eBook: IT-Security

Thema: "Mit einem Bein im Gefängnis? – IT-Sicherheit und Haftung"
(Stand: 13.09.2006)

Autor:

Max-Lion Keller
Rechtsanwalt

Tel: +49(0)89- 54 03 56 20
Fax: +49(0)89- 50 58 79

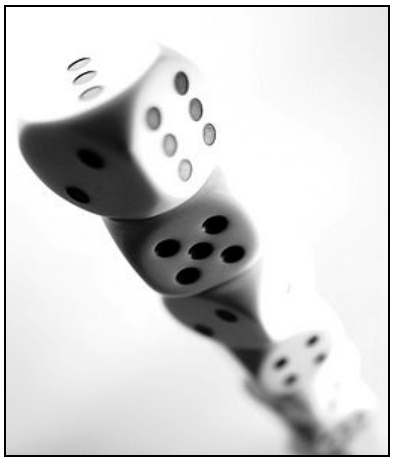
Alter Messeplatz 2
80339 München

E-Mail: M.Keller@IT-Recht-Kanzlei.de
www.IT-Recht-Kanzlei.de

Inhaltsverzeichnis

Kapitel A Einleitung: „IT-**Sicherheit** ist Chefsache“

Gerne wird auf Seminaren, Workshops oder etwa in den Medien das Thema IT-Sicherheit mit folgendendem Spruch eingeleitet: „IT-**Sicherheit ist auch Chefsa**che“.



Nur, der Spruch „IT-Sicherheit ist Chefsache“ kann auch in einem bösartigeren Sinn verstanden werden, nämlich dass **auch** der Chef für die IT-Sicherheit seinen Kopf hinhalten muss. Gerade dieser Aspekt der IT-Sicherheit soll Thema dieses eBooks sein.

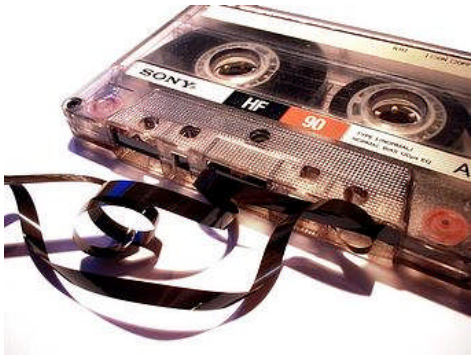
A. Teil 1 „IT-**Sicherheit wird zur Chefsa**che“

Hinsichtlich der Beschäftigung des Chefs mit der IT-Sicherheit seines Betriebes gibt es zwei Möglichkeiten. Entweder kümmert sich die Geschäftsführung bereits präventiv um die Belange der IT-Sicherheit, oder aber die IT-Sicherheit wird spätestens beim Eintritt eines Schadensfalls **zur Chefsache** und zwar in dem Sinne, dass dem Unternehmen wegen mangelnder IT-Sicherheit ein enormer Schaden entsteht und insoweit gar eine mögliche persönliche Haftung der Geschäftsführung bzw. des Vorstandvorsitzes in Frage kommt.

Das Thema „IT-Sicherheit“ geht also keineswegs nur Computer-Spezialisten an, sondern hat absolute unternehmerische Relevanz. Unternehmen, die der IT-Sicherheit nur wenig Beachtung finden, handeln **grob fahrlässig** und werden mittlerweile auch seitens der Gerichte als schlicht „blauäugig“ bezeichnet. Dazu im Folgenden ein recht anschaulicher Fall, den das OLG Hamm erst im Jahre 2003 zu entscheiden hatte. Hier wird besonders deutlich, welche rechtlichen Konsequenzen sich aus einer derartigen **Blauäugigkeit** für ein Unternehmen ergeben.

A. Teil 2 OLG Hamm: Mangelnde Datensicherung bei Unternehmen? → Selber schuld!

1. Sachverhalt: Ein Reiseunternehmen hatte Probleme mit seinem Server und beauftragte einen Computer-Reparaturdienst, nach dem Grund für eine bestimmte Fehlermeldung zu suchen. Der Angestellte des Reparaturdienstes wollte daraufhin eine Festplatte austauschen und erkundigte sich vorher, ob die betreffenden Daten gesichert sei. Dies bejahte das Reiseunternehmen und es kam, wie es kommen musste: Bei der Vorbereitung des Festplattenaustausches kam es zu einem Absturz des Servers mit der Folge, dass zahlreiche Geschäftsdaten gelöscht wurden.



Quelle:www.photocase.com

2. Problemstellung: Das Reiseunternehmen hatte seine Daten noch nicht einmal monatlich gesichert, so dass Teile der Daten tatsächlich unwiederbringlich gelöscht waren. Das Reisebüro verklagte nun den Computer-Reparaturdienst auf Zahlung von Schadensersatz mit der Begründung, dass der Reparaturdienstleister bei den Arbeiten an der Festplatte nicht sachgemäß vorgegangen sei und dabei das System zerstört oder beschädigt habe. Es sei jedenfalls nicht genügend Sorge für eine hinreichende Datensicherung vor diesen Arbeiten getragen worden. Dazu sei der Reparaturdienst aber verpflichtet gewesen.

Das Gericht hatte nun zu entscheiden, in wessen Verantwortungsbereich die Datensicherung fällt.

3. Lösung: Das OLG Hamm (Urteil vom 01.12.2003, 13 U 133/03) fand deutliche Worte:

Das OLG Hamm legte dem Reiseunternehmen zur Last, dass dieses nicht für eine zuverlässige Sicherheitsroutine gesorgt, sondern diese vielmehr grob vernachlässigt habe. So habe der nach dem Absturz festgestellte Stand der Komplettsicherung dem Stand vier Monate vor den Wartungsarbeiten entsprochen! Dies sei „grob fahrlässig, ja blauäugig, so das OLG **Hamm.** Schließlich habe eine Sicherung der Unternehmensdaten „täglich zu erfolgen, eine Vollsicherung mindestens einmal wöchentlich.

Das Gericht legte noch nach: Selbst wenn dem Angestellten eine Pflichtverletzung im Sinne der Wahrnehmung seiner Controllerpflichten vorzuwerfen wäre, bliebe es dabei, dass dem Reiseunternehmen eine Alleinschuld am entstanden Datenverlust und damit am finanziellen Schaden vorzuwerfen wäre.

4. Haftungsproblematik der Beteiligten: Die nun schon vielfach zitierte „Blauäugigkeit“ kann für den jeweiligen IT-Verantwortlichen in einem Unternehmen und unter Umständen auch für die Geschäftsleitung gravierende Folgen haben:

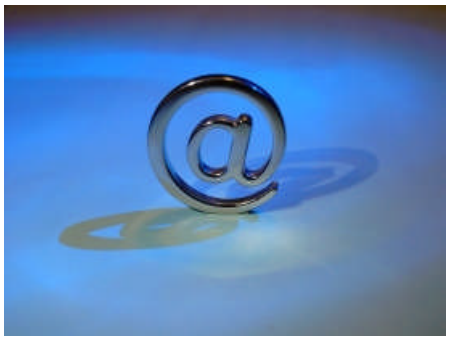
- So ist die Geschäftsleitung nach dem am 27.04.1998 in Kraft getretenen Kontroll- und Transparenzgesetz (KonTraG) verpflichtet, ein System zur frühzeitigen Erkennung von den Fortbestand des Unternehmens bedrohenden Entwicklungen und Risiken zu implementieren (ausführlich dazu unten). Schenkt die Geschäftsleitung der Gefahr einer fehlenden Datensicherung keine Beachtung, so ist in Anbetracht der zu erwartenden Schäden, die sogar eine Insolvenz des Unternehmens auslösen können, auch deren Verhalten als grob fahrlässig zu bezeichnen.

