

## Rechtliche Risiken fehlender IT-Sicherheit

**Verfasser:**

Rechtsanwalt Andreas Göbel  
Fachanwalt für Arbeitsrecht und Familienrecht

Rechtsanwälte Wolff, Göbel und Dreier  
Rechtsanwälte Fachanwälte  
Fleyer Strasse 61  
58097 Hagen  
Telefon: 02331/91490  
Fax: 02331/914914  
Email: [info@ragoebel.de](mailto:info@ragoebel.de)  
[www.ragoebel.de](http://www.ragoebel.de)

sh12271.doc

Sämtliche Rechte vorbehalten. Jedes Kopieren und unerlaubte Verbreiten ohne vorherige schriftliche Zustimmung des Verfassers ist untersagt.

## I. Allgemeines:

Durch das Gesetz über Kontrolle und Transparenz im Betrieb (KonTraG) vom 01.03.1996 sind zum Schutze der Eigentümer (Aktionäre, Gesellschafter) die Sorgfaltspflichten von Aufsichtsrat und GmbH-Geschäftsführer wesentlich verschärft worden. Insbesondere wurde im Aktiengesetz festgeschrieben, dass der Vorstand auch Mechanismen zur Früherkennung und Vermeidung von Risiken einzuführen hat.

Auch wenn nur das Aktiengesetz geändert wurde, gelten die nachstehend dargestellten Pflichten aber auch für den GmbH-Geschäftsführer.

Insoweit formuliert die Gesetzesbegründung eindeutig:

„In das GmbH-Gesetz soll keine entsprechende Regelung aufgenommen werden. Es ist davon auszugehen, dass für Gesellschaften mit beschränkter Haftung je nach ihrer Größe, Komplexität ihrer Struktur usw. **nichts anderes gilt** und die Neuregelung Ausstrahlungswirkung auf den Pflichtenrahmen der Geschäftsführer auch anderer Gesellschaftsformen hat.“

Damit kann also eine Verletzung der nachstehend beschriebenen Pflichten für Geschäftsführer einer GmbH zur Schadensersatzpflicht führen.

„Geschäftsführer haben in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmanns anzuwenden (§ 43 Abs. 1 GmbH Gesetz).“

Bei einer 1998 von Coopers & Lybrand durchgeführten Befragung von 300 Direktoren in Europa ergab sich folgende Reihenfolge den grössten Risiken:

- Marktveränderungen
- Wettbewerb
- Treasury/Wechselkurse
- Regierung/EU
- Umwelt
- Unternehmenskriminalität
- Ansehensverlust

Bei der Frage nach potenziellen Risikofeldern wurden genannt:

- EDV-System-Fehler
- nicht ausreichendes Marktverständnis
- Regierung
- Umwelt
- Kundenservice inadäquat
- Unternehmenskriminalität
- Informationstechnologien und Jahr-2000-Problem

Es kann daher keinem Zweifel unterliegen, dass eine ordnungsgemäße Überwachung und Abschirmung der EDV und der Datenbestände des Unternehmens zu den Kernaufgaben des Geschäftsführers gehört.

Unterlässt der Geschäftsführer es, hier schützende Maßnahmen zu ergreifen, muß er damit rechnen, sich persönlich gegenüber den Gesellschaftern haftbar zu machen.

Die Risiken, die sich durch eine falsch verstandene, falsch eingesetzte oder schlecht geschützte EDV ergeben können, gliedern sich in folgende Bereiche auf:

- Innere Revision
- Grundsätze ordnungsgemäßer Speicherbuchführung (GoBS)
- Unsicherer Vertragsschluß durch Email
- Abmahnungen im e-commerce.
- Vermeidung von Spamming
- Providerhaftung und Haftung für Links
- Datenschutz
- Schutz vor Angriffen von außen
- Schutz vor Angriffen von innen
- Vermeidung der Schädigung Dritter
- Email und Internet im Arbeitsrecht
- Strafrecht
- Verantwortlichkeit der Unternehmensleitung

## **II. Innere Revision und GoBS**

Die betriebswirtschaftliche Maßnahme einer inneren Revision wird von der herrschenden Literatur mittlerweile als absolut notwendig angesehen. Das gleiche gilt für die Einhaltung der Grundsätze der ordnungsgemäßen Speicherbuchführung. Ein insoweit nicht zertifiziertes Finanzbuchhaltungsprogramm muß daher ersetzt werden.

