Leitfaden
Rechtliche Pflichten im Bereich der IT-Sicherheit

von RA Robert Niedermeier und RA Dr. Markus Junker

HEUSSEN
Rechtsanwaltsgesellschaft mbH

A correspondent law firm of PRICEWATERHOUSECOOPERS

Rechtliche Pflichten im Bereich der IT-Sicherheit

Robert Niedermeier ist Mitglied der Information Communication Technology (ICT) Arbeitsgruppe bei der Heussen Rechtsanwaltsgesellschaft und überwiegend mit Fragen der Bereiche Recht, Technik und Organisation bei Datenschutz und IT-Security befaßt. Mit seinem internationalen Team projektiert er für Banken, Versicherungen und internationale Unternehmen den globalen Roll-out homogener Datenschutz- und IT Sicherheitsstrukturen im Konzern und entwickelt neue Modelle (homogene Datenschutzzelle, Custodian Concept) für rechtskonforme Datennutzung. Als Dozent für Datenschutz im Studiengang Electronic Marketing an der Bayerischen Akademie für Werbung beschäftigt er sich mit datenschutzrechtlichen Anforderungen an Werbung via Internet und Datawarehousing. In seiner Eigenschaft als Vorstand des European Institute for Computer Anti-Virus Research (www.eicar.org) diskutiert er mit der IT-Security Branche aktuelle Fragen zu Haftung und Exponierung von IT-Sicherheitsverantwortlichen.

Erstellt im Auftrag von SurfControl durch

HEUSSEN

Rechtsanwaltsgesellschaft mbH

A correspondent law firm of PRICEWATERHOUSECOOPERS

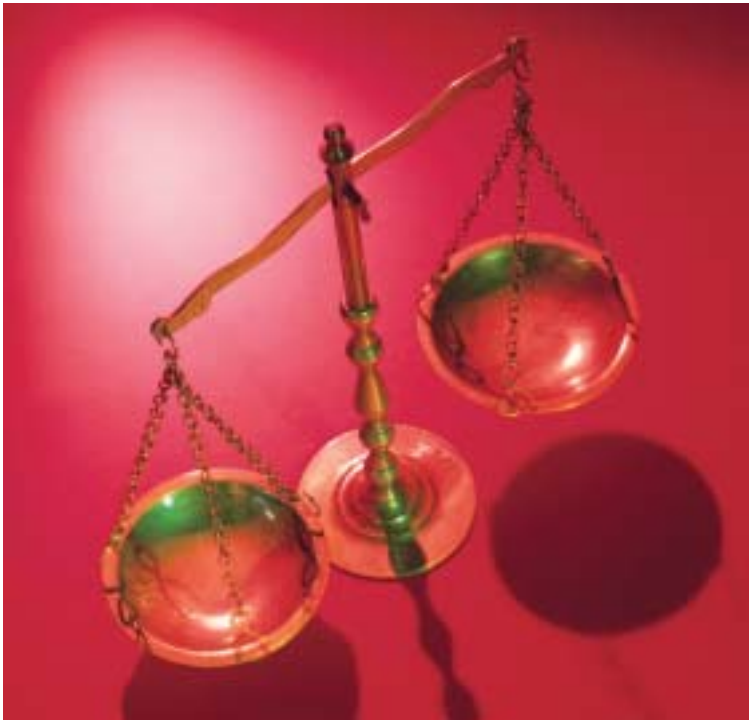
Hinweis

Dieses Dokument stellt einen generellen Leitfaden dar. Es sollte daher nicht als verbindliche Rechtsauskunft angesehen werden.

Wir geben keine Garantie und übernehmen keine Gewährleistung für die Genauigkeit oder Eignung der enthaltenen Richtlinien. Wir raten Unternehmen vor jeglicher Implementierung individuelle rechtliche Beratung einzuholen.

Rechtliche Pflichten im Bereich der IT-Sicherheit

Inhalt



Rechtliche Pflichten im Bereich der IT-Sicherheit

1. Rechtliche Aspekte der IT-Sicherheit

Unternehmen verstehen heute IT-Sicherheit immer noch weitgehend als Thema der Bereiche **Technik** und **Organisation.** Nur wenige **Profis** unter den IT-Verantwortlichen haben erkannt, dass das Spielfeld der IT-Sicherheit neben dem Bereich Technik und Organisation auch aus dem Bereich **Recht** besteht. Die Rechtslage verlangt von einem professionellen Verantwortlichen in der IT-Sicherheit die Kenntnis der wesentlichen rechtlichen Zusammenhänge für sein Aufgabengebiet, ebenso, wie ein Autofahrer die Straßenverkehrsordnung kennen muss. Ohne diese Kenntnisse werden IT-Sicherheitsverantwortliche ihre Aufgabe nicht korrekt erledigen können und zwangsläufig **Amateure** der IT-Sicherheit bleiben.