- Natürlich kann sich auch der unmittelbare IT-Verantwortliche aus dem Arbeits- bzw. Anstellungsvertrag haftbar machen. Es muss heutzutage zudem jedem klar sein, dass Pflichtverletzungen im Bereich der IT-Sicherheit arbeitsrechtliche Abmahnungen und im Wiederholungsfall gar Kündigungsfolgen nach sich ziehen können.

5. Fazit: Bei unzureichenden Datensicherungsmaßnahmen spielt es keine Rolle, wie diletantisch etwaige Wartungsarbeiten vorgenommen werden. Das Risiko des Datenverlusts tragen in diesen Fällen ausschließlich derart „blauäugige“ Unternehmen bzw. die jeweiligen Verantwortliche.

Kapitel B Bedeutung der Informationstechnologie für Unternehmen / Bedrohungspotential

Heutzutage sind in der Geschäftswelt nahezu alle denkbaren Prozesse von der Informationstechnologie (IT) abhängig. Man denke nur schon an die Textverarbeitung am Arbeitsplatz, die Buchhaltung, den Logistikbereich oder an die digitalisierten Datenbanken. Es erstaunt daher nicht, dass sich heutzutage in Deutschland so gut wie jedes Unternehmen der Informationstechnologie bedient.



Um dies näher zu veranschaulichen, soll auf die amtliche Statistik des „Statistischen Bundesamtes“ hingewiesen werden die einen Teilaspekt der IT beleuchtet, nämlich die Nutzung des Internet. So ermittelte das „Statistische Bundesamt“ erst im letzten Jahr (2005), dass 94 % aller Unternehmen in Deutschland (mit mindestens 10 Beschäftigten) einen Internetzugang besaßen (vgl. http://www.destatis.de/informationsgesellschaft/) und dabei 59% über eine eigene Website verfügten. Erstaunlich ist dabei nur, dass immer noch die meisten Unternehmen,

nämlich 44 %, die Verbindung zum Internet mittels ISDN herstellten – eine letztlich überkommene Technik.

B. Teil 1 Bedeutung und die Risiken des Internets

Die enge Verzahnung von unternehmerischem Handeln und dem Einsatz von Informationstechnologie hat jedoch auch eine Kehrseite. So haben in so gut wie allen Fällen ernst zu nehmende Ausfälle oder Störungen der IT direkte Auswirkungen auf den jeweiligen unternehmerischen Erfolg.

Quelle: www.photocase.com

Beispiel: Kommt es zu Ausfällen der Produktionssteuerung können vertraglich zugesagte Liefertermine nicht mehr eingehalten werden. **Oder:** Gehen unternehmenseigene Datenbestände verloren, kann dies zur Konsequenz haben, dass die betroffenen Unternehmen schlicht nicht mehr handlungsfähig sind und sowohl einen enormen finanziellen als auch zeitlichen Aufwand für die Datenrettung aufzubringen haben. Dies gelingt darüber hinaus bedauerlicher Weise in vielen Fällen nicht in vollem Umfang.

Gerade das Internet schafft in diesem Zusammenhang eine enorme Gefahrenquelle für Unternehmen. Auch wenn das „Netz der Netze“ mittlerweile für die Wirtschaft so gut wie unentbehrlich geworden ist[1], die Sicherheitsrisiken, denen sich jedes „angeschlossene“ Unternehmen dadurch aussetzt, sind enorm.

So kursiert im Internet etwa die Nachricht, dass für den Fall, dass man einen ungeschützten Computer heutzutage ins WorldWideWeb stelle, dieser statistisch gesehen innerhalb von nur 2 Minuten verseucht sei, ohne freilich, dass man dabei „kritische“ Websites besucht haben müsse. Dies kann jedoch vom Verfasser dieses eBooks nicht bestätigt werden, seine Erfahrungen waren andere…

[1] So enthält das Internet, welches durch den Zusammenschluss Abermillionen Rechner und vieler Tausender Rechnernetze gebildet wird, eine Informationsfülle, die etwa 1.000.000 mal mehr Informationen umfasst, als alle Bibliotheken der Welt zusammengenommen. Für Unternehmen aber weitaus interessanter ist die Tatsache, dass mittlerweile das Internet als neuer Vertriebsweg für nahezu alles, was Gegenstand von Handelsgeschäften sein kann, entdeckt wurde.

B. Teil 2 Exkurs: Selbstversuch des Verfassers

Im Folgenden nun eine Beschreibung des erst kürzlich vorgenommenen Versuchs des Verfassers, eine „frische“ Windows XP Version (Service Pack 1) auf eine neue Festplatte zu installieren und damit anschließend ins Internet zu gelangen. Der Verfasser wurde dabei fast wahnsinnig…

Quelle: www.photocase.com

Installation und Vorbereitung:
Der Verfasser installierte auf einer neuen, bisher unbenutzten Festplatte das Betriebssystem Windows XP Professional (Service Pack 1). Danach installierte er ein kostenlos erhältliches Firewall-Programm[2] sowie ein Antiviren-Schutzprogramm.

Verbindung zum Internet:
Als er nun die Verbindung zum Internet mittels eines DSL 16 anlegte, passierte folgendes:

- Ein paar Sekunden (!) nachdem er den Internet Explorer starte, meldete sein Virenscanner die ersten Trojaner, die sich auf seinem System niedergelassen hätten.

- Kurze Zeit darauf stellte das Firewall-Programm seinen Dienst ein. Es ließ sich daraufhin auch nicht mehr neu starten.

- Der Echtzeitscanner (engl. On-Access Scanner) seines Antivirenprogrammes deaktivierte sich. Der letzte Virus, den der Scanner erkannte, war die exe.Datei des (eigenen)Virenscanners. Diese wurde daraufhin automatisch gelöscht mit der Konsequenz, dass sich das Antiviren-Programm beendete und ab da an nicht mehr startbar war.

- Eine erneute Installation des Virenscanners oder der Firewall scheiterte daran, dass die entsprechenden Installationsprogramme auf einmal „corrupt“ waren - wie sich Windows ausdrückte…

- Der Versuch des Verfassers, eine spezielle Software zum Entfernen von „Würmern“ herunterzuladen scheiterte. Der „Internet Explorer“ weigerte sich, die entsprechende Datei downzuloaden. Der Verfasser nutzte daraufhin den Internet-Browser „Opera“ und es gelang ihm tatsächlich die Software herunterzuladen. Nur, installieren ließ sie sich nicht, da sie anscheinend „corrupt“ war, wie sich Windows äußerte…

[2] Eine Firewall (von engl. firewall [□faɪəwɔ:l] „die Brandwand“) ist ein System aus Software- und Hardwarekomponenten, das den Zugriff zwischen verschiedenen Rechnernetzen beschränkt, um ein Sicherheitskonzept umzusetzen.

