grundwissen über das Datenschutzrecht, die automatisierte Datenverarbeitung und die betrieblichen Zusammenhänge. Der Datenschutzbeauftragte muss mit der Organisation und Funktion des Betriebs vertraut sein und einen Überblick über alle Fachaufgaben haben. Die Zuverlässigkeit bezieht sich auf eine sorgfältige und gründliche Arbeitsweise, Belastbarkeit, Lernfähigkeit, Loyalität und Gewissen-haftigkeit. Der Datenschutzbeauftragte darf aufgrund seiner Stellung nicht in Interessenkollision mit anderen Funktionen oder Aufgaben geraten. Weil sie sich selbst nicht kontrollieren können, dürfen Inhaber, Geschäftsführer, Vorstände und andere Vertretungsorgane nicht zum Datenschutzbeauftragten bestellt werden. Das gleiche gilt für Personen, die im Betrieb für die Datenverarbeitung zuständig sind (z. B. Betriebsleiter, IT-Leiter). Mitarbeiter der Revision, der Rechtsabteilung und der Organisation können zum betrieblichen Datenschutzbeauftragten berufen werden. Der Datenschutzbeauftragte ist unmittelbar der Unternehmensleitung unterstellt und keinen Weisungen unterworfen (weisungsfrei). Aufgrund dieser eindeutigen Stellung auf Seiten des Arbeitgebers begegnet der betriebliche Datenschutzbeauftragte in der Praxis nicht selten dem Misstrauen des Betriebsrats; zum Wohle des Betriebs ist jedoch eine Zusammenarbeit notwendig. Fehlt ein Datenschutzbeauftragter, liegt eine Ordnungswidrigkeit vor, die mit Bußgeld geahndet werden kann.

### Datensicherheit

Besonders häufig vernachlässigen Unternehmen grundlegende technisch-organisatorische Datensicherheitsmaßnahmen. Dies gilt insbesondere für die revisionsfähige Benutzerverwaltung, den Schutz von Serverräumen, Notfallvorsorge und regelmäßige Auswertungen von Protokollen.

Erhebliche Sicherheitslücken ergeben sich, wenn benutzerbezogene Zugriffsberechtigungen lückenhaft oder gar nicht vorhanden sind. Jeder Arbeitnehmer sollte nur auf diejenigen Daten zugreifen können, die er für die Erfüllung der ihm zugewiesenen Aufgaben benötigt. Oft haben mehrere Mitarbeiter über ein Passwort Zugriff auf die gleiche Benutzeroberfläche. Um eine Revisionsfähigkeit der zu Zugriffsrechten geführten Unterlagen zu gewährleisten, sollte die Fachabteilung Zugriffsrechte nur nach schriftlichem Antrag erteilen. Es muss jederzeit nachvollziehbar sein, wer zu welcher Zeit welche Befugnisse und Zugriffsmöglichkeiten im IuK-System hatte. Die Verwendung von Gruppenkennungen und Gruppenpasswörtern ist daher zu verbieten. Tägliche Auswertungen von Log-Dateien stellen sicher, dass Sicherheitsverletzungen zeitnah entdeckt werden.

Der Ausfall der EDV kann einen gesamten Betrieb lahm legen. Liegt die Ursache hierfür in der Hardware und muss erst ein neues Teil beschafft werden, kann der Ausfall mehrere Tage dauern. Mit einer Notfallvorsorge kann bei einem Ausfall innerhalb kürzester Zeit eine angemessene Umgehung geschaffen werden, um den Betrieb der IT-Systeme zumindest zum Teil wieder herzustellen und so Schäden zu begrenzen. Im Rahmen von Übungen sollten Notfallkonzepte überprüft und die Wiederherstellung von Daten geübt werden. Sind Datenbestände nicht wieder herstellbar, haftet grundsätzlich der Betrieb selbst. Nach der Rechtsprechung ist die Datensicherung eine vorauszusetzende Selbstverständlichkeit. Jeder gewerbliche Betrieb muss selbst regelmäßig und zuverlässig für eine geeignete, lückenlose Datensicherung sorgen. Sicherungen müssen täglich, Vollsicherungen mindestens einmal wöchentlich erfolgen. Eine monatliche Komplettsicherung haben die Richter für unzureichend befunden. Eine „Blauäugigkeit“ in diesem Bereich führt zum Verlust von Ansprüchen, selbst wenn das IT-Systemhaus etwaige Beratungspflichten hierzu verletzt hat.