2. Welche Risiken bestehen, wenn rechtliche Pflichten zur Gewährleistung der IT-Sicherheit nicht erfüllt werden?

Mit der zunehmenden Vernetzung und Komplexität von IT-Systemen steigt das **Gefährdungspotential** rasant an. Auch wenn in der Vergangenheit spektakuläre Fälle an die Öffentlichkeit gelangt sind, so ist die Umsetzung von vollständiger IT-Sicherheitspolitik heute noch nicht Realität.

Rechtliche Pflichten im Bereich der IT-Sicherheit

Es gibt ganz unterschiedliche Szenarien, welchen **Bedrohungen** ein Unternehmen bei der Nutzung der Informationstechnologien ausgesetzt ist. Wer seinen Mitarbeitern beispielsweise den Zugang zum **Internet am Arbeitsplatz** eröffnet, muss nicht nur mit Kostenfolgen rechnen, wenn Arbeitszeit privat zum Surfen genutzt und die Internet- bzw. Intranet-Verbindung durch erhöhten Traffic belastet wird bzw. die Speichermedien durch gestiegenen Bedarf an Speicherplatz beeinträchtigt werden (etwa infolge von Spamming oder des Herunterladens großer Datenmengen).

Mit dem Zugang zum Internet erhalten umgekehrt auch Viren, Würmer, Trojaner und sonstige **schädliche Inhalte** Zugang zur IT-Infrastruktur des Unternehmens, sodass diese erheblich beeinträchtigt werden kann. Mitarbeiter können durch das Herunterladen und Installieren nicht lizenzierter Software **Urheberrechtsverletzungen** begehen und eine Haftung des Unternehmens und sogar der Unternehmensleitung hierfür verursachen. Durch das Herunterladen oder Versenden von Dateien mit extremistischen, sexistischen oder sogar pornografischen Inhalten, kann der **Betriebsfrieden** erheblich gestört werden. Schließlich besteht sogar die Gefahr, dass via E-Mail unkontrolliert **Betriebs- oder Geschäftsgeheimnisse** offenbart werden, etwa weil die Nachricht unverschlüsselt versendet wird und ein Dritter mitliest oder weil ein Mitarbeiter gezielt Informationen verraten möchte.

Jedes Ereignis, das aufgrund mangelnder oder unzureichend umgesetzter IT-Sicherheitsmaßnahmen eintritt, hat eine signifikante **finanzielle Auswirkung** auf Ihr Unternehmen, und zwar mit meist wesentlich höheren Kosten, als jenen für ein passendes IT-Sicherheitskonzept. Wer Vorsorge trifft, kann damit zukünftige Ausgaben verhindern oder zumindest vermindern **(Return on Security-Invest).** Eine vollständige IT-Sicherheitspolitik berücksichtigt immer, über die **technischen** Lösungen hinaus, die **organisatorischen** Maßnahmen und insbesondere rechtlichen Aspekte im Bereich IT-Sicherheit.

2.1 Top Ten der Exponierung

Aus den Erfahrungen der letzten Jahre lassen sich folgende Top Ten der rechtlichen Konsequenzen feststellen:

a. Schadensersatz

Unternehmen und Verantwortliche, die ohne Beachtung rechtlicher Vorgaben personenbezogene Daten prozessieren, haften für eintretende Nachteile auf Schadensersatz und Schmerzensgeld.

Rechtliche Pflichten im Bereich der IT-Sicherheit

b. Bußgeld

Verantwortliche, die personenbezogene Daten ohne entsprechende Einwilligung des Betroffenen oder ohne Berufung auf eine gesetzliche Ermächtigungsgrundlage prozessieren, werden mit einem Bußgeld bis zu 250.000 Euro bestraft.

c. Haftstrafe oder Geldstrafe

Verantwortliche, die Daten unter Verstoß gegen das Fernmeldegeheimnis oder Vorschriften des Bundesdatenschutzgesetzes prozessieren, riskieren eine Geld- oder Haftstrafe.

d. Gewerberecht/Wettbewerbsrecht

Unternehmen, die aufgrund ihres Geschäftsgebarens fortlaufend Defizite im Bereich IT-Sicherheit erkennen lassen, werden vom Wettbewerb beim Gewerbeamt angezeigt und müssen befürchten wegen Fehlen der erforderlichen Zuverlässigkeit ihre Gewerbeerlaubnis zu verlieren.

e. Reputationsverlust

Unternehmen und Verantwortliche, die durch fehlende Professionalität im Bereich IT-Sicherheit auffallen, werden in der Branche als „Risikofaktor“ angesehen.

f. Aufsichtsbehörden

Unternehmen und Verantwortliche, die durch nicht rechtskonforme Prozessierung personenbezogener Daten auffallen, riskieren Adressat einer Überprüfung durch die Datenschutzaufsichtsbehörde zu werden.

g. Beweisprobleme

Werden beweisrelevante Daten unter Verstoß gegen rechtliche Vorgaben erhoben, so können Sie etwa in Arbeitsgerichtsverfahren nicht verwendet werden.