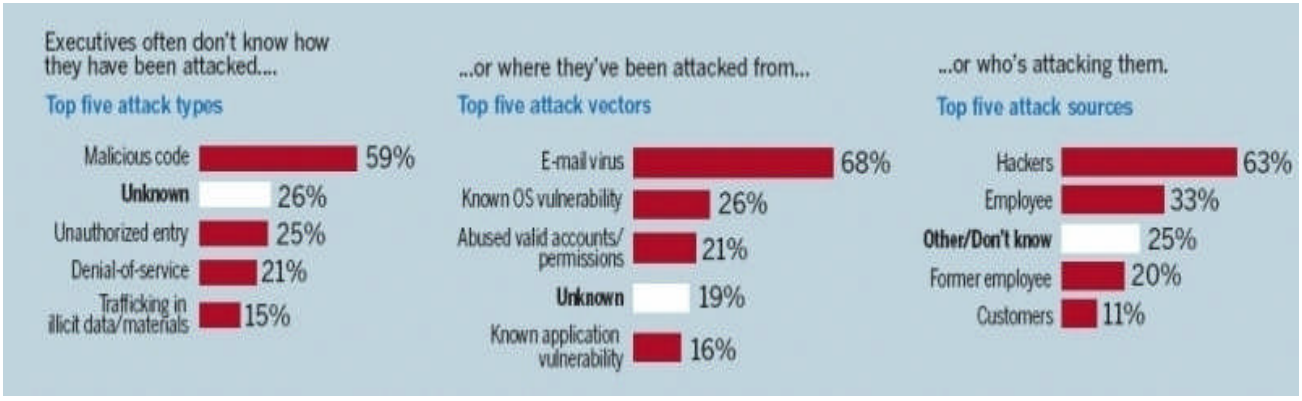
- Das Statusfenster des DSL-Zugangsproblem zeigte höchste permanente Aktivität an und zwar sowohl auf der Download- und der Uploadseite. Dabei war der Verfasser selber nicht im Internet aktiv.

Fazit: Dem Verfasser gelang es auch nach mehreren Versuchen nicht, sich mit dem oben erwähnten Betriebssystem ins Internet einzuloggen. Vielmehr wurde sein Computer bereits Sekunden nach dem Anschluss ans Internet mit schadensstiftender Software aller Art befallen mit der Konsequenz, dass der Verfasser innerhalb kürzester Zeit praktisch „entmündigt" wurde. Sein Rechner agierte wie ferngesteuert bzw. reagierte nicht mehr auf die Befehle des Verfassers.

B. Teil 3 Sicherheitsprobleme nehmen zu!

Das Fachmagazin CIO ermittelte auf Grund einer Befragung[3], dass die Zahl sicherheitsrelevanter Vorfälle in der IT-Welt immer weiter steigt. So stieg etwa die Zahl dieser Vorfälle allein im Jahr 2005 um 22 % gegenüber dem Vorjahr. Insgesamt blieben nur 36 % der befragten Betriebe von Sicherheitsproblemen verschont. Die übrigen Unternehmen registrierten zwischen einem und neun Vorfällen. Dabei gehen die mit Abstand meisten Sicherheitsprobleme (63%) auf das Konto von Hackern, denen es gelang, Viren auf Unternehmensservern zu schleusen. Darüber hinaus wurde jeder dritte Vorfall durch eigene Angestellte verursacht, ein Fünftel davon von ehemaligen Mitarbeitern.

Interessant dabei ist, dass von einem Viertel der Sicherheitsvorfälle die Verantwortlichen selber nicht wussten, wer oder was diese verursacht hatte. Dies wird durch die folgende Grafik verdeutlicht:



Quelle: www.cio.de

[3] http://www.cio.de/_misc/article/print/index.cfm?pid=158&pk=813936&op=prn

B. Teil 4 Begriff der IT-Sicherheit

Angesichts der oben beschriebenen wachsenden Verwundbarkeit und der Gefahr massiver wirtschaftlicher Schäden in Folge von IT-Risiken wäre schon viel gewonnen, wenn sich **flächendeckend** in der Wirtschaft (gerade bei kleinen und mittelgroßen Unternehmen) und auch bei der öffentlichen Hand die Erkenntnis durchsetzen würde, dass der Sicherheit der eigenen IT-Infrastruktur ein hoher Stellenwert einzuräumen ist. Schließlich stellt sie heutzutage die Grundlage jedes unternehmerischen oder verwaltungstechnischen Handelns dar bzw. ist ein integraler Bestandteil jedes Planungs- und Steuerungsprozesses.

IT-Sicherheit bedeutet letztlich nichts anderes, als dass die ständige

- **Verfügbarkeit,**
- die **Vertraulichkeit** und
- die **Unversehrtheit** von Daten bzw. der Informationstechnik

zur Aufrechterhaltung der Geschäftsprozesse und der Abwehr von Schäden, gewährleistet werden muss. Diese drei Begriffe werden so gut wie immer erwähnt, wenn es um das Thema IT-Sicherheit geht. Im Folgenden soll nun geklärt werden, was damit im Einzelnen gemeint ist.

B. Teil 4.1 Verfügbarkeit der Daten

Mit diesem Schlagwort ist der Schutz vor **Informationsverlusten** oder gar dem **Informationsentzug** gemeint. Gerade die ständige Verfügbarkeit der vorhandenen unternehmenseigenen IT-Infrastruktur sowie der zugehörigen Datenbeständen bei Unternehmen wird immer kritischer, da so gut wie kein Geschäftsprozess mehr ohne IT-Unterstützung funktioniert.

Aus diesem Grund hat sich jedes Unternehmen zu vergewissern, ob das jeweils bei ihm eingesetzte IT-System tatsächlich in der Lage ist zu gewährleisten, dass

- das System bei einem **autorisierten Zugriff** zu jedem definierten Zeitpunkt in der gewünschten Art und Weise reagiert.

- das System bei **nicht autorisierten Zugriffen** unter allen Umständen verhindert, dass z.B. unbefugte Dritte von außen auf die Verfügbarkeit Einfluss nehmen.

Hinzu kommt: Immer mehr Unternehmen, gerade im Online-Bereich, sind zu jeder Tages- und Nachtzeit auf den Zugriff der unternehmenseigenen Datenbestände und damit auf eine möglichst störungsfreie IT-Infrastruktur angewiesen. Dies stellt wiederum eine enorme Her-

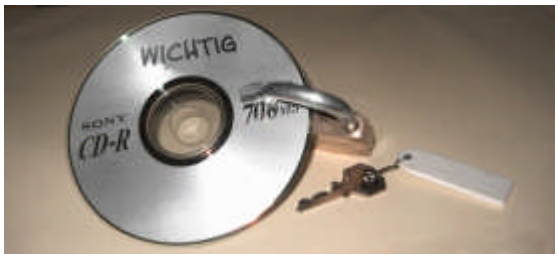
ausforderung an die Wartung der Systeme dar und gerade hier ist es unerlässlich, sich vor möglichen Ausfällen durch Backup-Systeme und einer regelmäßigen Datensicherung abzusichern.