### Risikomanagement

Schwierigkeiten ergeben sich in der Praxis vor allem, wenn in Unternehmen Maßnahmen zu detailliert und umfassend geregelt sind. Beispielsweise ist der Notfallplan nicht selten ein mehrbändiges Werk, von dem nur sein Standort nicht aber die Inhalte bekannt sind. Selbst in den Fachabteilungen verfügen die einzelnen Mitarbeiter jeweils über Expertenwissen. Ein gemeinsames Wissen über die Abhängigkeiten und Verflechtungen der zugrunde liegenden Strukturen ist oft jedoch nur als vage Vorstellung vorhanden.

Das Risikomanagement ist ein Prozess, der insbesondere Folgendes beinhalten sollte:

- Darstellung der von der Unternehmensleitung festgelegten Risikomanagementstrategie,

- Analyse, Identifikation und Bewertung von Risiken und Risikoursachen,
- Verhaltensanweisungen zur Risikovermeidung bzw. Risikominimierung, z. B. Brandsicherer Serverraum, technische Zugangskontrollen, Verlagerung auf Outsourcing-Partner oder Versicherung,
- Risikoüberwachung (Kontrolle).

Die Umsetzung dieser Leitlinien führt geradewegs in die Einrichtung eines internen Kontrollsystems. Die Forderung nach einem internen Kontrollsystem ergibt sich aus den Prüfungsstandards für Wirtschaftsprüfer. Der Abschlussprüfer soll danach Aufbau, Angemessenheit und Funktion des IT-Systems beurteilen und drei Kernfragen zur eingesetzten IT beantworten:

- Risikomanagement: Gibt es einen angemessenen Prozess, wonach IT-Risiken systematisch entdeckt, analysiert, bewertet und verringert werden?
- IT-Kontrollsysteme: Gibt es ein angemessenes System zur Planung und Kontrolle des ordnungsgemäßen IT-Betriebs?
- Werden Risikomanagementsystem und IT-Kontrollsystem im operativen Betrieb effektiv gesteuert und verringern sie tatsächlich IT-Risiken?

Es erscheint insofern angebracht, betriebsintern ein zentrales (digitalisiertes) Risikomanagementhandbuch zu führen. Darunter ist nicht etwa ein Handbuch im klassischen Sinne zu verstehen. Vielmehr wären an einem zentralen Share-Point die für das betriebliche Risikomanagement bedeutenden Unterlagen und Anweisungen so zusammen zu führen, dass Mitarbeiter sich jederzeit effizient über die jeweiligen Zuständigkeiten, Maßnahmen und Anweisungen informieren können. In einem solchen Risikomanagementhandbuch könnten beispielsweise folgende Unterlagen hinterlegt werden (nicht abschließend):

- Leitlinien zur Risikokultur, Risikopolitik, organisatorischen Einbindung des Risikomanagements und zur Ablauforganisation, ein Überblick über bestehende Versicherungsverträge und Zuständigkeiten im Bereich Versicherungen
- ein Überblick über bestehende IT-Verträge und damit verbundenen innerbetrieblichen Aufgaben und Zuständigkeiten,
- Verhaltensanweisungen an Mitarbeiter,
- Nutzungsordnung bzw. Betriebsvereinbarung
- Notfallplanung (Notfallmanagement)
- Überblick zum Datenschutz (nämlich: Systemschutz, Datensicherung, Kontrollen, Umgang mit personenbezogenen Daten),
- Dokumentationen von Mitarbeiterschulungen.

Fehlen eigene Fachleute, beauftragen Unternehmen häufig externe Spezialisten mit der Erledigung bestimmter Aufgaben. Aus einer jahrelangen Zusammenarbeit folgen teilweise umfangreiche IT-Outsourcing-Projekte. Diese Art der Zusammenarbeit kann bereits zu einer Haftungsverlagerung auf den externen Partner führen und minimiert somit die eigenen Haftungsrisiken. Oft ist diese Art der Zusammenarbeit gerade für mittelständische Betriebe kostengünstiger als eigene Experten zu werben und zu beschäftigen.

**Hinweis**



Monika Sekara
Rechtsanwältin
Herfurth & Partner Rechtsanwälte GBR
Luisenstraße 5
30159 Hannover
Telefon: +49 (0)511- 307 56-0
E-Mail: info@herfurth.de

**Mehr Information**

Für mehr Informationen zum Bereich Datenmanagement und Compliance besuchen Sie unsere Website:

**ibm.com**/software/de/itsolutions/data/

IBM Deutschland GmbH
70548 Stuttgart
**ibm.com**/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
**ibm.com**/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
**ibm.com**/ch

Die IBM Homepage finden Sie unter:
ibm.com