Rechtliche Pflichten im Bereich der IT-Sicherheit

h. Versicherung

Unternehmen, die ihrer Organisationsverpflichtung nicht genügen sowie den Benchmark für Betriebssicherheit gem. Art 4. der Europäischen Richtlinie zum Datenschutz bei der elektronischen Kommunikation nicht erfüllen, bezahlen jedenfalls Teile ihrer Versicherungsprämie für die Betriebshaftpflicht umsonst. Bei Versicherungsschäden im Zusammenhang mit Defiziten im Bereich der IT-Sicherheit werden Versicherer die Versicherungsleistungen unter dem Vorbehalt eines Mitverschuldens kürzen und gegebenenfalls für zukünftige Fälle die Versicherungsprämie erhöhen. Zudem besteht die Gefahr, dass Versicherungen, wie die Directors & Officers Versicherung, zur Absicherung der Geschäftsleitung keine volle Protektion entfalten.

i. Urheberrechtsverstöße

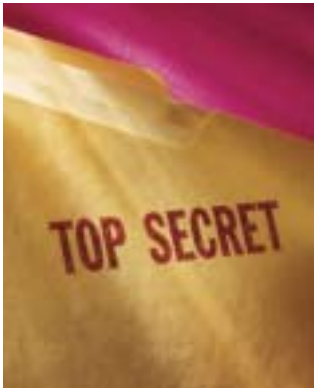
Tauchen in unternehmenseigenen IT-Infrastrukturen Musik- oder Filmdateien auf, die fremdem Copyright unterliegen, haften die Verantwortlichen auf Schadensersatz und Unterlassung, sowie nach den Regeln des Strafrechts. Eine Exculpation kommt hier nur in Betracht, wenn die Verantwortlichen nachweisen, dass sie Strukturen zur Kontrolle solcher Inhalte, etwa eine geeignete Software, implementiert haben.

k. Jugendschutz

Unternehmen, die Jugendliche beschäftigen und diesen Zugang zum Internet geben, müssen sicherstellen, dass kein Zugang zu jugendgefährdenden Inhalten möglich ist. Im Falle des Verstoßes drohen dem Verantwortlichen des Unternehmens Konsequenzen in Form eines Bußgeldes, sowie eine strafrechtliche Verfolgung.

Rechtliche Pflichten im Bereich der IT-Sicherheit

2.2 Wer ist für die IT-Sicherheit im Unternehmen verantwortlich?



Für IT-Sicherheit rechtlich verantwortlich ist die **Unternehmensleitung,** etwa die Geschäftsführung oder der Vorstand. Sie entscheiden, ob und welche technischen und organisatorischen Maßnahmen erforderlich sind.

Die Unternehmensleitung kann Entscheidungsbefugnisse an Mitarbeiter des Unternehmens delegieren, insbesondere an **leitende Angestellte,** etwa den Prokuristen oder den Leiter der IT-Abteilung. Diese können ihrerseits innerhalb ihres Verantwortungsbereichs Verantwortung delegieren, etwa an die **Administratoren** oder andere Mitarbeiter der IT-Abteilung. In jedem Fall sind die betreffenden Personen sorgfältig auszuwählen und zu überwachen, und es ist – etwa durch Schulungen und die Zurverfügungstellung der erforderlichen Sachmittel – sicherzustellen, dass sie ihre Aufgaben erfüllen können.

Die Unternehmensleitung erhält Unterstützung von besonderen Beauftragten, die die IT-Sicherheit überwachen, ihr hierüber berichten und Vorschläge unterbreiten sollen, ohne aber selbst über Entscheidungs- oder Weisungsbefugnisse zu verfügen. Dies gilt zum einen für den **betrieblichen oder behördlichen Datenschutzbeauftragten,** der unter den Voraussetzungen des Datenschutzrechts zwingend zu bestellen ist, und zum anderen für den **IT-Sicherheitsbeauftragten,** dessen Bestellung zwar nur ausnahmsweise – etwa im Telekommunikationsrecht oder für bestimmte Behörden – rechtlich geregelt ist, aber faktisch zur Gewährleistung der IT-Sicherheit erforderlich ist.

2.3 Stehe ich als Verantwortlicher für IT-Sicherheit mit einem Bein im Gefängnis?

Wird eine IT-spezifische Straftat im Aufgabenbereich eines IT-Veranwortlichen entdeckt, so kann sich dieser entweder persönlich oder als **Repräsentant** des Unternehmens stellvertretend für dieses strafbar gemacht haben.