B. Teil 4.2 Unversehrtheit der Daten

Bei der notwendigen „Unversehrtheit der Daten“ geht es darum, dass eine **unautorisierte Informationsveränderung** verhindert wird. Es muss hier sichergestellt werden, dass das eingesetzte IT-System in der Lage ist zu verhindern, dass

- Informationen unerlaubt verändert werden oder
- Angaben, etwa zum Autor, verfälscht werden oder
- etwa der Zeitpunkt der Erstellung manipuliert werden kann.

.



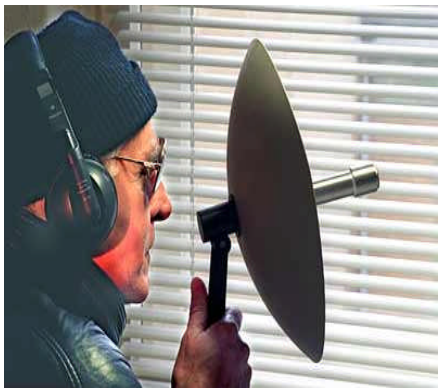
Quelle: www.photocase.com

Es muss sichergestellt sein, dass unternehmenseigene Daten und die sie verarbeitenden Systeme vollständig und unverändert bleiben. Dazu gehört auch, dass eine wie auch immer vorgenommene Veränderung der Daten sofort offensichtlich wird und nachvollgezogen werden kann.

Nur am Rande: Diese Forderungen erfüllt übrigens die gesetzliche "qualifizierte" elektronische Signatur.

B. Teil 4.3 Vertraulichkeit der Daten

Die Schutzrichtung Vertraulichkeit meint dagegen nicht den Schutz vor einer wie auch immer gearteten Datenmanipulation. Vielmehr geht es darum, dass ein unbefugtes Ausspähen unternehmenseigener Daten verhindert werden soll.



Hierbei spielt insbesondere das Thema Wirtschaftsspionage eine große Rolle, etwa

- wenn es um Angriffe von Wettbewerbern mit dem Ziel der Konkurrenzausspähung geht
- oder um fremde Nachrichtendienste, die im Rahmen der Wirtschaftsspionage tätig werden.

Gerade die Wirtschaftsspionage eigentlich befreundeter Staaten sollte nicht unterschätzt werden. So stellt es heutzutage kein Geheimnis mehr dar, dass entsprechende Dienste in Russland und der Ukraine gesetzlich dazu verpflichtet sind, die heimische Wirtschaft zu unterstützen, indem sie den Unternehmen des Heimatlandes Informationen beschaffen, die diesen sonst nicht oder nur mit erheblichem finanziellen Aufwand zugänglich wären. In diesem Zusammenhang soll auch nicht unerwähnt bleiben, dass man in Europa befürchtet, dass etwa die USA mit ihrem Spionagesystem Echelon systematische Wirtschaftsspionage zugunsten von US-Unternehmen betreiben.

Die immer weiter fortschreitende Technik, gerade im Bereich der IT, führt dazu, dass gerade die so genannten „Fernmelde- und elektronischen Aufklärung“ im Rahmen der Wirtschaftsspionage eine immer größere Bedeutung spielt. Darunter hat man sich etwa das Abhören von Telefonen oder das Mitlesen von Fernschreiben, Faxen und anderen Datenströmen[4] vorzustellen. Wirkungsvolle Gegenmaßnahmen lassen sich hier nur treffen, wenn das jeweils eingesetzte IT-System in der Lage ist, relevante und sensible Informationen tatsächlich nur den berechtigten Teilnehmern zugänglich zu machen. Ein unberechtigter Teilnehmer darf in einer automatisierungstechnischen Anlage eben keinen Zugriff auf übertragene oder gespeicherte Daten bekommen. Zumindest muss aber gewährleistet sein, dass er aus den erhaltenen Daten keine Informationen gewinnen kann, was wiederum beispielsweise durch Verschlüsselung erreicht werden kann.

Es darf nicht übersehen werden, dass sich gerade auf der Exklusivität jener Informationen, die als Betriebs- oder Geschäftsgeheimnisse das Resultat von Innovation und Investition darstellen[5], der wirtschaftliche Erfolg so manches Unternehmen gründet.

[4] Weitere Informationen zum Schutz vor Wirtschaftsspionage und Wirtschaftskriminalität, s. etwa http://www.nrw-export.de/export/644.asp.

[5] vgl. hierzu auch Heckmann, IT-Sicherheit, MMR 5/2006.

Kapitel C Rechtliche Anforderungen an die IT-Sicherheit im Unternehmen

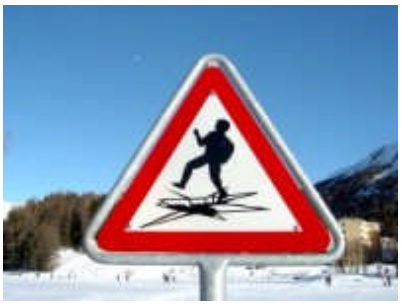
Ein Gesetz, welches sämtliche Regelungen mit Bezug zur IT-Sicherheit zusammenfassen würde, gibt es nicht. Vielmehr hat man sich die entsprechenden gesetzlichen Regelungen mühsam aus verschiedenen gesetzlichen Bestimmungen (vgl. untere Auflistung) zusammenzusuchen.

Quelle: www.photocase.com

Dies wird wohl auch ein Grund mit dafür sein, dass sich viele Unternehmen bzw. deren Geschäftsführung noch immer nicht darüber im klaren sind, dass der Gesetzgeber sie konkret zur Errichtung einer effizienten und vor allem sicheren IT-Infrastruktur verpflichtet hat. Nur wer einen Überblick über die relevanten Gesetze und Verordnungen hat und über ein geeignetes Sicherheitskonzept verfolgt, kann sich vor hier rechtlichen Konsequenzen schützen.

C. Teil 1 Der Rechtsrahmen zur IT-Security

Der Gesetzgeber nimmt die Unternehmen und deren Verantwortliche mit Gesetzen, Verordnungen und Richtlinien in die Pflicht. Dies dient einerseits dem Schutz der eigenen Unternehmensdaten, andererseits müssen überlassene Daten vor unberechtigtem Zugriff geschützt werden - insbesondere personenbezogene Datenbestände.



Quelle: www.photocase.com

So lassen sich insbesondere aus den folgenden gesetzlichen und vertraglichen Regelungen zu Fragen der IT-Sicherheit **unmittelbare Handlungs- wie auch Haftungsverpflichtungen der Geschäftsführung bzw. des Vorstands eines Unternehmens** ableiten:

C. Teil 1.1 Risikofrüherkennung gem. KonTrag

Hierbei muss in aller Kürze auf das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) hingewiesen werden. Dieses Gesetz wurde bereits im Mai 1998 verabschiedet und der Gesetzgeber bezweckte damit die Verbesserung der Kontrolle und der Transparenz in Aktiengesellschaften und auch in größeren GmbHs. Dies wurde regelungstechnisch dadurch erreicht, dass durch das KonTraG das damals bereits vorhandene AktG sowie das GmbH-Gesetz entsprechend ergänzt (§91 II AktG, §116 AktG) bzw. entsprechend angewendet werden (§ 43 GmbHG).

