CHEFSACHE IT-SICHERHEIT

- Abschlussprüfung
- Basel II
- SOX
- Vorstandshaftung
- KonTraG
- UMAG

NÖRR STIEFENHOFER LUTZ
RECHTSANWÄLTE STEUERBERATER WIRTSCHAFTSPRÜFER • PARTNERSCHAFT

NÖRR STIEFENHOFER LUTZ

Inhalt

Hacker, Cracker und Computerviren bedrohen nicht nur Dotcom-Unternehmen

Die Zeiten, in denen Computerviren ein bloßes Ärgernis waren und Hacker noch als romantische Helden im digitalen Cyberspace angesehen wurden, sind vorbei. Unternehmen erleiden heute aufgrund mangelhafter IT-Sicherheit immense Schäden, und ihre Vorstände und Geschäftsführer stehen dabei in der Schusslinie. Verursacht werden diese Schäden durch die immer häufiger auftretenden Virenepidemien, durch Computerbetrug oder die Ausforschung hochsensibler Unternehmensdaten.

Komplexität vs. Sicherheit

Durch fehlende IT-Sicherheitsrichtlinien, intransparente System- und Benutzerstrukturen sowie mangelhafte Überwachungs- und Kontrollmechanismen können Viren und Hacker Sicherheitslücken in der Software ausnutzen. Diese sind vielfältiger Art und reichen von einfachen Programmierfehlern über schlecht konfigurierte und administrierte Systeme bis hin zu bewusstem oder unbewusstem Fehlverhalten der Benutzer. Hinzu kommt die heutzutage ständig steigende Komplexität der Software, die zunehmende Vernetzung von Informationen und die wachsende Medienkonvergenz. Nicht zuletzt auch das zögerliche Verhalten der IT-Industrie im Hinblick auf die Sicherheit ihrer Produkte erschwert deren Absicherung.

Falls aber auch nur ein einziges Sicherheitsloch besteht, stehen die Unternehmensnetzwerke offen und die Geschäftsdaten sind schutzlos der Neugier von Konkurrenten oder der Zerstörungswut von schadenstiftender Software ausgeliefert.

Durch die unproblematische Verfügbarkeit leicht bedienbarer Hacker-Tools hat sich zudem der Kreis der potenziellen Angreifer stark vergrößert. Im Zuge der damit verbundenen erkennbaren Kommerzialisierung der Hacker-Szene kommt es zudem zu immer professionelleren und gezielteren Angriffen auf exponierte IT-Systeme von Wirtschaftsunternehmen. Dabei werden Geschäftsgeheimnisse und Mitarbeiteridentitäten gestohlen oder sensible Unternehmensbereiche durch elektronische Attacken sabotiert. Professionell durchgeführte und gut bezahlte Online-Industriespionage ist heute für Unternehmen jeder Größe eine akute Bedrohung. Je stärker bedeutende Wirtschaftsunternehmen global vernetzt sind und dabei vom störungsfreien Funktionieren ihrer Informationstechnologie abhängig sind, desto erheblicher wirken sich Sicherheitsvorfälle auf die nationale und globale Wirtschaftslage aus.

Auch die Politik hat das Problem erkannt

Erst vor kurzem reagierte nun auch die Bundesregierung auf diese Entwicklung. Mit einem nationalen Aktionsplan will das Bundesinnenministerium den Schutz von Unternehmen und Verbrauchern vor Computerviren, Hacker-Angriffen und Online-Betrug verbessern. Dafür baut das Bonner Bundesamt für Sicherheit in der Informationstechnik (BIS) nun ein Krisenreaktionszentrum auf, das ein Frühwarnsystem entwickeln und Informationen über Gefahren im Internet verbreiten soll. Die IT-Wirtschaft beteiligt sich an der Initiative. Auch in anderen Ländern wurde der Staat aktiv. In Großbritannien gibt es bereits eine Sonderabteilung des Justizministeriums mit Computerexperten und Kriminologen, die sich dem Kampf gegen Internetkriminalität widmen.

IT-Sicherheit:
Eine neue Herausforderung für Unternehmen

Computerviren gibt es, seitdem 1986 der Amerikaner Fred Cohen den ersten geschrieben hat. Und auch wenn der wohl berühmteste Vertreter seiner Zunft, der Hacker Kevin Mitnick, erst 1995 vom FBI gestellt und für seine äußerst erfolgreichen Angriffe auf Firmennetzwerke verurteilt wurde, gibt es Hacker ebenso lange, wie Universitäten und Unternehmen Computersysteme einsetzen.

In den letzten 20 Jahren haben sich jedoch nicht nur die öffentliche Wahrnehmung, sondern auch die rechtlichen Umstände entscheidend geändert. Heute existieren nicht nur spezifische Straftatbestände für Computerkriminalität, sondern anders als früher auch gesetzliche Haftungstatbestände und Schadensersatzansprüche gegen die Verantwortlichen.

