CASTON

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

Risikomanagement und IT-Sicherheit

Monika Sekara, Rechtsanwältin in Hannover

No. 271 – 10/2008

Insbesondere Unternehmen mit Auslandstätigkeit sehen sich in verstärktem Maße Gefährdungen durch Schadprogramme oder Datenausspähungen ausgesetzt. Häufig begünstigt die Nachlässigkeit der eigenen Mitarbeiter eine solche Situation. Studien bestätigen diese Einschätzung. Selbst große Unternehmen in Deutschland betreiben ein nur mangelhaftes Risikomanagement. 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.

In rechtlicher Hinsicht ist ein optimales Risikomanagement darauf ausgerichtet, die gesetzlichen Comliance-Anforderungen umzusetzen bzw. hierdurch Haftung zu vermeiden. Compliance-Anforderungen ergeben sich aus dem Gesellschaftsrecht (KonTraG, §§ 91 Abs. 2, 116 AktG bzw. § 43 Abs. 1 GmbHG), 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.

Haftung von Geschäftsleitung und IT-Leitern

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 Verschuldensanteilen. 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.

Folgen mangelnder IT-Sicherheit

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 Überprüfungen 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.

Haftungsfallen

Datenschutz

Das unternehmenseigene Sicherungskonzept muss die Einhaltung des Bundesdatenschutzgeseztes (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 IP-Adressen. 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 Gewissenhaftigkeit.

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.

Wege zur Risikominimierung

Schwierigkeiten ergeben sich in der Praxis vor allem, wenn in Unternehmen Maßnahmen zu detailliert und umfassen 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.

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 abschließende):

- 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),

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 eine kostengünstiger als eigene Experten zu werben und zu beschäftigen.

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