Das benutzte Finanzbuchhaltungsprogramm muss den Vorschriften der §§ 145 –147 der Abgabenordnung sowie den §§ 238, 239, 257 und 261 HGB entsprechen.

Ein solches Programm muss auch gewährleisten, dass die Buchführung aller Geschäftsvorfälle prüfbar bleibt und zwar retrograd und progressiv. Die Prüfung muss dementsprechend vom Beleg ausgehend über Grundaufzeichnungen zu den Konten bis zur Bilanz/Gewinn- und Verlustrechnung und endlich zur Steueranmeldung/Steuererklärung prüfbar sein. Die Prüfung muss jedoch für den Steuerprüfer auch in die andere Richtung, das heißt von der Steuererklärung zurück bis hin zum eigentlichen Beleg nachverfolgbar sein.

Das Programm muss sicherstellen, dass Buchungen (grundsätzlich) nicht verändert werden können. Veränderungen in den Buchungen stellen bereits ein steuerrechtliches Vergehen dar.

Buchungen können ausnahmsweise nur entsprechend § 146 Abs. 4 der Abgabenordnung geändert werden.

Das Programm muss weiterhin eine Verfahrensdokumentation nebst einem internen Kontrollsystem beinhalten, für welche der Buchführungspflichtige verantwortlich ist.

Das heisst, es muss wirksam eingerichtete Kontrollen und Sicherungen geben, nach denen Prüfungsfelder eingegrenzt oder ganz abgehandelt werden können.

Die mittels dieses Systems aufgezeichneten Daten müssen so gespeichert sein, dass sie nicht geändert werden können, das heisst sie dürfen nur auf einem ROM (Read Only Memory) Datenträger gespeichert werden.

Das gesamte datengeschützte Buchhaltungssystem muss eine Dokumentation beinhalten, welche gewährleistet, dass die einzelnen Buchführungsschritte und Verknüpfungen von dem jeweiligen Buchprüfer auch nachvollzogen werden können.

Das heisst, nicht nur die Daten selbst müssen von Buchführungspflichtigen aufbewahrt werden, sondern auch die Verfahrensdokumentation sowie das Programm selbst.

Die Aufbewahrungspflichten für diese Daten und Verfahrensdokumentation betragen minimal sechs Jahre, für Daten mit Belegfunktion und für alle sonstigen Daten mit Grundbuch- oder Kontenfunktion zehn Jahre.

Inhalt der Verfahrensdokumentation ist auch eine klare Regelung dazu, welche Daten in welcher Art und Weise, von wem, wie gespeichert werden.

Es muss für den Buchprüfer klar und kenntlich sein, wer welche Daten oder Belege wie speichert und wo diese registriert und abgelegt sind.

Sind diese Voraussetzungen nicht erfüllt, so handelt der Buchführungspflichtige zumindest ordnungswidrig. In vielen Fällen macht er sich sogar strafbar. Auch die Hardware muss bereit gehalten werden, um dem Prüfer die Gelegenheit zu geben, die Prüfung auch tatsächlich durchzuführen.

### **III. Unsicherer Vertragsschluß durch Email:**

Emails sind keine sicheren Beweismittel für den Abschluß eines Vertrages. Nach fast übereinstimmender Meinung in der Rechtsprechung und in der Literatur beweisen Emails gar nichts, weil sie gefälscht werden können. Auch die Bestätigung des Empfangs einer Email kann gefälscht werden und hat deswegen ebenfalls keinen Beweiswert. Wer deswegen sicher sein will, einen Vertrag geschlossen zu haben, muß dies immer noch in Papierform tun, z.B. indem er sich eine Auftragsbestätigung mit Unterschrift des Kunden zurückfaxen läßt.