C. Teil 1.1.1 Einrichtung eines Überwachungssystems

Neu bei Inkrafttreten des KonTraG war nun insbesondere, dass der Vorstand einer AG verpflichtet wurde, geeignete Maßnahmen zu frühzeitigen Erkennung von Entwicklungen zu treffen, die den Fortbestand der Gesellschaft konkret gefährden (vgl. § 91 II AktG). Um dies zu gewährleisten bedarf es eines Überwachungssystems, welches in der Lage ist, bei kritischen Situationen auch tatsächlich frühzeitig Alarm zu schlagen.

Quelle: www.photocase.com

C. Teil 1.1.2 Einrichtung eines Risikomanagement

Damit aber nicht genug. Zugleich wird der Geschäftsführung durch Gesetz auferlegt, ein unternehmensweites Risikomanagement zu installieren, welches alle Bedrohungen erfasst, die durch IT-Systeme und deren Einsatz entstehen können. Demnach sind also die Vorstände nicht nur unmittelbar gesetzlich aufgefordert, angemessene Überbwachungsmechanismen einzurichten. Sie haben vielmehr auch präventiv durch entsprechende Informations- und Vorsorgemaßnahmen die Sicherheit der in ihrem Unternehmen verwendeten IT-Systeme zu gewährleisten. Ein solches unternehmerisches Risikomanagement hat man sich wie folgt vorzustellen:

→ **1. Schritt:** Zunächst müssen im Rahmen einer Risikoanalyse alle Risiken im Zusammenhang mit dem Einsatz von unternehmenseigenen IT-Systemen ermittelt und analysiert werden, um dadurch in die Lage versetzt zu werden, das Gesamtrisiko für das Unternehmen einschätzen zu können.

→ **2. Schritt:** Anschließend gilt es ein Sicherheitskonzept zu erstellen, um das ermittelte Risiko basierend auf einer wirksamen Risikoprävention zu reduzieren. Dabei wäre tatsächlich schon viel gewonnen, wenn sich das jeweilige Unternehmen zunächst einmal zum Ziel setzen würde, die bereits eingangs erwähnten Grundwerte der IT-Sicherheit (Verfügbarkeit, Unver-

sertheit, Vertraulichkeit der Daten) sicher zu stellen. Dazu gehört insbesondere eine regelmäßig wie auch häufige Datensicherung, ein wirksamer Sabotage- und Ausfallschutz und natürlich auch der Schutz vor missbräuchlicher IT-Nutzung (durch Mitarbeiter oder Dritte).

→ **3. Schritt:** Dieses Sicherheitskonzept ist dann auch in die Praxis umzusetzen und vor allem penibel einzuhalten.

C. Teil 1.2 Datenschutzrecht

Während die oben genannten Formulierungen für den juristischen Laien teilweise recht allgemein und eher unverbindlich klingen („Sorgfalt eines ordentlichen Geschäftsmannes"), wird das Datenschutzrecht in dieser Hinsicht sehr viel genauer. So verpflichtet § 9 BDSG i.V.m. der Anlage zu § 9 Satz 1 BDSG alle datenverarbeitende Stellen, durch geeignete technische wie auch organisatorische Maßnahmen die Gewährleistung der datenschutzrechtlichen Anforderungen sicherzustellen

C. Teil 1.2.1 Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle

Aus der Anlage zu § 9 Satz 1 BDSG wird deutlich, welche Maßnahmen in diesem Zusammenhang konkret gemeint sind, wobei im Folgenden insbesondere auf die drei wichtigsten Maßnahmen eingegangen werden soll:

- **Zugangskontrolle:** Das datenverarbeitende Unternehmen hat sicherzustellen, dass kein Unbefugter Zutritt zu den Computern hat, auf denen personenbezogene Daten verarbeitet werden Es entspricht der Realität, dass sich PCs meist in normalen Büroräumen befinden, in denen auch ein Publikumsverkehr möglich sein muss und in aller Regel auch keine besonderen Zutrittsregelungen für Besucher oder etwa Gebäude- und Raumreiniger gibt. Schon einfache organisatorische Maßnahmen können hierbei helfen, das Risiko mit einzudämmen. So gehören etwa PCs, die als Server eingesetzt werden, natürlich in einen zugangsgeschützten Extraraum.

- **Zugriffskontrolle:** Das datenverarbeitende Unternehmen hat sicherzustellen, dass die Berechtigten nur auf die Daten zugreifen können, für die sie eine Zugriffsberechtigung haben. Das IT-System muss daher in der Lage sein, differenzierte Zugriffsberechtigungen technisch umzusetzen – etwa durch eine Benutzerkontrolle, die die berechtigten Benutzer identifiziert und auch authentifiziert.

- **Weitergabekontrolle:** Gerade der sog. Weitergabekontrolle (oder auch Datenträgerkontrolle) kommt beim PC-Einsatz eine herausragende Bedeutung zu. So gehört es heute zur Grunderkenntnis der IT-Sicherheit, dass etwa der Umgang mit Disketten, CDs oder sonstigen Speichermedien, die in großen Mengen vorhanden sein können, trotz eines hohen organisatorischen Aufwandes kaum mit hinreichender Sicherheit organisiert werden kann. Daher müssen hier nach Möglichkeit Maßnahmen getroffen werden, die die Verwendung beweglicher Datenträger beschränkt - etwa auf bestimmte Benutzergruppen.

C. Teil 1.2.2 Bestellung eines Datenschutzbeauftragten

Noch vor ein paar Wochen musste jedes private Unternehmen, das personenbezogene Daten automatisiert nutzte und mehr als vier Arbeitnehmer beschäftigte, einen betrieblichen Datenschutzbeauftragten bestellen.

Quelle: www.photocase.com

Angesichts des Umstands, dass heutzutage in nahezu jedem Unternehmen jedenfalls in der IT-Abteilung, im Personalwesen und der Buchhaltung, oft aber auch in den Fachabteilungen über Netzwerke verbundene PCs vorhanden sind und mit personenbezogenen Daten gearbeitet wird, entgingen nur wirklich kleine Unternehmen der Pflicht zur Bestellung des Beauftragten.

Der Gesetzgeber plante nun auch diejenigen Unternehmen, die höchstens neun Personen beschäftigen, zu entlasten. So schuf er das "Erste Gesetz zum Abbau bürokratischer Hemmnisse insbesondere in der mittelständischen Wirtschaft[6]"“ und es kam am 26.08.2006 zu einer entsprechenden Novellierung des Bundesdatenschutzgesetzes mit folgenden Konsequenzen:

- Die Pflicht zur Bestellung von Datenschutzbeauftragten wird auf Unternehmen reduziert, die mindestens 10 (statt bisher 5) mit Personendatenverarbeitung betrauten Personen beschäftigen. Damit entfällt für viele kleine Unternehmen die kostenintensive Bestellung eines betrieblichen Datenschutzbeauftragen[7]. Aber Vorsicht: Auch der Bezugsgegenstand ändert sich, da nunmehr das Gesetz auf **Personen** abhebt. „Personen“ im Gesetzessinn sind dabei alle im Unternehmen tätigen Menschen, also nicht nur, wie zuvor Angestellte, sondern auch z.B. Auszubildende und Geschäftsführer.
- Die erwähnte Anhebung dieses Schwellenwerts gilt nicht nur für die Bestellung eines betrieblichen Datenschutzbeauftragten, sondern auch für die Meldepflichten des Unternehmen.