Rechtliche Pflichten im Bereich der IT-Sicherheit

Die strafrechtlichen Risiken beim Einsatz technischer Mittel zur Gewährleistung der IT-Sicherheit sind vielfältig und häufig nur unzureichend bekannt. Dies gilt etwa für unbefugte **Überwachungsmaßnahmen** (etwa den Eingriff in das Telekommunikationsgeheimnis) oder das unbefugte **Löschen von Daten** (etwa bei einer unbefugten E-Mail-Filterung). Aus diesem Grund kann nur empfohlen werden, den Einsatz von Überwachungssoftware durch die Rechtsabteilung oder externe Berater zu begleiten.
Ein weiteres Risiko stellt die unbefugte **Offenbarung geheimer Informationen** über das Unternehmen (Betriebs- und Geschäftsgeheimnisse) oder über Mitarbeiter (personenbezogene Daten) dar. Die Unternehmensleitung unterliegt hier strengen Anforderungen. Strafbar macht sich dabei auch, wer es (etwa aus Kostengründen) pflichtwidrig **unterlässt,** die erforderlichen Sicherheitsmaßnahmen zu implementieren, und dabei billigend in Kauf nimmt, dass beispielsweise geheime Informationen Dritten zugänglich gemacht werden.

In der Praxis kommt es nur selten zu einer Verurteilung. Häufig wird das **Ermittlungsverfahren** gegen Zahlung eines Geldbetrags eingestellt. Hinzu kommen die durch das Verfahren entstehenden Kosten und gegebenenfalls Durchsuchungen und Beschlagnahmen im Unternehmen.

2.4 Hafte ich als Verantwortlicher mit meinem Privatvermögen?

Sind im Unternehmen die notwendigen IT-Sicherheitsstrukturen nicht oder unzureichend implementiert worden, so riskiert der IT-Verantwortliche die **Haftung** des Unternehmens und seiner eigenen Person, d. h. er muss gegebenenfalls mit seinem Privatvermögen für entstandene Schäden aufkommen. Anders als im Strafrecht haftet der IT-Verantwortliche im Zivilrecht auch für Fahrlässigkeit.

Fahrlässig handelt, wer die im Geschäftsverkehr einem ordentlichen Geschäftsmann obliegende Sorgfaltspflicht verletzt. Woraus sich diese Sorgfaltspflichten ergeben können, wurde oben bereits dargestellt. Wer **grob fahrlässig** Sicherheitsmaßnahmen unterlässt, muss übrigens damit rechnen, dass ihm entstandene Schäden nicht oder nicht vollständig ersetzt werden. So kann der Schädiger den Einwand des **Mitverschuldens** anführen, weil der Schaden nur in geringerem Umfang entstanden wäre. Die **Versicherung** kann die Leistung verweigern, wenn die IT-Sicherheit betreffende Obliegenheiten in den Versicherungsbedingungen verletzt wurden.

Rechtliche Pflichten im Bereich der IT-Sicherheit

2.5 Welche sonstigen Sanktionen drohen?

Eine Haftung mit dem Privatvermögen kommt lediglich bei Vermögensschäden in Betracht. Darüber hinaus drohen IT-Verantwortlichen in der Unternehmensleitung die Abberufung und **Kündigung** der Anstellungsverträge oder zumindest eine Abmahnung.

Nicht zu unterschätzen sind auch die mittelbaren Folgen eines IT-Sicherheitsvorfalls. Im Unternehmen entsteht unter Umständen hoher Aufwand zur Beseitigung der Folgen. Gelangt der Vorfall in die Presse oder ansonsten in die Öffentlichkeit, so droht zudem ein **Imageverlust.**

2.6 Wer kontrolliert die Einhaltung der rechtlichen Pflichten zur Gewährleistung der IT-Sicherheit?

Die Kontrolldichte für Maßnahmen der IT-Sicherheit wird generell unterschätzt. In der Praxis vor Ort ist zunächst an die **Mitarbeitervertretung,** soweit eine solche existiert, sowie an den **Datenschutzbeauftragten** zu denken.

In IT-sicherheitsrelevanten Schadensfällen drohen **Gerichtsverfahren** mit einer Überprüfung der IT-Sicherheit durch das Gericht und den Gegner mit Hilfe von Sachverständigen. Hat ein solcher Vorfall Wettbewerbsbezug, so drohen zudem kostenpflichtige Abmahnungen von **Konkurrenten.** Hat er strafrechtliche Bezüge, drohen Ermittlungsverfahren der **Staatsanwaltschaft.** Kommt es zum Versicherungsfall, drohen wie bereits erwähnt Untersuchungen des Versicherers.

Aber auch unabhängig von einem IT-Sicherheitsrelevanten Vorfall wird die IT-Sicherheit überprüft, etwa wenn **Banken** im Rahmen eines Ratings die Bonität eines Unternehmens prüfen oder allgemein **Investoren** die Risiken eines Unternehmens bewerten wollen. Aus ähnlichen Erwägungen nehmen auch **Vergabestellen** den Nachweis einer ausreichenden IT-Sicherheit in ihre Ausschreibungsbedingungen auf.

IT-Verantwortliche in börsennotierten Aktiengesellschaften sollten daran denken, dass die **Wirtschaftsprüfer** im Rahmen der Prüfung des Jahresabschlusses verpflichtet sind zu beurteilen, ob der Vorstand die erforderlichen Maßnahmen zur Einrichtung des Überwachungssystems getroffen hat und ob dieses System seine Aufgabe erfüllen kann.