### **IV. Abmahnungen beim e-commerce:**

Es rollt eine Abmahnwelle, in der die Betreiber von e-shops auf Korrektur ihrer Shops in Anspruch genommen werden.

Nach einer Untersuchung sind mehr als 90 % aller aktuellen e-shops nicht den rechtlichen Regeln entsprechend erstellt. Jeder von ihnen verstößt gegen mindestens eine Rechtsnorm. Das verwundert auch nicht, weil eine geschlossene Darstellung der Anforderungen an einen fehlerfreien e-shop im Rahmen eines Skriptes des Unterzeichners allein 48 Seiten erfordert.

Die Anforderungen an die Gestaltung des Shops und der damit zusammenhängenden Datenschutzvorschriften machen insgesamt die Einrichtung von mindestens sechs neuen Masken und vier neuen Buttons erforderlich.

Zivilrechtlich enthält das BGB in den §§ 312 b bis e, 355, 356, 357 BGB umfangreiche Vorschriften darüber, wie ein e-commerce-Auftritt gestaltet sein muß. Der Platz reicht hier nicht aus, um dies alles darzulegen. Nur eines sei hervorgehoben:

Entgegen einem weit verbreiteten Vorurteil gilt auch bei b2b eine Mindestanforderung an den e-shop mit folgenden Merkmalen:

- Der Absender einer Bestellung muß eine Mailbestätigung über den Eingang der Bestellung bekommen
- Es muß die technische Möglichkeit der Beseitigung von Eingabefehlern geben
- Die technische Möglichkeit der Beseitigung von Eingabefehlern muß auch erläutert sein, damit man sie betätigen kann
- Die Anbieterkennung, die nachstehend beim Datenschutz beschrieben ist, muß vollständig angegeben sein
- Die Allgemeinen Geschäftsbedingungen und die besonderen Geschäftsbedingungen für den gerade abgeschlossenen Vertrag müssen abrufbar und speicherbar sein
- Aus dem Auftritt muß deutlich werden, wann und wie technisch der Vertrag zustande kommt, welche Sprachen für den Vertragsschluss bereit stehen und welchen Verhaltensregelungen (Schiedsgerichtsordnungen, Handelsrichtlinien, Handelsbräuchen usw.) sich der Verkäufer unterwirft.

## V. Spam:

### 1. Allgemeines:

Es gibt Erhebungen, wonach mittlerweile die Hälfte aller versandten Mails unerbetene Werbemails (Spam) sind. Der Schaden wird auf 12 Milliarden Euro jährlich geschätzt, der hauptsächlich von den Providern getragen wird, die für zusätzlichen Traffic, Filtermaßnahmen und dabei aufgewendete Arbeitszeit zahlen. Das führt zu erheblichen Beeinträchtigungen des Gewerbebetriebes des Providers und jedes anderen Empfängers von Spam.

Spam kann aber auch Viren, Würmer und andere Schadprogramme enthalten. Schließlich kann die Mailbox durch Spam voll werden, so dass erwünschte Mails nicht mehr gespeichert werden können.

Durch diese Spammails können dann weitreichende Schäden eintreten.

## 2. Technik von Spam:

- a) Oft werden sogenannte offene Relay-Server benutzt, das heißt solche, die nicht prüfen, von wem die zu versendende Mail kommt. Es gibt daher bereits Spamfilterprogramme, die jede Mail eines Unternehmens, das einmal eine Mail von einem offenen Relay-Server gesendet hat, als Spam einordnet. Das kann zur Folge haben, dass das Unternehmen immer auf der Blacklist steht und deswegen der Mailverkehr teilweise nicht mehr möglich ist. Das Unternehmen wird dann gesperrt.
- b) Moderne Spammethoden verwenden fremde Domains, was zu einer Rufschädigung desjenigen führt, dessen Domain verwendet wurde. Es führt für diesen auch zu einer Flut von Rücksendungen bis hin zu einer Blockade oder zumindest einer Beeinträchtigung seines Geschäftsbetriebes.