---

[6] Der kompletten Gesetzestext zum Ersten Gesetz zum Abbau bürokratischer Hemmnisse, insbesondere in der mittelständischen Wirtschaft, ist auf dem Internetportal der IT-Recht Kanzlei (http://www.it-recht-kanzlei.de/?id=gv_Datenschutz) nachzulesen.

[7] Datenschützer wie der Bundesdatenschutzbeauftragte Peter Schaar kritisieren die Neuregelung. Es könne nicht sein, dass nun viele Unternehmen, etwa in den Bereichen des Handel, des Handwerk sowie in freien Berufen, auf internen Datenschutz verzichten könnten, obwohl auch gerade hier der Umfang der gesammelten Daten, etwa in Form von Kundenkarten oder der Nutzung elektronischer Zahlungsverfahren, immer größeren Ausmaß erreiche.

- Besteht eine Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz, ist die Verpflichtung spätestens innerhalb eines Monats nach Aufnahme der betrieblichen Tätigkeit zu erfüllen.
- Von der Gesetzesänderung nicht betroffen ist die Pflicht zur Bestellung eins Datenschutzbeauftragten im Bereich des gewerblichen Adresshandels. Unabhängig von der Anzahl der bei dem jeweiligen Betrieb beschäftigten Personen, muss auch hier weiterhin ein Datenschutzbeauftragter bestellt werden.

C. Teil 1.3 Sonderregelungen

Zum Teil stellen branchenspezifische Regelungen auch strengere Anforderungen als die oben bereits erwähnten Regelungen an die IT-Sicherheit, etwa bei Banken oder Versicherungen. Zudem enthält das Strafgesetzbuch für bestimmte Berufsgruppen, wie Ärzte, Rechtsanwälte oder Angehörige sozialer Berufe Sonderregelungen, die Freiheitsstrafen vorsehen, wenn etwa vertrauliche Angaben von Patienten, Mandanten bzw. Klienten ohne deren ausdrückliche Einwilligung öffentlich gemacht werden (§ 203 StGB).

Quelle: www.photocase.com

Unter Umständen kann somit bereits ein fahrlässiger Umgang mit Informationstechnik diesen Tatbestand erfüllen.

C. Teil 1.4 Vertragliche Regelungen

Selbstverständlich lassen sich auch über vertragliche Regelungen Rechtspflichten im Hinblick auf die IT-Sicherheit begründen. Beispiele dafür können etwa sein:

- **Vertraulichkeitsvereinbarungen (non-disclosure agreement):** Hier geht es zumeist um eine Vereinbarung zwischen einem Unternehmer und einer für den Unternehmer tätig werdenden Person, die ihn vor der Weitergabe vertraulicher Informationen an Dritte schützen soll. Der Unterzeichner stimmt dabei zu, ihm im Rahmen seiner Tätigkeit zugänglich gemachte Daten, Informationen und Wissen (insbesondere Betriebsgeheimnisse wie technologisches oder Prozesswissen) geheim zu halten.

- **Softwarehinterlegungsvereinbarung (Escrow Agent Agreement):** Der Escrow-Agent hat den Quellcode gemäß den zwischen allen Parteien in einem Hinterlegungsvertrag niedergelegten Bestimmungen aufzubewahren. Unter anderem legt dieser Vertrag auch fest, unter welchen Umständen der Quellcode an den Anwender herausgegeben werden muss. Der Escrow-Agent hat hierbei in aller Regel die vertragliche Verpflichtung, den unberechtigten Zugriff auf die hinterlegte Software unter allen Umständen zu verhindern.
- **IT-Outsourcing:** Natürlich besteht auch für IT-Outsourcing Dienstleister die vertragliche Verpflichtung, die Absicherung der verwendeten IT-Systeme sicherzustellen. Dies gilt insbesondere für die Vertraulichkeit der Daten (zu diesem Begriff, B. Teil 4.3.).
-

Kapitel D Mögliche Folgen bei Vernachlässigung der IT-Sicherheit / Adressaten

Die Folgen einer vernachlässigten IT-Sicherheitsinfrastruktur können einem Unternehmen und dessen Verantwortliche teuer zu stehen kommen.

Hinsichtlich der möglichen Konsequenzen ist hierbei im Folgenden zu unterscheiden zwischen

- der zivilrechtlichen Haftung,
- öffentliche-rechtlichen Sanktionen,
- der vertraglichen Haftung und
- sonstigen finanzielle Nachteile.

D. Teil 1 Zivilrechtliche Haftung

D. Teil 1.1 Missachtung der gesetzlichen Verpflichtungen zur IT-Sicherheit nach KonTraG

Im **Aktiengesetz ist** festgelegt, dass eine persönliche Haftung des Vorstand dann in Betracht kommt, wenn er Entwicklungen, die zukünftig ein Risiko für das Unternehmen darstellen könnten, nicht durch ein Risikomanagement überwacht und durch geeignete Maßnahmen vorbeugt (§ 91 Abs. 2 und § 93 Abs. 2 AktG). Nahezu dieselben Anforderungen gelten:

- Für den Geschäftsführer einer GmbH, der „der Sorgfalt eines ordentlichen Geschäftsmannes“ auf zu bringen hat (§ 43 Abs. 1 GmbHG). Diese, zugegebenermaßen eher allgemein gehaltene Formulierung, beinhaltet in der rechtlichen Praxis ganz ähnliche Folgerungen für das Risikomanagement wie für Vorstände nach dem Aktiengesetz.
- Für andere Gesellschaftsformen, wie etwa die Offene Handelsgesellschaft oder die Kommanditgesellschaft. Diese sind nämlich den Kapitalgesellschaften hinsichtlich der Rechtspflichten zur IT-Sicherheit dann gleichgestellt, wenn sie keine natürliche Person als persönlich haftende Gesellschafter haben (vgl. dazu das Kapitalgesellschaften- und Co- Richtlinie-Gesetz, „KapCoRiLiG“).

Kommt die Geschäftsführung oder der Vorstand – als Verantwortliche – der oben beschriebenen Risikovorsorgepflicht nicht nach und entsteht dadurch dem Unternehmen ein finanzieller Schaden, kann dies zu einer persönlichen Haftung der Mitglieder des Vorstands und der Geschäftsführung unter Umständen auch der Aufsichtsratmitglieder (§116 AktG) führen.

In diesem Zusammenhang stellt sich nun die Frage, ob derlei Risiken durch eine Versicherung absicherbar sind?

Dies ist natürlich möglich. Manager können sich in Deutschland gegen gewisse Risiken versichern lassen, etwa wenn es um die Ansprüche ihres Unternehmens ihnen gegenüber geht. Derlei Versicherungen, „directors & officers liabilty insurance“ genannt, umfassen jedoch nur die Haftung aufgrund von IT-Problemen und nur dann wenn dem Manager kein Vorsatz oder etwa eine „wissentliche Pflichtverletzung nachgewiesen werden kann[8].

Beispiel: Ein Manager wurde aufgrund eines unternehmensinternen Expertengutachten ausdrücklich darüber in Kenntnis gesetzt, dass die Verfügbarkeit (zum Begriff, siehe oben B. Teil 4.1) gerade hinsichtlich bestimmter, sensibler Datenbestände nicht gewährleistet sei. Bliebe der Manager nun untätig, wäre ihm damit eine „wissentliche Pflichtverletzung“ im vorgenannten Sinne sicherlich vorwerfbar mit der Konsequenz, dass ein entsprechender Versicherungsschutz erlöschen würde.