Schließlich besteht die Möglichkeit einer Überprüfung der IT-Sicherheit im Unternehmen durch die **Datenschutzaufsicht,** sowie die **Gewerbeaufsicht** bzw. besonderen bereichsspezifischen Aufsichtsbehörden, wie etwa die berufsständischen **Kammern.**

Rechtliche Pflichten im Bereich der IT-Sicherheit

3. Woraus ergibt sich die rechtliche Pflicht zur Gewährleistung der IT-Sicherheit?

Häufig ist denjenigen, die für IT-Sicherheit verantwortlich sind, nicht bewusst, dass und unter welchen rechtlichen Gesichtspunkten sie gesetzlich dazu verpflichtet sind, bestimmte technische und organisatorische Maßnahmen zur Gewährleistung eines sicheren Betriebs der unternehmensinternen IT-Infrastruktur zu treffen.

3.1 Wirtschaftserwaltungsrecht

Unternehmen sind nach **gewerbeordnungsrechtlichen Grundsätzen** dazu verpflichtet, ihre IT-Infrastruktur entsprechend Art und Umfang der betriebenen Geschäfte so auszugestalten, wie dies für eine ordentliche Durchführung des Geschäfts erforderlich ist. Hierzu zählen über die notwendigen Sicherheitsmaßnahmen hinaus verschiedene Organisationspflichten, die die einwandfreie Abwicklung eines IT-Betriebs ermöglichen und sicherstellen. Soweit in bestimmten Branchen bestimmte Geheimhaltungspflichten bestehen (etwa hinsichtlich des Bank-, Mandanten-, Patienten- oder Telekommunikationsgeheimnisses), gelten besondere Maßstäbe.

Nach dem **Telekommunikationsgesetz** hat beispielsweise der Betreiber von Telekommunikationsanlagen, die dem geschäftsmäßigen Erbringen von Telekommunikationsdiensten dienen, wozu auch das Anbieten von E-Mail und sonstigen Internet-Diensten für Mitarbeiter des Unternehmens zählt, bei den zu diesem Zwecke betriebenen Telekommunikations- und Datenverarbeitungssystemen **angemessene technische Vorkehrungen** oder sonstige Maßnahmen zu treffen. Diese sollten folgende Punkte umfassen: **Schutz des Telekommunikationsgeheimnisses und personenbezogener Daten,** Schutz der programmgesteuerten Telekommunikations- und Datenverarbeitungssysteme gegen **unerlaubte Zugriffe,** Schutz gegen **Störungen,** die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen und schließlich Schutz von Telekommunikations- und Datenverarbeitungssystemen gegen **äußere Angriffe** und Einwirkungen von Katastrophen.

Welche Maßnahmen angemessen sind, ergibt sich nicht unmittelbar aus dem Gesetz. Der für die Schutzmaßnahmen zu erbringende **technische und wirtschaftliche Aufwand** ist zum einen von der Bedeutung der zu schützenden Rechte und zum anderen von dem **Stand der technischen Entwicklung** abhängig.

Die Regulierungsbehörde für Telekommunikation und Post sollte im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen **Katalog von Sicherheitsanforderungen** für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen erstellen, um eine nach dem Stand der Technik und internationalen Maßstäben **angemessene Standardsicherheit** zu erreichen.

Rechtliche Pflichten im Bereich der IT-Sicherheit

Wie auch der Bundesbeauftragte für den Datenschutz mehrfach bemängelt hat, entspricht der vorgelegte Katalog nicht diesen Maßstäben. In der Praxis ist daher zur Bestimmung des Stands der technischen Entwicklung auf Sachverständigengutachten und Fachveröffentlichungen zurückzugreifen. Anhaltspunkte für die Anforderungen der Aufsichtsbehörden können **Veröffentlichungen** der Datenschutzbehörden oder des Bundesamts für Sicherheit in der Informationstechnik (BSI) geben, etwa das IT-Grundschutzhandbuch.

3.2 Datenschutzrecht

Eine weitere Verpflichtung zur Gewährleistung der IT-Sicherheit ergibt sich aus dem Datenschutzrecht. Die Verpflichtung hierzu ist auf europäischer Ebene in verschiedenen Datenschutz-Richtlinien verankert und wurde auf nationaler Ebene in den einzelnen Datenschutzgesetzen umgesetzt. Das deutsche **Datenschutzrecht** ist in einer Vielzahl von Gesetzen geregelt. So ist zwischen dem Bundesdatenschutzgesetz, den verschiedenen Landesdatenschutzgesetzen sowie einer Vielzahl bereichsspezifischer Datenschutzgesetze zu unterscheiden (etwa für den Bereich des Sozialrechts das Sozialgesetzbuch und für den Bereich des Internet das Telekommunikationsgesetz samt Telekommunikations-Datenschutzverordnung sowie das Teledienstedatenschutzgesetz und den Mediendienste-Staatsvertrag).