Speziell das Wirtschaftsrecht wurde durch neue gesetzliche Bestimmungen wie das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) entscheidend verschärft. Dieser rechtliche Faktor wird durch wirtschaftliche Erfordernisse ergänzt, die Unternehmen zur IT-Sicherheit verpflichten. Hierzu gehören wirtschaftliche Finanzabkommen wie Basel II, gehobene Anforderungen der Versicherungswirtschaft und nicht zuletzt Neuerungen bei den Bestimmungen, denen Wirtschaftsprüfer bei der Prüfung der Jahresabschlussberichte unterliegen.

Die wichtigsten IT-Risiken

Viren

Schadenstiftende Software wie Viren und Würmer verursachen der Wirtschaft mittlerweile extrem hohe Schäden. Der Virus Code Red soll allein in den USA Ausfälle im Wert von 6 Milliarden US-Dollar nach sich gezogen haben. Der Wurm Zotob bremste am 17. August 2005 die Arbeit in 13 Werken des Autoherstellers Chrysler in den USA und brachte große Nachrichtensender wie CNN dazu, wieder die Schreibmaschinen hervorzuholen. Mitarbeiter mussten bis zu 50 Minuten lang die Arbeit unterbrechen. In Europa entstehen jedes Jahr allein bei kleinen und mittelständischen Unternehmen Schäden von rund 22 Milliarden Euro.

Phishing-Angriffe, Trojaner und Spyware

Vertrauliche Daten sind das häufigste Ziel von automatisierten Angriffen auf Firmennetzwerke. Phishing-Angriffe bauen darauf, dass vertraut erscheinende Webseiten oder augenscheinlich bekannte Software im Hintergrund sensible Daten verraten. Derartige Versuche von Betrügern, Internet-User auf gefälschte Webseiten zu locken, damit sie dort persönliche PIN-Codes oder Passwörter hinterlassen, haben stark zugenommen. Bei Erfolg ermöglichen sie Identitätsdiebstähle, die Unternehmen und Privatleute gleichermaßen betreffen. Trojanische Pferde dienen schließlich – oft als legitime und nützliche kleine Programme getarnt – dazu, den befallenen Computer unter die Herrschaft von Dritten zu bringen. Spyware schließlich kann dazu genutzt werden, heimlich Informationen über das befallene Computersystem und seine Anwender zu sammeln.

Die wichtigsten IT-Risiken

Hacker

Wenn es um komplexe Angriffe auf Unternehmensnetzwerke geht, die technisches Know-how und große Erfahrung mit den verbreitetsten Betriebssystemen erfordern, kommen die Hacker ins Spiel. Früher war es ein intellektueller Sport, Systeme wie etwa das der CIA oder des FBI zu knacken. Heute ist die Hacking-Szene kommerziell geworden. Ein anschauliches Beispiel ist der Angriff auf die Clearing-Stelle für Visa und Mastercard (Card Solutions). Hacker erbeuteten hier 40 Millionen Datensätze von Kreditkarten, private genauso wie Unternehmenskarten. Auch Karten von Apple und Microsoft waren dabei. Kurz darauf konnte man in einem Internetshop fremde Kreditkartendaten für 10 US-Dollar pro Nummer erwerben.

Genauso gut könnte sich aber zum Beispiel auch ein Wettbewerber von einem Hacker Informationen darüber beschaffen lassen, wie sich die Produkte seines Konkurrenten wirklich verkaufen oder sogar dessen Systeme sabotieren. Laut Zeitungsberichten wird derzeit zum Beispiel ein amerikanischer Geschäftsmann vom FBI gesucht, weil er angeblich Hacker angeheuert hatte, um die Internetseiten seiner Konkurrenz außer Gefecht zu setzen. Der hierbei entstandene Schaden beträgt über 1 Million US-Dollar. Oft werden solche Taten auch von ehemaligen Mitarbeitern begangen, die sich an ihrem alten Arbeitgeber rächen wollen.

Sogar Spamwellen kann man mittlerweile bei Hackern bestellen. Erst infizieren sie zehntausende Rechner von nichts ahnenden Privatleuten oder unvorbereiteten Unternehmen mit Trojanischen Pferden. Diese Zombi-Armeen verschicken dann beispielsweise Spam-E-Mails in alle Welt oder setzen gezielt die E-Mail-Systeme anderer Unternehmen außer Gefecht. Da Spam-E-Mails aus Sicht der Anbieter tatsächlich immer noch für den notwendigen Absatz sorgen, werden solche Fälle immer wieder auftauchen.

Selbst ein Bankraub ist inzwischen per Internet möglich: In diesem Frühjahr erleichterten Hacker die Sumitomo Mitsui Bank um ca. 220 Millionen Euro.

IT-Sicherheit ist Chefsache, weil es das Gesetz verlangt

Rechtspflichten zur IT-Sicherheit: KonTraG, AktG und HGB

Frühwarnsysteme für Aktiengesellschaften

Das KonTraG (ein Artikelgesetz mit dem erklärten Ziel, die Unternehmenswelt transparenter und damit überprüfbarer werden zu lassen) hat die Regelung des § 91 Abs. 2 in das Aktiengesetz (AktG) gebracht. Danach müssen Vorstände von Aktiengesellschaften ein Risikofrüherkennungs- und Überwachungssystem einrichten.