[8] Zudem hat der jeweilige Aufsichtsrat den Vorstand dahingehend zu kontrollieren, ob dieser alle erforderlichen Maßnahmen im Rahmen des Risikomanagements getroffen hat oder eben nicht. Auch hier wäre eine persönliche Haftung des Aufsichtsrats für den Fall denkbar, dass er seiner Kontrollpflicht nur unzureichend nachkäme und dadurch ergebliche Schäden eintreten sollten.

D. Teil 1.2 Schadensersatz

Die mangelhafte IT-Sicherheit eines Unternehmens kann auch Schadensersatzansprüche desjenigen Vertragpartners nach sich ziehen, dem durch die Leistungserbringung des Unternehmens konkret bezifferbare Schäden entstanden sind, etwa in Form eines kompletten oder auch nur teilweisen Produktions- oder gar Betriebsausfalles. Dasselbe gilt für den Fall, dass vertrauliche fremde Informationen abhanden gekommen sind. Als Haftungsgrundlage kommen hierbei schuldrechtliche Schadensersatzansprüche in Betracht, gemäß § 280ff. BGB. Gerade in diesem Zusammenhang ist auch § 241 Abs. 2 BGB zu beachten, wonach die Pflicht besteht, auf die Rechte, Rechtsgüter und Interessen des Vertragspartners Rücksicht zu nehmen. Hierzu gehören insbesondere die Beachtung von Schutzpflichten, Aufklärungs- und Beratungspflichten.

D. Teil 1.3 Datenschutzrechtliche Haftung

Die Haftungsrisiken im Bereich des Datenschutzrechts sind enorm, sowohl für das Unternehmen als auch für die Geschäftsführung. So ergibt sich aus § 7 S. 1 BDSG ein verschuldensunabhängiger Schadensersatzanspruch. Diese Vorschrift bestimmt nämlich, dass ein Unternehmen für alle Schäden verschuldensunabhängig (!) und unbegrenzt haftet, die es Dritten durch unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten zufügt.

Darüber hinaus kommen hierbei auch deliktische Ansprüche gem. § 823 BGB in Betracht, da das von § 823 I BGB geschützte Rechtsgut Eigentum eben auch die Integrität von Daten umfasst. Nicht zuletzt wäre hier auch eine Verletzung des allgemeinen Persönlichkeitsrecht zu denken, etwa wenn es um personenbezogene Daten geht.

Beispiel: Ein Hacker kann Kundendaten auslesen, weil keine Firewall eingesetzt wird, vgl. Anlage zu § 9 Satz 1 BDSG Nr. 2.

Dabei ist insbesondere für Unternehmen die in § 7 BDSG **enthaltene Beweislastumkehr** problematisch. Es wird nämlich zunächst immer erst einmal von einem Verschulden des Unternehmers ausgegangen. Bezüglich der Haftung gilt nur für den Fall etwas anderes, in dem das Unternehmen die „gebotene Sorgfalt“ (vgl. § 7 S. 2 BDSG) beachtet hat. Dies ist natürlich dann der Fall, wenn es die oben aufgeführten Verpflichtungen zur Einhaltung des Datenschutzes beachtet und auch umgesetzt hat.

D. Teil 2 Öffentlich-rechtliche Sanktionen

D. Teil 2.1 1. Bußgelder und Freiheitsstrafe

Auch in den Fällen, bei denen noch kein Schaden entstanden ist, kann die mangelnde Umsetzung von IT-Sicherheitsbestimmungen im besonders sensiblen Bereich des Datenschutzes teuer werden. So können in Fällen, in denen personenbezogene Daten nicht ausreichend gemäß den Vorgaben des BDSG geschützt werden, je nach Schwere des Verstoßes

Quelle: www.photocase.com

- Bußgelder (bis zu 250.000 Euro, auch bei fahrlässiger Begehungsweise, § 43 BDSG)
- und sogar Freiheitsstrafen von bis zu zwei Jahren gegen die Verantwortlichen

verhängt werden (vgl. § 44 BDSG).

In solchen Fällen können die IT-Verantwortlichen – gleich ob Vorstand, Geschäftsführer, Behördenleiter, angestellter oder externer IT-Administrator – tatsächlich mit "einem Bein im Gefängnis stehen".

D. Teil 2.2 Exkurs: Wann Unternehmen als Telekommunikationsanbieter-Anbieter gerade stehen…

Es ist erstaunlich aber nur die wenigsten Unternehmen (nämlich ca. 20 %) regeln die private Nutzung von E-Mail und Internet durch ihre Angestellten. So wird in den meisten Unternehmen die private Nutzung der unternehmenseigenen Kommunikationseinrichtungen auch für private Zwecke gestattet bzw. zumindest stillschweigend geduldet. Viele Unternehmen scheinen sich dabei jedoch über die folgende Konsequenz nicht wirklich im Klaren zu sein:

Stellt man den betriebseigenen Internetzugang für betriebsfremde Zwecke zur Verfügung, indem man etwa den Angestellten die private Nutzung des Internet/E-Mailzugangs gestattet, wird das Unternehmen in diesem Fall geschäftsmäßiger Anbieter von Telekommunikationsdiensten. Keine Rolle spielt hierbei, ob die private Nutzung, etwa des Internets, entgeltlich oder unentgeltlich angeboten wird.

Unternehmen, die die private Nutzung des Internet/E-Mailzugangs erlauben unterliegen als Telekommunikations- und Telediensteanbieter folgenden rechtlichen Pflichten:

- Jegliche Überwachung der Inhalte und Verbindungsdaten ist unzulässig und stellt ein Verstoß gegen das Fernmeldegeheimnis dar, welches als Grundrecht nach §10 des Grundgesetzes nicht nur in der Sprachkommunikation sondern auch bei der Daten-

übertragung und der Internet-Nutzung Gültigkeit besitzt. Der nicht legitimierte Eingriff in das Fernmeldegeheimnisses ist nach dem Telekommunikationsgesetz mit einer Geldstrafe oder Freiheitsstrafe bis zu 2 Jahren belegt.

- Alle Inhalts- und Verbindungsdaten, die Auskunft über die an der Internetnutzung oder am Emailverkehr Beteiligten geben könnten, sind durch angemessene technische Vorkehrungen und sonstige Maßnahmen vor Kenntnisnahme zu schützen.

- Die Erhebung von personenbezogenen Daten ist auf ein Mindestmaß zu reduzieren

- Nur soweit zu Abrechnungszwecken erforderlich, ist die Protokollierung der privaten Nutzung überhaupt zulässig. Entfällt dieser Zweck, sind die Daten unverzüglich zu löschen.

D. Teil 2.3 IT-Sicherheit als Obliegenheit des Unternehmens: Nichtberücksichtigung bei der Vergabe öffentlicher Aufträge

Die Einhaltung von IT-Sicherheitsbestimmungen kann auch Auswirkungen auf den Erfolg bei der Bewerbung um öffentlich-rechtliche Aufträge haben, da öffentliche Auftraggeber verstärkt dazu übergehen, bei IT-relevanten Aufträgen auch Nachweise über die IT-Sicherheitsstruktur des Anbieters einzufordern.