3.3 Europäische Vorschriften für die Ausgestaltung der IT-Sicherheit

Wie die **„Datenschutzrichtlinie für elektronische Kommunikation"** bestimmt, muss der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes geeignete **technische und organisatorische Maßnahmen** ergreifen, um die Sicherheit seiner Dienste zu gewährleisten; auf die Netzsicherheit ist hierbei erforderlichenfalls zusammen mit dem Betreiber des öffentlichen Kommunikationsnetzes zu achten. Diese Maßnahmen müssen unter Berücksichtigung des **Standes der Technik** und der Kosten ihrer Durchführung ein Sicherheitsniveau gewährleisten, das angesichts des bestehenden Risikos **angemessen** ist.

Ähnliche Formulierungen befinden sich in den einzelnen deutschen Datenschutzgesetzen. In einer Anlage zum Bundesdatenschutzgesetz und in bereichsspezifischen Datenschutzgesetzen werden verschiedene Arten solcher Maßnahmen aufgeführt. So ist im Rahmen der so genannten **Weitergabekontrolle** beispielsweise durch Verschlüsselungssoftware und durch Überwachungssoftware zu gewährleisten, dass personenbezogene Daten nicht unbefugt übertragen werden können. Ferner ist im Rahmen der so genannten **Verfügbarkeitskontrolle** zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hierzu kann beispielsweise Filtersoftware einen wertvollen Beitrag leisten, die schädliche Inhalte wie Viren abblockt.

Rechtliche Pflichten im Bereich der IT-Sicherheit

3.4 Vertragliche Regelungen

Die Parteien können IT-Sicherheit ausdrücklich zum Gegenstand einer vertraglichen Vereinbarung machen. Dies kann von Absprachen hinsichtlich der Verschlüsselung von Informationen oder des Einsatzes von Virenscannern beim Versand von Nachrichten bis hin zur Einhaltung bestimmter IT-Sicherheitsrichtlinien etwa bei Outsourcing-Projekten reichen. Die Rechtsprechung hatte sich übrigens bereits mit den Anforderungen an Verträge zur Erstellung und Implementierung von **IT-Sicherheitskonzepten** zu beschäftigen (Landgericht Köln, JurPC Web-Dok. 62/2004 - URL: http://www.jurpc.de/rechtspr/20040062.htm).

Eine Pflicht zur Schaffung und Unterhaltung einer sicheren IT-Infrastruktur kann sich auch aus ungeschriebenen Nebenpflichten eines Vertrages ergeben (**Schutzpflicht** gegenüber dem Vertragspartner).

So sind im Online-Bereich tätige **Banken** unter Umständen verpflichtet, geeignete technische und organisatorische Vorkehrungen zu treffen, um beispielsweise durch **softwaremäßige Kontrollmechanismen** sicherzustellen, dass im Internet erteilte unplausible und offensichtlich irrtümliche Aufträge und Fehlbuchungen als solche erkannt werden oder dass es bei der Online-Abwicklung von Depotgeschäften nicht zu einem doppelten Verkauf eines Wertpapierbestandes kommen kann (siehe Oberlandesgericht Nürnberg, JurPC Web-Dok. 85/2003 - URL: http://www.jurpc.de/rechtspr/20030085.htm; und Oberlandesgericht Schleswig, JurPC Web-Dok. 87/2003 - URL: http://www.jurpc.de/rechtspr/20030087.htm).

Eine Pflicht zum Schutz des Vertragspartners besteht auch im Arbeitsverhältnis, und zwar im Verhältnis des Arbeitgebers zum Arbeitnehmer unter dem Aspekt der Fürsorgepflicht. Dies gilt in besonderem Maße und zusätzlich unter dem Aspekt des Jugendschutzes im Verhältnis des aufsichtspflichtigen Arbeitgebers zu seinen minderjährigen Auszubildenden. Es ist – am sinnvollsten durch geeignete Software-Lösungen – sicherzustellen, dass diesen keine E-Mails oder Web-Seiten mit jugendgefährdenden Inhalten zugänglich gemacht werden.

3.5 Risikofrüherkennungssystem nach KonTraG

Mit dem am 01.05.1998 in Kraft getretenem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (sog. KonTraG) wurde die Pflicht zur Schaffung eines unternehmensinternen **Risikofrüherkennungssystems** im Recht der Aktiengesellschaften eingeführt: Der Vorstand hat danach geeignete Maßnahmen zu treffen, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden. Den Fortbestand der Gesellschaft kann unter anderem eine fehlende IT-Sicherheit gefährden.

Rechtliche Pflichten im Bereich der IT-Sicherheit

Ob ein solches Risikofrüherkennungssystem besteht, ist unter Umständen von den **Wirtschaftsprüfern** im Rahmen des Jahresabschlusses zu prüfen. Ist es nicht ordnungsgemäß eingerichtet worden und entstehen dadurch Schäden, so droht dem Vorstand eine **Haftung** mit seinem Privatvermögen. Wie das Landgericht Berlin darüber hinaus bereits im Jahr 2002 entschieden hat, kann die Verletzung der Pflicht zur Einrichtung eines solchen Systems ein wichtiger Grund für eine **außerordentliche Kündigung** des Anstellungsverhältnisses des Vorstandes sein.