§ 91 AktG
(2) Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.

Zu den akuten Bedrohungen für das Unternehmen, die hiermit angesprochen werden, gehören nach Ansicht von Rechtsexperten mittlerweile auch und gerade die IT-Risiken. Es gilt dabei als selbstverständlich, dass der Gesetzgeber nicht nur die bloße Erkennung von drohenden Gefahren verlangt, sondern im Interesse des Unternehmens auch eine proaktive Reduzierung der gegebenen Risiken durch vorbeugende Maßnahmen fordert.

Unmittelbar betroffen durch das KonTraG sind neben Aktiengesellschaften auch andere Gesellschaften, die mindestens zwei der folgenden Kriterien nach § 267 HGB erfüllen:

- Bilanzsumme > 4,015 Millionen Euro
- Umsatz > 8,03 Millionen Euro
- Mitarbeiterzahl > 50

Geltung auch für andere Gesellschaftsformen

Über Verweisungsnormen im GmbH-Gesetz und im HGB hinaus gilt die Logik dieser Vorschriften im Übrigen auch für die Sorgfaltsmaßstäbe aller anderen handelsrechtlichen Gesellschaftsformen wie GmbH, GmbH & Co. KG, OHG und KG. Grundlage dafür ist jeweils die Definition der Sorgfalt eines ordentlichen Kaufmanns. In Zukunft wird sich im Schadensfall kein Geschäftsführer mit der Aussage verteidigen können, er sei sich über die gegebenen Risiken nicht bewusst gewesen.

IT-Sicherheit im Rahmen des Lageberichts

Zudem ist im (Konzern-) Lagebericht auf Risikomanagementziele und -methoden der Gesellschaft einschließlich IT-Risiken einzugehen. Der (Konzern-) Lagebericht ist wiederum Gegenstand der Prüfung durch einen Abschlussprüfer, der insbesondere auch die Tauglichkeit und Effektivität des Frühwarnsystems beurteilen muss.

§ 317 HGB
(4) Bei einer börsennotierten Aktiengesellschaft ist außerdem im Rahmen der Prüfung zu beurteilen, ob der Vorstand die ihm nach § 91 Abs. 2 des Aktiengesetzes obliegenden Maßnahmen in einer geeigneten Form getroffen hat und ob das danach einzurichtende Überwachungssystem seine Aufgaben erfüllen kann.

IT-Sicherheit ist Chefsache, weil der Chef persönlich haftet

Haftungsrisiken im Bereich IT-Sicherheit

Die Haftung der Vorstände

Vorstände und Geschäftsführer haften persönlich gegenüber ihrem Unternehmen, wenn sie ihre Pflichten verletzen und dem Unternehmen dadurch ein Schaden entsteht.

§ 93 AktG
Sorgfaltspflicht und Verantwortlichkeit der Vorstandsmitglieder

(1) Die Vorstandsmitglieder haben bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden (…).

(2) Vorstandsmitglieder, die ihre Pflichten verletzen, sind der Gesellschaft zum Ersatz des daraus entstehenden Schadens als Gesamtschuldner verpflichtet. Ist streitig, ob sie die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters angewandt haben, so trifft sie die Beweislast.

Ein Beispiel hierfür kann sein, wenn ein Hacker sich Daten des Unternehmens besorgt, diese an die Konkurrenz verkauft oder in der Öffentlichkeit zugänglich macht. In vielen Fällen dürfte für den Schaden schon genügen, dass überhaupt bekannt wird, die Daten eines Unternehmens seien nicht sicher verwahrt. Aber wenn ein Unternehmen seine Produktion anhalten muss, wichtige Daten unwiederbringlich verliert oder von Wettbewerbern vom Markt verdrängt wird, stehen die Vorstände in der Haftung.

Alle Manager sind bedroht

Selbst wenn der Aufsichtsrat mit einer Klage gegen den Vorstand zögert: Vom 1. November 2005 an können Minderheitsaktionäre die Durchsetzung dieser Schadensersatzansprüche leichter einklagen als bisher. Das nötige Quorum wird vom Gesetz zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts (UMAG) von 1 Million oder 10 Prozent des Grundkapitals auf gerade einmal 100.000 (Nominalwert) oder 1 Prozent des Grundkapitals abgesenkt. Und wenn auch die Kleinaktionäre nicht klagen, der Insolvenzverwalter wird es sicher tun, weil er per Gesetz verpflichtet ist, solche Ansprüche einzutreiben.

IT-Sicherheit ist Chefsache, weil der Chef persönlich haftet

Haftungsrisiken im Bereich IT-Sicherheit

Haftung des Unternehmens

Nicht vergessen werden darf, dass auch das Unternehmen selbst haftet, wenn Dritte – zum Beispiel Kunden oder Geschäftspartner – infolge mangelhafter IT-Sicherheit zu Schaden kommen. Unbemerkt per E-Mail verschickte Viren oder fahrlässig zerstörte Kundendaten wirken folglich nicht nur äußerst rufschädigend, sondern können zu hohen Entschädigungsforderungen führen.