Betrifft die Einhaltung der Sicherheitsbestimmungen das anbietende Unternehmen selbst, werden die Einhaltung der geforderten IT-Sicherheitskriterien bei der Eignungsprüfung (Fachkunde, Leistungsfähigkeit und Zuverlässigkeit) gewürdigt. Beziehen sich die geforderten IT-Sicherheitsbestimmungen auf den Inhalt der anzubietenden IT-Leistung, werden die Antworten des Bieters auf die IT-Sicherheitsanforderungen des öffentlichen Auftraggebers im Rahmen der Leistungsbewertung Berücksichtigung finden. Ein Unternehmen, das insofern auf Forderungen der Vergabestelle nicht eingeht, riskiert ohne weiteres, entweder bereits bei der Eignungsprüfung oder bei der Bewertung der von ihm angebotenen IT-Leistung ausgeschlossen zu werden.

Derzeit in der Diskussion ist die Forderung vieler Vergabestellen, IT-Sicherheitsanforderungen zu instrumentalisieren, um ungewünschte Angebote auszuschließen zu können. Hierzu gehört etwa die Forderung, den Quellcode der anzubietenden Software als vermeintliche Voraussetzung für IT-Sicherheit offen zu legen. Anbieter proprietärer Software werden hier nicht anbieten können.

D. Teil 3 Vertragliche Haftung

Verletzt ein Vertragspartner vertragliche Pflichten, die ihm gerade in Bezug auf die IT-Sicherheit auferlegt wurden (Beispielsfälle s.o. unter C. Teil 1.4), treffen ihn die Sanktionen, die der jeweilige Vertragstext für diesen Fall vorhält.

D. Teil 4 Sonstige mittelbare oder unmittelbare finanziellen Nachteile

Die hier vorstellbaren Konsequenzen sind mannigfaltig und reichen von der Herabstufung der Bonität („Basel II“) über den Imageverlust des Unternehmens bis hin zur Erhöhung der Versicherungsbeiträge:

D. Teil 4.1 Basel II: Herabstufung der Bonität

Das Bundeskabinett verabschiedete Mitte Februar dieses Jahres den Gesetzesentwurf zur Umsetzung der Banken- und Kapitaladäquanzrichtlinie, besser bekannt unter dem Namen "Basel II". Dies hat zur Folge, dass auch die Banken und Finanzinstitute in Deutschland ab 2007 gesetzlich verpflichtet sind, die Vorgaben des Basel II Abkommens umzusetzen und insbesondere eine individuelle Bonitätseinschätzung des jeweiligen kreditsuchenden Unternehmen durchführen. Mittels dieser Bonitätseinschätzung kann sodann ermittelt werden, wie hoch die Wahrscheinlichkeit ist, dass der Kredit an die Bank auch wieder zurückgezahlt wird („Ausfallrisiko“). Sollte dabei das Risiko eines Ausfalls als hoch eingestuft werden, wird sich die Bank dies bezahlen lassen indem sie die Bonität des kreditsuchenden Unternehmens herabsetzt und nur ungünstige Kreditkonditionen weitergibt. Im schlechtesten Falle kommt es gar zu einer Weigerung einer Kreditgewährung.

Es ist selbstverständlich, dass in diesem Zusammenhang ein besonderes Augenmerk auf das operationale Risiko "IT-Sicherheit" liegen muss. Bereits in der Einleitung dieses eBooks wurde auf die fundamentale Bedeutung der IT-Infrastruktur für ein jedes Unternehmen eingegangen, da sie in den meisten Fällen unternehmerisches Handeln überhaupt erst ermöglicht. Fallen die IT-Systeme aus, sind in aller Regel die Unternehmen heutzutage nicht mehr handlungsfähig und der Betrieb steht still. Aus diesem Grund werden die Banken sehr genau prüfen, ob der Kreditnehmer zumindest die Grundanforderungen zur IT-Sicherheit (s.o.) durch die Einhaltung bestimmter Sicherheitsvorkehrungen getroffen hat, die ihn vor einem IT-Ausfall schützen.

D. Teil 4.2 Finanzielle Verluste des Unternehmens / Imageverlust /Versicherung

Ausfälle der IT-Infrastrukur können natürlich dem betroffenen Unternehmen auch direkt hohe finanzielle Verluste bescheren, etwa wenn es um einen länger andauernde Ausfall der unternehmenseigenen IT-Infrastruktur geht (Stichwort Datenverlust). Hinzu kann zudem der Imageverlust des Unternehmens kommen, weil etwa grobe Versäumnisse im Bereich des Datenschutzes an die Öffentlichkeit gelangen sollten.

Nur am Rande sei noch erwähnt, dass Defizite im Bereich der IT-Sicherheit dazu führen können, dass die Versicherungen ihre Leistungen kürzen und sich dabei auf ein mögliches Mitverschulden des „blauäugigen“ Unternehmen berufen. In diesem Zusammenhang kann es dann auch leicht zu einer Erhöhung der Versicherungsprämie für zukünftige Fälle kommen.

Kapitel E Wie haben die Verantwortlichen die IT-Sicherheit zu gewährleisten?

Angesichts der oben beschriebenen Sanktionen bei nur mangelhaft umgesetzter IT-Sicherheit stellt sich natürlich für die Unternehmen bzw. die jeweiligen Verantwortlichen die Frage, wie das Haftungsrisiko nach Möglichkeit verringert, ja möglichst ausgeschlossen werden kann. Zumindest für die bisher in diesem Bereich Untätiggebliebenen drängt die Zeit, da Störfälle, die die IT-Sicherheit betreffen, überdurchschnittlich zunehmen:

- So kam es allein im Jahr 2004 bei 80 Prozent aller Unternehmen zu Störfällen, wobei diese hauptursächlich von Hackern, unachtsamen Mitarbeitern und mangelhaft geschultem Personal verursacht wurden.

- Insgesamt verursachten Angriffe auf die IT-Sicherheit in jedem zwölften Zwischenfall einen Totalausfall des Netzwerks und aller Dienste.

- Nur eine Minderheit von etwa 20 Prozent der IT-Verantwortlichen gab an, keinen finanziellen Schaden durch Angriffe auf die Datensicherheit erlitten zu haben.

Zu diesen Ergebnissen kommt die Studie IT-Security 2005 der InformationWeek, die zusammen mit Steria Mummert Consulting ausgewertet wurde.

Das Thema der Einrichtung wirksamer IT-Sicherheitsmechanismen sprengt nun den Rahmen dieses eBooks . Zudem ist hierzu der „Leitfaden IT-Sicherheit“ des „Bundesamt für Sicherheit in der Informationstechnik“ (BSI) kostenlos erhältlich, der einen kompakten Überblick über die wichtigsten organisatorischen, infrastrukturellen und technischen IT-Sicherheitsmaßnahmen gibt. Dieser richtet sich an IT-Verantwortliche und Administratoren in kleinen und mittelständischen Unternehmen sowie an Behörden (zu beziehen unter www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf) und gibt insbesondere 50 goldene Regeln vor, die im Rahmen der IT-Security zu beachten sind.

Nützliche Links zum Thema IT-Security:

http://www.bsi.de/ (Bundesamt für Sicherheit in der Informationstechnik)
http://www.bitkom.de/de/publikationen/38337.aspx (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.)