## 3. Rechtslage:

- a) Nach der Rechtsprechung ist das Zusenden von Spam verboten. Es gilt der Grundsatz des Opt-in (Optional dabei), das heißt der Nutzer muss erst durch eine positive Erklärung zu erkennen geben, dass er die Mails haben will. Tut er dies nicht, ist er grundsätzlich erst einmal „out“ und bekommt keine Mails. Begründung sind beim Privatmann das Recht auf Unterlassung jeder Störung gem. § 1004 BGB, für Unternehmen folgt diese aus § 823 BGB in Form des eingerichteten und ausgeübten Gewerbebetriebes.
- b) Eine gesetzliche Grundlage ist jetzt teilweise geschaffen in § 7 Abs. 1 Nr. 3, 4 des Gesetzes gegen unlauteren Wettbewerb (UWG):
  - aa) Danach gilt erst einmal jede Mail als unzumutbare Belästigung, auch bei Gewerbebetrieben, wenn der Empfänger nicht **vorher** dem Empfang zugestimmt hat, z.B. durch Anforderung von Newslettern.
  - bb) Ausnahme: Vorherige Kundenbeziehung. Dann muss die Adresse im Zusammenhang mit dem früheren Verkauf einer Ware oder einer Dienstleistung erlangt worden sein. Die Mailadresse darf dann auch nur für das Angebot **ähnlicher** Waren oder Dienstleistungen verwendet werden. Schließlich darf kein späterer Widerspruch des Kunden vorliegen.

- cc) Nachteil: Gilt nur für Unternehmen, nicht Privatpersonen. Auch kann der Anspruch nur von direkten Mitbewerbern geltend gemacht werden und nicht von Unternehmen, die keine Mitbewerber sind. Erhält also ein Softwarehaus eine unerlaubte Mail einer Reifenfirma, ist dies nicht gem. § 7 Abs. 1 Nr. 3, 4 UWG abmahnfähig, sondern allenfalls als Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb gem. § 823 BGB zu sehen.

#### 4. E-Cards:

Auch wer elektronische Karten anbietet, kann bereits als Störer im Sinne der §§ 1004, 823 BGB in Anspruch genommen werden (OLG München, MMR 04, 324 für politische Parteien). Die Missbrauchsmöglichkeit muss der Anbieter der E-Cards ggf. auch durch Einstellung der Dienste unterbinden.

#### 5. Subdomains:

Der Unterlassungsanspruch richtet sich auch gegen den Vermieter von Subdomains (Landgericht Leipzig, Urteil 13.11.2003, Aktenzeichen 12 S 2595/03; jurPC Webdoc 66/04).

#### 6. Spam für 0190-Nummern:

Hier gilt die Sondernorm des § 13 a TKV. Danach muss der Anbieter der Telekommunikationsleistung, also der Provider des Spammers den Spamer darauf hinweisen, dass er keine gesetzeswidrige Werbung ausführen darf.

Hat der Provider gesicherte Kenntnis von wiederholten oder schwerwiegenden Verstößen, muss er seinen Kunden abmahnen und, wenn er das Handeln fortsetzt, sperren.

Gesicherte Kenntnis hat der Provider, wenn ihm wiederholt Verstöße unter Angabe einzelner Rufnummern bekannt gegeben werden (Landgericht Köln, MMR 2003, 676).

#### 7. Ansprüche des Providers gegen den Spamer bei unberechtigter Nutzung:

- a) Anspruch auf Unterlassung und Schadenersatz gem. § 823 BGB:

Voraussetzung: Eine Blockade oder zumindest eine Fehlfunktion seiner Anlage z.B. durch erhebliche Rückmails.

- b) § 823 BGB wegen Eingriff in den Gewerbebetrieb.  
c) § 826 BGB wegen sittenwidriger vorsätzlicher Schädigung – wird nie vorliegen, weil ein Vorsatz nicht gegeben ist.  
d) § 823 Abs. 2 in Verbindung mit Straftatbeständen wie Erschleichen von Leistungen - § 265 a StGB, Datenveränderung-

§ 303 a StGB, Computersabotage - § 303 b StGB, Störung von Telekommunikationsanlagen - § 317 StGB.