3.6 Rating nach Basel II

Die Unternehmensleitung ist schließlich vertraglich und gesetzlich dazu verpflichtet, vorhersehbare Vermögenseinbußen des Unternehmens zu verhindern. Eine solche Vermögenseinbuße droht beispielsweise dann, wenn sich das Unternehmen nicht hinreichend auf ein Rating nach den Vorschlägen des Baseler Ausschusses für Bankenaufsicht (**„Basel II"**) vorbereitet und zu diesem Zweck für eine sichere unternehmensinterne IT-Infrastruktur sorgt.

Das hat folgenden Hintergrund: Bei nahezu jeder **Insolvenz** eines Unternehmens sind auch Banken als Kreditgeber betroffen. Meist bleiben auch sie auf zumindest einem Teil ihrer Forderung sitzen, da eventuell vorhandene Sicherheiten häufig nicht zur Deckung der noch ausstehenden Summen ausreichen bzw. die Insolvenzmasse nicht zur vollen Befriedigung der Forderung ausreicht. Diese Forderungsausfälle können die Solvenz der Bank selbst gefährden. Um dem vorzubeugen, sollen Kredite von vornherein mit einem gewissen Anteil an **Eigenkapital** der Bank unterlegt sein.

Nach den Vorschlägen von Basel II soll sich der für den einzelnen Kredit zu hinterlegende Betrag nicht mehr wie bei Basel I pauschal nach der Einteilung in bestimmte Gruppen, sondern nach dem **Ausfallrisiko im Einzelfall** richten. Im Ergebnis erhält ein Unternehmen um so bessere Kreditkonditionen, je unwahrscheinlicher das Risiko seiner Insolvenz ist. Zur Beurteilung dieses Risikos dienen den Banken Ratings, mit denen die Situation des Unternehmens umfassend überprüft werden soll. Die Bedeutung der IT-Infrastruktur hängt wiederum damit zusammen, dass heutzutage in allen wesentlichen Unternehmensprozessen IT-Systeme eingesetzt werden und diese somit das Rückgrat des Unternehmens bilden. Neben betriebswirtschaftlichen fließen daher auch IT-Sicherheitsspezifische Risikoeinschätzungen in das Rating ein.

Rechtliche Pflichten im Bereich der IT-Sicherheit

4. Was kann ich als Verantwortlicher tun?

IT-Sicherheit hat eine technische, eine organisatorische und eine rechtliche Säule.

4.1 Welche technischen Möglichkeiten gibt es?

An erster Stelle ist zu empfehlen, zum Schutz der IT-Sicherheitsinfrastruktur geeignete **Software** zu implementieren, welche es innerhalb des rechtlichen Rahmens zulässt, den Datenverkehr zu scannen, die Log-Files zu speichern und gegebenenfalls bestimmte Inhalte in E-Mails zu filtern oder Zugriffe zu Web-Seiten zu blocken. IT-Sicherheitsverantwortliche, die keine Tools einsetzen, um Sicherheitsaspekte der IT-Infrastruktur im Griff zu haben, müssen sich dem Vorwurf der fehlenden Professionalität stellen.

4.2 Welche organisatorische Maßnahmen gibt es?

Technische Maßnahmen müssen von einer Reihe organisatorischer Maßnahmen flankiert werden. Am wichtigsten ist es, die IT-Sicherheitspolitik zu koordinieren und etwa auf der Grundlage einer IT-Sicherheitsrichtlinie ein **IT-Sicherheitskonzept** zu entwickeln und zu implementieren. Ein solches Vorhaben hilft zudem die Schwachstellen innerhalb der IT-Sicherheits-Infrastruktur zu identifizieren. Vorbereitend und ergänzend kann ein **IT-Sicherheitsaudit** durchgeführt und dessen Erfolg mit einem **„Gütesiegel"** dokumentiert werden. Neben den rein zivilen Audits macht es für exponierte Unternehmen auch immer mehr Sinn sich einem Audit nach militärischen Benchmarks zu unterziehen.

Ein schriftliches IT-Sicherheitskonzept dokumentiert die Organisation der IT-Infrastruktur und deren Überwachung. Nur auf diesem Weg ist es zuverlässig möglich, im Streitfall den **(Entlastungs-)Beweis** zu führen, die gesetzlichen Anforderungen an die IT-Sicherheit erfüllt zu haben.

Ein wesentlicher Teil organisatorischer Maßnahmen liegt im **psychologischen** Bereich. Bei der Implementierung des IT-Sicherheitskonzepts sind das Bewusstsein der Mitarbeiter für IT-Sicherheit (**IT-Security-Awareness**) und die Akzeptanz der erforderlichen Maßnahmen entscheidende Faktoren. Soweit eine Mitarbeitervertretung besteht, sollte dies frühzeitig mit einbezogen werden.