Kann ein Unternehmen keinen ausreichenden Nachweis führen, dass es das Thema IT-Sicherheit verantwortungsvoll gehandhabt und entsprechende Maßnahmen umgesetzt hat, wird es sich kaum gegen diese Ansprüche verteidigen können.

Erhöhter Druck von Außen

Der US-Kongress diskutiert derzeit über Gesetzesvorlagen, die angesichts der sich häufenden Pannen Unternehmen und Finanzinstitute mit strikteren datensicherheitsrechtlichen Auflagen belegen. Diese sehen unter anderem zwingend eine umgehende Information der Öffentlichkeit im Falle von Sicherheitsproblemen und Schadensersatzansprüche für die Geschädigten vor.

IT-Sicherheitsexperten gehen davon aus, dass vor diesem Hintergrund alle größeren Unternehmen über kurz oder lang Vorstände haben werden, die sich ausschließlich um Sicherheitsaspekte kümmern werden.

IT-Sicherheit ist Chefsache, weil der Chef persönlich haftet

Datenschutzrechtliche Haftungsrisiken: BDSG und TKG

Datenschutz bedeutet auch Datensicherheit

Datenschutz bedeutet nicht nur, dass personenbezogene Daten nur mit Einwilligung verarbeitet oder weitergegeben werden dürfen, sondern auch, dass niemand unberechtigt auf diese Daten zugreifen können darf. Daher heißt Datenschutz zwangsläufig auch Datensicherheit.

Vorgaben des Gesetzgebers

Ein gutes Arbeitsprogramm, mit dem zumindest grundlegende Elemente der IT-Sicherheit aufgebaut werden können, enthält § 9 Bundesdatenschutzgesetz (BDSG) mit seiner Anlage.

Darin regelt der Gesetzgeber vergleichsweise ausführlich, welche Maßnahmen bei der automatischen Verarbeitung personenbezogener Daten zu treffen sind. Hierzu gehören insbesondere:

- Zugangskontrollen
- Datenträgerkontrollen
- Speicherkontrollen
- Benutzerkontrollen
- Zugriffskontrollen
- Übermittlungskontrollen
- Transportkontrollen
- Organisationskontrollen

Werden durch eine mangelhaft implementierte IT-Sicherheit datenschutzrechtliche Bestimmungen verletzt, drohen gemäß §§ 47 und 48 BDSG Bußgelder bis zu 250.000 Euro und unter Umständen sogar Freiheitsstrafen.

Das Unternehmen als unfreiwilliger Telekommunikationsanbieter

Die wenigsten Unternehmen, die ihren Mitarbeitern die private Nutzung des Internets zur Verfügung stellen (z.B. für das Versenden von privaten E-Mails oder zum Surfen im Internet), wissen, dass sie dadurch aus rechtlicher Sicht zu Anbietern von Telekommunikationsdiensten (TK-Dienste) werden. Dadurch laufen sie nach Meinung einiger Juristen Gefahr, denselben Bestimmungen wie große TK-Unternehmen z.B. Telekom, Vodafone oder Arcor zu unterliegen.

In erster Linie hat das die Konsequenz, dass diese Unternehmen dem Schutz des Fernmeldegeheimnisses unterliegen. Das Telekommunikationsgesetz (TKG) regelt in diesem Zusammenhang sehr detailliert die Rechte und Pflichten des Unternehmens. Ein Schwerpunkt hierbei liegt auf der Speicherung und Verarbeitung von Verbindungsdaten. Abgesehen von einigen Ausnahmen dürfen diese grundsätzlich nicht gespeichert werden. Dies hat unter Umständen gravierende Konsequenzen für die Arbeit mit E-Mail-Spamfiltern und Firewalls.

Verletzungen des Fernmeldegeheimnisses unterliegen Geld- oder Freiheitsstrafen bis zu fünf Jahren.

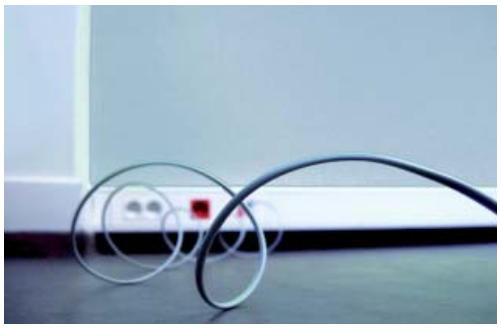
IT-Sicherheit ist Chefsache, weil der Chef persönlich haftet

Der wirtschaftliche Hintergrund: IT-Sicherheit im Rahmen der Jahresabschlussprüfung

Der Prüfungsstandard PS 330

Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) hat bereits 2002 den Prüfungsstandard „Abschlussprüfung bei Einsatz von Informationstechnologie“ (IDW PS 330) herausgegeben. Das IDW legt in diesem Prüfungsstandard die Anforderungen nieder, nach denen Wirtschaftsprüfer im Rahmen von Abschlussprüfungen bei Einsatz von Informationstechnologie IT-Systemprüfungen durchführen müssen.