Die Möglichkeiten des Providers auf Schadenersatz sind daher nur dann gegeben, wenn es zu erheblichen Beeinträchtigungen beim Provider kommt.

#### 8. Missbrauch fremder Domains und falsche Adressangabe:

Spamer verschicken ihre Mails immer öfter unter Angabe fremder Domains und fremder Absenderadresse.

Damit unterläuft der Spamer den Filterschutz von normalen Programmen. Dagegen ist juristisch kaum etwas zu machen, den:

- a) Häufig sitzen die Täter und die Server im Ausland.
- b) Wegen der Verwendung fremder Domains ist der Urheber häufig überhaupt nicht identifizierbar.
- c) Computersabotage, § 303 b StGB kann Anspruchsgrundlage sein, wenn der Server zusammenbricht. Bricht er nicht zusammen, ist der Tatbestand nicht erfüllt.
- d) § 143 Markengesetz ist der Straftatbestand, der nur bei Wettbewerbsverletzungen gilt. Dann müsste die Verwendung der fremden Domain vorsätzlich in **verwechslungsfähiger Absicht** erfolgt sein. Das will der Absender aber gerade nicht. Er will nicht verwechselt werden mit dem Absender; er will den Anschein erwecken, als habe der Absender die Mail geschickt.

#### 9. Technische Gegenmaßnahmen:

- a) Abweisung von Mails aus offenen Relays.
- b) Blockieren von Adressen, von denen Spam kam (Blacklist).
- c) Filtern nach Spam-Wahrscheinlichkeit.

#### 10. Rechtliche Zulässigkeit von Filtern, Löschen, Blockieren und Umleiten:

Grundsätzlich gilt, dass hier zwischen den Belangen der betroffenen Nutzer und dem Schutzbedürfnis des Betreibers der Anlage abzuwägen ist.

Rahmen ist insoweit immer der Schutzzweck. Geht es um Virenabwehr, soll die gesamte EDV-Anlage geschützt werden. Dann ist der Rahmen weiter gesteckt als lediglich bei dem Wunsch, unangenehme Werbung (Spam) zu unterbinden.

Bei der Beurteilung der Rechtmäßigkeit einer Maßnahme, das heißt der Abwägung der betroffenen Belange sind schließlich die betroffenen Rechte der Parteien zu berücksichtigen, insbesondere das Recht auf informationelle Selbstbestimmung des Nutzers, die Wissenschaftsfreiheit und das Telekommunikationsgeheimnis.

### 10.1 Blockieren:

Das generelle Blockieren ist bedenklich, weil

- a) der Nutzer ein Interesse am Erhalt auch von unerwünschter Werbung haben kann.
- b) das generelle Blockieren auch seriöse Mitteilungen betreffen kann.
- c) der Provider vertraglich verpflichtet ist, alle Mails weiterzuleiten.
- d) ein Eingriff in das Telekommunikationsgeheimnis gem. § 206 Abs. 2 Nr. 2 Strafgesetzbuch vorliegen kann, wenn private Nutzung erlaubt ist, und
- e) Datenunterdrückung gem. § 303 a Abs. 1 Alternative 2 StGB vorliegt.

Das gänzliche Blockieren ist daher unzulässig.

### 10.2 Filtern:

#### 10.2.1 Vorgang:

Die Absenderangabe (Header) wird auf spezielle Merkmale durchsucht. Nachteil: Dieses Verfahren ist einfach zu unterlaufen und führt auch zum Ausschluss erwünschter Mails. So ist eine Vorlage zum Jugendschutz im britischen Unterhaus nicht weitergeleitet worden, weil das Wort „Sex“ darin vorkam.