Rechtliche Pflichten im Bereich der IT-Sicherheit

Ohne eine geeignete IT-Sicherheitsrichtlinie ist zumindest in größeren Unternehmen kein ordnungsgemäßer Betrieb der IT-Infrastruktur möglich. Da die technischen und rechtlichen Anforderungen einem ständigen Wandel unterliegen, muss das IT-Sicherheitskonzept **dynamisch** sein und in regelmäßigen Abständen fortgeschrieben werden.
Soweit der Arbeitgeber die Nutzung von E-Mail und World Wide Web durch seine Arbeitnehmer kontrollieren möchte, ist es dringend zu empfehlen, im Zuge der Implementierung des IT-Sicherheitskonzepts eine **IT-Nutzungsordnung** in arbeitsrechtlich wirksamer Art und Weise im Betrieb einzuführen und ein **Verbot der privaten Nutzung des Internet** festzuschreiben. Abzuraten ist auch von Kompromissen, wie beispielsweise der Erlaubnis, das Internet nur in festgelegten Zeiten oder zumindest webbasierte E-Mail-Dienste privat zu nutzen.

Um das Entstehen einer so genannten **betrieblichen Übung** zu verhindern, dürfen die Verantwortlichen die private Nutzung auch nicht stillschweigend dulden. Vorsorglich sollte festgelegt werden, dass die Aufhebung des Verbots der privaten Internet-Nutzung nur schriftlich erfolgen kann.

Bestandteil der organisatorischen Maßnahmen muss ferner sein, die Sicherung von elektronischen Beweisen zu ermöglichen (**Network-Forensic Services**). Ohne verwertbare Beweise ist eine spätere Rechtsverfolgung in der Regel aussichtslos. Ergänzend ist an **strukturelle investigative Maßnahmen** zu denken, mit denen der Datenverkehr nach verdächtigen Mustern überwacht werden kann.

Zusätzlich sollten **Krisenpapiere** entwickelt werden, etwa für den Fall, dass staatsanwaltschaftliche **Durchsuchungen** und Beschlagnahmen drohen, oder für den Fall, dass auf einem Speichermedium im Betrieb strafbare Inhalte wie etwa Raubkopien oder **kinderpornografisches** Material entdeckt wird.

4.3 Welche rechtlichen Möglichkeiten gibt es?

Die technischen und organisatorischen Maßnahmen müssen sich innerhalb des rechtlich zulässigen Rahmens halten. Daher ist es dringend zu empfehlen, den Einsatz von Überwachungssoftware **rechtlich begleiten** zu lassen. Ansonsten besteht das Risiko, sich beispielsweise durch das Filtern von E-Mail wegen Datenunterdrückung und Verletzung des Telekommunikationsgeheimnisses strafbar zu machen. Zudem müssen – gegebenenfalls in Absprache mit der Mitarbeitervertretung – mit Blick auf das Datenschutzrecht, die **Einzelheiten der Überwachung** festgelegt werden. Wie bereits erwähnt, ist aus rechtlichen Gründen dringend zu empfehlen, die private Nutzung des Internet im Betrieb zu untersagen.

Rechtliche Pflichten im Bereich der IT-Sicherheit

5 Zusammenfassung

Die Existenz von IT-Sicherheitsrisiken ist objektiv gegeben. IT-Sicherheit ist daher **„Chefsache".** Wer für IT-Sicherheit verantwortlich ist, sollte sich daher über die rechtlichen Vorgaben und daraus resultierenden Risiken informieren, die erforderlichen Schritte initiieren und seine Mitarbeiter entsprechend instruieren. In jedem Falle wird empfohlen die IT-Infrastruktur durch geeignete Software-Tools zu kontrollieren sowie gleichzeitig korrespondierende Strukturen zu implementieren um rechtskonformen Betrieb zu gewährleisten. Entscheidend ist, in welchem Maße es gelingt, existierende Risiken zu erkennen und diese durch **technische, organisatorische** und **rechtliche** Maßnahmen zu minimieren.

RA Robert Niedermeier **RA Dr. Markus Junker**

Heussen Rechtsanwaltsgesellschaft München

HEUSSEN

Rechtsanwaltsgesellschaft mbH

A correspondent law firm of PRICEWATERHOUSECOOPERS

Rechtliche Pflichten im Bereich der IT-Sicherheit

Weiterführende Links:

www.cybercourt.de
www.recht.de
www.internet4jurists.at
www.juris.de
www.jura.uni-sb.de
www.meta-jur.de
www.jura.uni-muenster.de
www.metalaw.de

Relevante Gesetze:

Europäische Richtlinie über Datenschutz bei der elektronischen Kommunikation
Bundesdatenschutzgesetz
Telekommunikationsgesetz
Strafgesetzbuch
Bürgerliches Gesetzbuch
Gewerbeordnung
Handelsgesetzbuch
Urhebergesetz
Jugendschutzgesetz