Der IDW-Prüfungsstandard betrifft dabei sämtliche Abschlussprüfungen, d.h. Prüfungen von Jahres-, Konzern- und Zwischenabschlüssen im Sinne des IDW-Prüfungsstandards „Ziele und allgemeine Grundsätze der Durchführung von Abschlussprüfungen“ (IDW PS 200).



IT-Systemprüfungen als Bestandteil der Abschlussprüfung

Der Abschlussprüfer hat folglich IT-gestützte Rechnungslegungssysteme daraufhin zu beurteilen, ob diese den gesetzlichen Anforderungen – insbesondere den Ordnungsmäßigkeits- und Sicherheitsanforderungen – entsprechen. Hierzu gehören vor allem die nach § 322 Abs. 1 Satz 1 HGB in Verbindung mit § 317 Abs. 1 Satz 1 HGB und § 321 Abs. 2 Satz 3 HGB geforderten Prüfungsaussagen über die Ordnungsmäßigkeit der Buchführung.

Folglich ist es die Aufgabe des Abschlussprüfers, bei der Erstellung eines Berichts auch das IT-System des zu prüfenden Unternehmens insoweit zu untersuchen, als dieses rechnungslegungsrelevante Daten verarbeitet. Der Begriff der Rechnungslegung umfasst dabei die Buchführung, den Jahresabschluss und den Lagebericht bzw. auf Konzernebene den Konzernabschluss und den Konzernlagebericht.

Ein wesentlicher Aspekt der IT-Systemprüfung ist dabei eine Risikobeurteilung. Hierbei werden die Risiken festgestellt, die die Entwicklung des Unternehmens beeinträchtigen oder der Erreichung der Unternehmensziele entgegenstehen können.

IT-Sicherheit ist Chefsache, weil der Chef persönlich haftet

Der wirtschaftliche Hintergrund: Basel II, Corporate Compliance und der Sarbanes Oxley Act

Basel II – die Banken achten jetzt auf die Eigenkapitalabsicherung

Die neue Basler Eigenkapitalvereinbarung (Basel II) behandelt insbesondere bankenaufsichtliche Überprüfungsprozesse. Weil hiernach die Banken wesentlich stärker auf die Risiken bei der Rückzahlung ihrer Darlehen achten müssen, hängen Zinskonditionen für ein Unternehmen von nun an von einer Risikobewertung ab. Deswegen spielt IT-Sicherheit auch für die Unternehmensfinanzierung eine Rolle: Wenn bei einer Versicherung oder einem Unternehmen wie Amazon oder Neckermann die IT ausfällt, kann das schlimmere Folgen haben, als herkömmliche Risiken wie die Abschreibung von Forderungen aus dem Exportgeschäft.

Sind IT-Risiken nicht vollständig erfasst oder die Sicherheitsvorkehrungen mangelhaft, verschlechtern sich das Rating und damit auch die Kreditkonditionen. Ganz zu schweigen von dem Image- und Kursrisiko, das beispielsweise eine Bank eingeht, wenn eine Rating-Agentur rügt, die IT-Sicherheit sei mangelhaft. Diese Verantwortung lässt sich nur begrenzt delegieren oder auslagern. Selbst wer einen renommierten Dienstleister mit der IT-Sicherheit beauftragt, ist also nicht aus dem Schneider. Ihn treffen auch dann noch Überwachungspflichten.

Sarbanes Oxley Act (SOX): US-Recht diktiert IT-Sicherheit auch in Europa

SOX ist eine Reaktion auf die diversen jüngeren Finanzskandale in den USA, insbesondere aber auf Enron und WorldCom. Ziel des Gesetzes ist es, Investoren zu schützen und das verloren gegangene Vertrauen der Märkte wiederzugewinnen.

Die Regelungen des Gesetzes betreffen dabei alle Unternehmen weltweit, die an einer amerikanischen Wertpapierbörse notiert sind sowie unter bestimmten Voraussetzungen auch deren Tochterfirmen. Die den Unternehmen eingeräumte Übergangsfrist läuft dabei zum Ende des Fiscal Year 2005 ab.

Die für die Überwachung und Durchsetzung von SOX zuständige Behörde verlangt von allen betroffenen Unternehmen, die Integrität ihrer Daten sicher zu stellen. Andernfalls drohen den Verantwortlichen Bußgelder und für Vorstände sogar bis zu 20 Jahre Gefängnis. Bislang gab es allerdings keinen Fall, in dem die Behörde versucht hat ausländische Manager strafrechtlich zu verfolgen. Ein wahrscheinlicheres Szenario ist, dass ausländische Unternehmen wegen mangelnder IT-Sicherheit aus dem NYSE-Listing heraus fallen.