10.2.2 Das Filtern ist auch rechtlich unzulässig, weil dabei der Inhalt geprüft wird und deswegen das Telekommunikationsgeheimnis verletzt wird. Das ist nur anders, wenn von den Schutzgegenständen des Telekommunikationsgeheimnisses keine Kenntnis genommen wird, nämlich Absender, Empfänger und Verbindungsdaten, das heißt Umfang der Nachricht, Dauer, Zeitpunkt usw. **Zulässig** ist daher einzig ein automatisiertes Verfahren, bei dem ohne Kenntnisnahme auch nur des Administrators die Mail auf etwaige Spam-Kriterien durchsucht wird, der Mail ein Punktesystem zugeordnet wird, aus der sich eine Spam-Wahrscheinlichkeit ergibt und dies an den Nutzer weitergeleitet wird. Der kann dann entscheiden, ob er die Mail öffnet oder nicht. Nur in diesem Fall wird nämlich von der Nachricht nichts unterdrückt. Der Header wird vielmehr nur um die Spam-Wahrscheinlichkeit ergänzt. Das ist zulässig.

### 10.3 Weitere Bearbeitung der Spam-Mail:

Auf jeden Fall ist die weitere Bearbeitung nur mit Zustimmung des Nutzers zulässig. Auch ein Filtern nach Stichwörtern kann hier erst mit vorheriger

Zustimmung und Definition durch den Nutzer selbst erfolgen. Denn beim Filtern wird die Mail, sobald eines der Stichwörter gefunden wird, ja sofort gelöscht oder zurückgeschickt.

Nur wenn der Nutzer selbst entscheiden kann, ob gespeichert oder gelöscht wird, sind diese Vorgänge zulässig.

## **VI. Haftung für Links:**

Die im früheren § 6 Teledienstegesetz (TDG) geregelte Verantwortlichkeit für Links dahingehend, dass man die verlinkte Seite nur bei Verlinkung überprüfen mußte und danach darauf vertrauen durfte, dass der Inhalt „sauber“ bleibt ist vom Gesetzgeber absichtlich gestrichen worden. Es gelten daher nur noch die allgemeinen Gesetze. Das Oberlandesgericht München hat daraus bereits eine allgemeine Verkehrssicherungspflicht abgeleitet mit der Folge, dass man angeblich regelmässig überprüfen muss, ob sich auf den verlinkten Seiten etwas geändert hat.

Schließlich muss man immer noch alle geltenden Gesetze beachten, die neben den Strafgesetzen gelten.

Danach kann man z.B. immer noch Verletzungen von Markenrechten, Wettbewerbsrecht, Urheberrecht oder Persönlichkeitsrecht hervorrufen. Wer z. B. auf eine eine Person diskriminierende Seite linkt, diskriminiert selbst diese Person. Wer als Gebrauchtwagenhändler auf die Seite von BMW verlinkt, gibt sich den Anschein, als er arbeite er mit dieser Firma zusammen und kann deswegen von BMW gem. §§ 1, 3 UWG wegen Schmarotzens abgemahnt werden. Das gleiche gilt für die Verletzung des Logos.

Wer schließlich auf urheberrechtsgeschützte Seiten verweist und damit dem Anwender die Möglichkeit gibt oder zumindest nahelegt, dies urheberrechtswidrig zu kopieren, ist Mittäter, zumindest aber Anstifter einer Urheberrechtsverletzung.

## **VII. Datenschutz**

Verstößt man gegen die Vorschriften des Datenschutzes muß man mit Bußgeldern bis zu 250.000,00 € rechnen. Unterläßt man die notwendige Anbieterkennung, das heißt die Angabe von Gesellschaftsform, Namen und Vornamen des Geschäftsführers, Adresse, Telefonnummer, Faxnummer, Email Adresse, Handelsregisternummer und Umsatzsteueridentifikationsnummer riskiert man Abmahnungen, die üblicherweise an Anwaltsgebühren 600,00 € bis 1.000,00 € kosten.

Es sollen allerdings das Weglassen von Umsatzsteueridentifikationsnummer und Handelsregisternummer nach einigen Urteil nicht abmahnfähig sein. Die Entwicklung bleibt abzuwarten.