Zusammenfassung

Die schwerwiegendsten Probleme aus juristischer Sicht

Haftungsgefahren der Vorstände und Geschäftsführer

Die persönliche Haftung für Vorstände von Aktiengesellschaften und auch für Geschäftsführer anderer Gesellschaftsformen können unter Umständen existenzbedrohende Ausmaße annehmen.

Haftung des Unternehmens

Aber auch die Unternehmen müssen im Rahmen ihres eigenen Risikomanagements die Gefährdung ihrer IT-Systeme berücksichtigen und entsprechende IT-Sicherheitsinfrastrukturen aufbauen, um Haftungsgefahren zu eliminieren.

Betriebswirtschaftliche Konsequenzen für Unternehmen

Dank Basel II und SOX stehen die Unternehmen auch gegenüber den kreditvergebenden Banken immer mehr im Rampenlicht. Unternehmen, deren IT-Sicherheitsinfrastrukturen nicht sorgfältig aufgestellt und im Zweifel nachweisbar strukturiert sind, werden diese Versäumnisse in Form schlechter Konditionen bei der Kreditvergabe spüren.

Die Jahresabschlussprüfungen setzen ohnehin schon das Bestehen von sicheren IT-Systemen voraus und werden im Zweifelsfall von den Wirtschaftsprüfern ausführlich daraufhin überprüft.

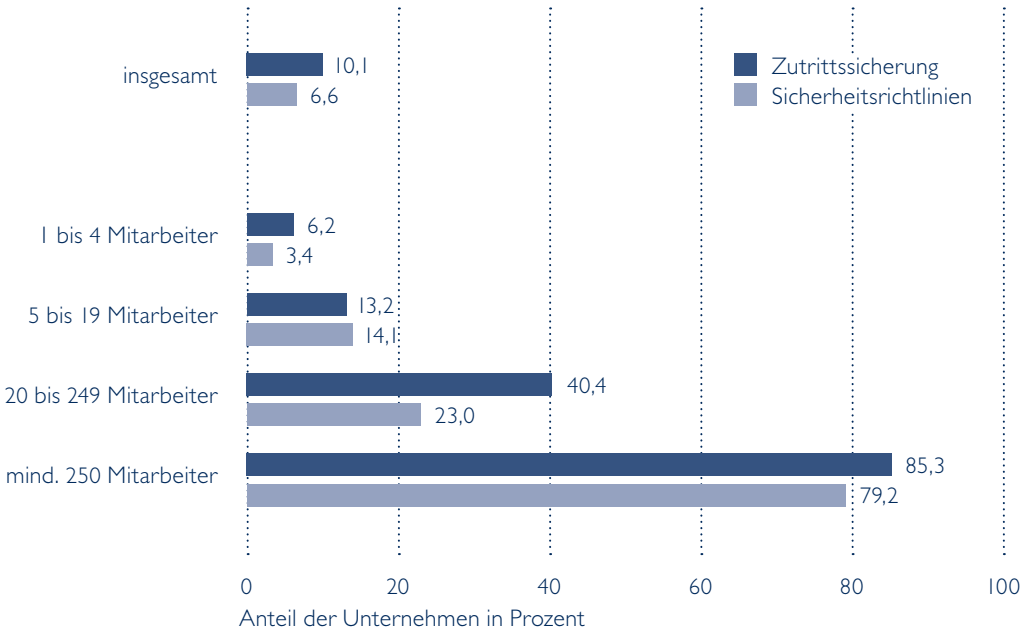
Störungen der Betriebsabläufe und Image-Schäden

IT-Sicherheitsvorfälle sind weiterhin die denkbar schlechteste Publicity für jedes Unternehmen. Je mehr zudem die Kerngebiete des Unternehmens von der positiven Einstellung seiner Kunden abhängen (also speziell im Dienstleistungssektor, wo das Kundenvertrauen eine immer größere Rolle spielt), desto drastischer kann sich fehlende Sensibilität für Sicherheitsaspekte auf die Unternehmenszahlen auswirken.

Abgesehen davon sind die wirtschaftlichen Verluste durch IT-Sicherheitsvorfälle immens. Viren können die Geschäftsprozesse einer ganzen Firma lähmen, und ein einziger Hacker kann das Ergebnis von jahrelangen Bemühungen um neue Produkte oder zahlende Kunden zunichte machen.

Ausblick: Die Wirtschaft wappnet sich …

Größere Unternehmen haben die Gefahr erkannt und schon eine gewisse Basis geschaffen. Hinreichend sicher im Bezug auf ihre Haftungsrisiken dürfen sich aber selbst diese Unternehmen in der Regel nicht fühlen – ausreichend sind diese Maßnahmen in den seltensten Fällen.