Ferner muss jedes Unternehmen, bei dem in der Regel fünf Arbeitnehmer mit der Verarbeitung personenbezogener Daten in Berührung kommen, einen Datenschutzbeauftragten benennen.

Wir das nicht eingehalten, drohen ebenfalls Bußgelder bis 25.000,00 €.

Obendrein muss man danach die Kosten für den Datenschutzbeauftragten und seine Ausbildung dann doch noch ausgeben. Es empfiehlt sich daher, dies unverzüglich sofort zu tun. Insoweit sei darauf hingewiesen, dass öffentliche Ausschreibungen mittlerweile darauf abstellen, ob die Anbieter die Datenschutzvorschriften einhalten.

In Schleswig-Holstein werden mittlerweile Anbieter bevorzugt, die darüber hinaus auch noch ein Gütesiegel im Datenschutz erworben haben.

Dieses Verwaltungshandeln gibt es zur Zeit nur in Schleswig-Holstein. Auch das Gütesiegel kann man zur Zeit nur beim Datenschutzzentrum in Schleswig-Holstein erwerben. In Kürze wird dies aber bundesweit möglich sein.

Will man die Datenschutzvorschriften im Bezug auf den e-commerce einhalten, schreibt dies allein die konkrete Umgestaltung eines Web-Auftritts und die Einrichtung von mindestens drei zusätzlichen Belehrungen und mindestens drei zusätzlichen Abruf-Buttons voraus.

Auch hier besteht Handlungsbedarf, um Abmahnungen zu vermeiden.

#### **VIII. Schutz vor Angriffen von außen:**

Immer neue Viren halten den Schutz einer EDV-Anlage vor Angriffen von Außen ständig in der Diskussion.

Datenbestände werden zerstört, die üblicherweise nur mit erheblichem finanziellen Aufwand und manchmal gar nicht wieder hergestellt werden können. Der Verlust einer Kundenkartei, des Auftragsbestandes oder des Lagerbestandes kann verheerende Folgen für ein Unternehmen haben. Es unterliegt daher keinen Zweifeln, dass die Einführung und Kontrolle eines ordnungsgemäßen Antivirenprogramms zu den selbstverständlichen Pflichten eines Geschäftsführers gehört.

Das gleiche gilt für den Schutz des Unternehmens vor Zugriffen Dritter mittels einer Firewall.

Einfache, im Internet vorhandene Programme ermöglichen es, innerhalb von Sekunden die EDV-Struktur fremder Unternehmen abzubilden.

#### **IX. Schutz vor Angriffen von innen:**

80 % aller Angriffe gegen Datenbestände eines Unternehmens stammen aber nach gesicherter wissenschaftlicher Erkenntnis von Mitarbeitern des Unternehmens selbst. Der bereits gekündigte, verbitterte Mitarbeiter hinterläßt ein „Abschiedsgeschenk“, das das Unternehmen in größte Schwierigkeiten stürzen kann. Auch hier ist es notwendig, interne

Schutzmaßnahmen wie interne Firewalls und Zugriffsbeschränkungen zu ergreifen, vielleicht aber auch die sofortige Entfernung gekündigter Arbeitnehmer von gefahrbelasteten Arbeitsplätzen durchzusetzen.

Das setzt eine Analyse der betrieblichen Verhältnisse voraus und eine Entscheidung, wer auf welche Daten zugreifen kann. Gleichzeitig ist dabei Disziplin der einzelnen Mitarbeiter verlangt, nämlich ihr Passwort wirklich geheim zu halten, den Rechner herunterzufahren, wenn man den Arbeitsplatz verläßt usw.

#### **X. Vermeidung der Schädigung Dritter:**

Versendet ein Mitarbeiter eines Unternehmens eine virenverseuchte Email, und zerstört der Virus bei dem Geschäftspartner, an den die Email gerichtet war, Datenbestände, kommt möglicherweise eine Haftung des absendenden Unternehmens in Betracht. Es handelt sich nämlich um eine Zerstörung von Eigentum (Daten) des Empfängers. Der Absender haftet gem. § 823 BGB dafür, wenn dies vorhersehbar und vermeidbar war.