Verwendung von Zutrittssicherung und Sicherheitsrichtlinien nach Anzahl der Mitarbeiter

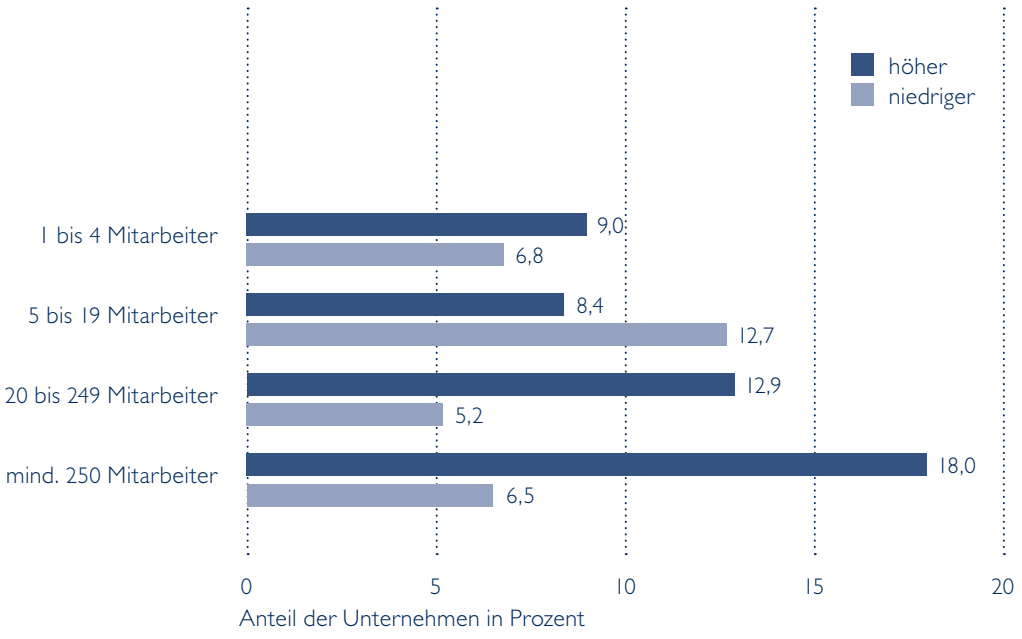
Lesehilfe: 6,2 Prozent der Unternehmen mit 1 bis 4 Mitarbeitern, die IT-Sicherheitsmaßnahmen einsetzen, verwenden Zutrittssicherungen für Räume mit zentraler IT-Hardware

Anmerkung: Angaben hochgerechnet auf die der Befragung zugrunde liegende Grundgesamtheit

Quelle: FAZIT-Unternehmensbefragung, Frühjahr 2005; Berechnungen des ZEW

Ausblick: Die Wirtschaft wappnet sich …

Die Unternehmen planen zudem, im Jahre 2005 mehr Geld für IT-Sicherheit auszugeben als im Vorjahr. Dabei haben vor allem die großen Unternehmen die Zeichen der Zeit erkannt und erhöhen ihre IT- Budgets, um den neuen Anforderungen gerecht zu werden.



Erwarteter Anteil für IT-Sicherheit am IT-Budget für 2005 im Vergleich zu 2004 nach Anzahl der Mitarbeiter

Lesehilfe: 9 Prozent der Unternehmen mit weniger als 5 Beschäftigten rechnen mit einem steigenden IT-Sicherheitsanteil am IT-Budget für 2005 im Vergleich zu 2004

Anmerkung: Angaben hochgerechnet auf die der Befragung zugrunde liegende Grundgesamtheit

Quelle: FAZIT-Unternehmensbefragung, Frühjahr 2005; Berechnungen des ZEW

5 Schritte zum professionellen Corporate Information Security Management

Die Erste-Hilfe-Checkliste für Unternehmen, Vorstände und Geschäftsführer

1. Bedrohungsanalyse

- Identifizierung der gegebenen Gefahren und Analyse ihrer Auswirkungen
- Integration der IT-Sicherheit in das betriebliche Risikomanagement
- Feststellung der konkreten Haftungspotenziale des Unternehmens und der Unternehmensführung

2. Schutzbedarfsdefinition

- Technische Überprüfung der IT-Sicherheit (ggf. durch externe IT-Sicherheitsexperten, mit IT-Sicherheits-Audits der Systeme und Penetrations-Tests der Netzwerke – auch zur Vorbereitung der Unternehmensberichte)
- Rechtliche Überprüfung der bestehenden Verträge mit Geschäftspartnern und Dienstleistern sowie der gängigen Vertragsmuster im Hinblick auf begrenzbare Haftungsrisiken im Bereich IT-Sicherheit

3. IT-Sicherheit etablieren

- Festlegung von Schutzzielen, die rechtlich und wirtschaftlich verhältnismäßig sind
- Erstellung einer unternehmensweiten, verbindlichen IT-Sicherheitsrichtlinie zum Nachweis der erforderlichen kaufmännischen Sorgfalt im Schadensfall
- Durchführung von Mitarbeiterschulungen zur Sensibilisierung und zur internen Kommunikation der neuen Maßnahmen
- Bestellung eines IT-Sicherheitsbeauftragten zur fortlaufenden Betreuung und Überprüfung der IT-Sicherheit im Unternehmen
- Outsourcen von IT-Sicherheit durch Managed Security Services (MSS)

4. Kontrolle und Anpassung

- Regelmäßige und andauernde Überprüfung der Wirksamkeit der IT-Sicherheitsinfrastruktur
- Gegebenenfalls periodische Hinzuziehung von externen IT-Sicherheitsexperten und regelmäßige Durchführung von Penetrations-Tests

5. Notfallplanung

- Erstellung von Notfallplänen und Desaster-Recovery-Policies
- Auslagerung von Sicherheitskopien gefährdeter Ressourcen (Software-Sourcecodes, Forschungsergebnisse oder Kundendaten) an spezielle Dienstleister (DataVaults)
- Schulung von speziellen Mitarbeitern in den Grundlagen der IT-Forensik, um im Schadensfall keine wichtigen Spuren zu zerstören

Ihre Ansprechpartner

Dr. Jyn Schultze-Melling, LL.M., Rechtsanwalt
Tel. +49(0)89 286 28-542
E-Mail jyn.schultze-melling@noerr.com

Ralf Hansen, Wirtschaftsprüfer und Steuerberater
Tel. +49(0)30 2094-2084
E-Mail ralf.hansen@noerr.com

Dr. Peter Bräutigam, Rechtsanwalt
Tel. +49-(0)89-286 28-145
E-Mail peter.braeutigam@noerr.com

Unsere Standorte

NÖRR STIEFENHOFER LUTZ
Rechtsanwälte Steuerberater Wirtschaftsprüfer • Partnerschaft

Berlin
Charlottenstraße 57
10117 Berlin
Tel. +49 30-20 94 20 00

Dresden
Louis-Braille-Straße 5
01099 Dresden
Tel. +49 351-81 66 00

Düsseldorf
Victoriaplatz 2
40477 Düsseldorf
Tel. +49 211-499 86 0

Frankfurt am Main
Friedrichstraße 2-6
60323 Frankfurt am Main
Tel. +49 69-97 14 77 0

München
Brienner Straße 28
80333 München
Tel. +49 89-28 62 80

New York
Representative Office
375 Park Avenue, Suite 2608
New York, NY 10022
Tel. +12 12-433 13 96

Bratislava
NÖRR STIEFENHOFER LUTZ s.r.o.
AC Diplomat
Palisády 29/A
SK-811 06 Bratislava
Tel. +421-259 10 10 10

Budapest
Rozgonyi Nyalka Gonda
NÖRR STIEFENHOFER LUTZ
Ügyvédi Iroda
Fő utca 14-18.
H-1011 Budapest
Tel. +36 1-224 09 00

Bukarest
Cabinet de Avocat
Zsolt Karl Radnóczy
NÖRR STIEFENHOFER LUTZ
Str. General Constantin
Budişteanu nr. 28 C, sector 1
RO-010775 Bucureşti
Tel. +40 21-3 12 58 88

Moskau
NÖRR STIEFENHOFER LUTZ ooo
Zwetnoj Boulevard 25, Geb. 3
Business Zentrum „Mosenka-2"
127051 Moskau
Russische Föderation
Tel. +70 95-7 99 56 96

Prag
NÖRR STIEFENHOFER LUTZ v.o.s.
Na Příkopě 15
CZ-11000 Praha 1
Tel. +4 20-233 112 111

Warschau
NÖRR STIEFENHOFER LUTZ
Sp. z o.o. Radnóczy Sp.k.
Kancelaria prawna
Al. Armii Ludowej 26
PL-00-609 Warszawa
Tel. +48 22-579 30 60

Die Sozietät

Mehr als 50 Jahre unternehmerisches Denken und eine konsequente Politik der Eigenständigkeit haben uns zu einer bedeutenden Größe im europäischen Rechtsmarkt gemacht. Wir sind international und multidisziplinär aufgestellt, unsere Beratungskompetenz erstreckt sich über alle Bereiche des Wirtschaftsrechts bis hin zu Financial Advice und Consulting Services.

Mit insgesamt elf eigenen Büros und über 300 Berufsträgern sind wir in den wichtigsten Wirtschaftszentren Deutschlands, Mittel- und Osteuropas präsent. In Westeuropa und den Vereinigten Staaten können wir uns auf langjährige Best Friends-Beziehungen verlassen. Außerdem gehören wir Lex Mundi an, dem weltweit führenden Netzwerk unabhängiger Rechtsanwaltkanzleien.

Unternehmen jeder Größe finden bei uns eine exakt auf ihre Bedürfnisse zugeschnittene Full Service-Beratung. Auf vielen Rechtsgebieten und in wichtigen Branchen sind unsere Partner national und international profilierte Experten. Eine eigene Practice Group Prozessrecht und Schiedsgerichtsbarkeit schützt Ihre Interessen auch im Konfliktfall.

Mehr über unsere Sozietät finden Sie im Internet unter **www.noerr.com.**

Stand: Oktober 2005

BERLIN

BRATISLAVA

BUDAPEST

BUKAREST

DRESDEN

DÜSSELDORF

FRANKFURT / M.

MOSKAU

MÜNCHEN

NEW YORK

PRAG

WARSCHAU

NOERR.COM