Eine Vorhersehbarkeit wird von der Rechtsprechung ohne weiteres bejaht, weil jeder damit rechnen muß, dass Viren auch auf seinem Rechner vorhanden sind. Damit kommt es allein auf die Vermeidbarkeit an. Das wiederum setzt voraus, dass man ein Antivirenprogramm betreibt, das sich auch in den nach dem Stand der Technik üblichen Zeiten über aktuelle Viren informiert und sich dagegen immun macht. Auch hier gehört deswegen die Anschaffung eines entsprechenden Systems zu den selbstverständlichen Pflichten des Geschäftsführers.

Zusätzlich gehören Anweisungen an die Mitarbeiter, z.B. Emails fremder Absender oder Emails ohne Text und nur mit Attachment nicht zu öffnen oder weiterzuleiten sondern dem Vorgesetzten zu melden, zu den selbstverständlichen Pflichten eines Geschäftsführers. Die Pflicht, das Unternehmen intern ausreichend zu organisieren, tritt damit zwingend neben die Pflicht zur Anschaffung der schützenden Technik.

Schließlich ist auch im Geschäftsverkehr die Nutzung des Internet geeignet, Schäden für das Unternehmen hervorzurufen:

Es ist auch überhaupt nicht einzusehen, warum alle Mitarbeiter berechtigt seien sollen, unkontrolliert Emails zu empfangen, zu versenden und im Internet zu surfen. Eine konkrete Richtlinie könnte das Verhalten im Netz regeln.

Ein Entwurf, wie eine solche Richtlinie aussehen sollte, ist diesem Skript beigelegt.

#### **XI. Email und Internet im Arbeitsrecht:**

11. Ob das Scannen nach Viren und anderen Schadprogrammen etc. rechtlich möglich ist, hängt von einer Interessenabwägung ab. Die gegeneinander abzuwägenden Interessen sind folgende:

- Datensicherheit und Schutz vor Abstürzen, Ablauf des Betriebes,

- Schutz personenbezogener Daten, Telekommunikationsgeheimnis (besonders bei Mailboxes gem. § 89 TKG),
- Recht zur informationellen Selbstbestimmung und Fernmeldegeheimnis,
- Wissenschaftsfreiheit

#### 12. Abwägung:

Grundsatz: Jegliche Kenntnisnahme von Inhalt und Verbindungsdaten ist verboten.

Das gilt immer, wenn Privatnutzung von Internet und Email am Arbeitsplatz erlaubt ist. Das gilt also auch dann, wenn private und geschäftliche Nutzung nicht getrennt sind oder getrennt werden können. Denn dann könnte ja eine private Nachricht erfasst sein.

Trennungsmöglichkeiten: Getrennte Accounts oder Privatnutzung über Freemail-Dienste.

Verletzt man vorstehenden Grundsatz, von Inhalt und Verbindungsdaten keine Kenntnis zu nehmen, verstößt man gegen das Telekommunikationsgeheimnis und macht sich strafbar gem. § 206 Abs. 2 Alternative 2 StGB.

Bereits der Zugriff auf Logdateien des Virenschanners ist unzulässig.

Weiter erschwert wird das Vorgehen in diesem Bereich dadurch, dass ggf. die Zustimmung des Betriebsrates/Personalrates eingeholt werden muss. Der kann allerdings den Zugriff auf private Daten nicht gestatten, weil das ein höchst persönliches Recht des einzelnen Arbeitnehmers ist.

#### 13. Scanning:

Auch hier ist das Telekommunikationsgeheimnis zu berücksichtigen. Danach ist das Scannen nur zulässig, wenn es automatisiert erfolgt und selbst der Administrator keine Kenntnis **vom Kontrollvorgang** und **den Kontrollergebnissen** erhält.

Auch hier gilt, dass nur nach bekannten Viren-Signaturen gesucht werden darf, nicht aber nach frei wählbaren Stichwörtern. Denn dann würde ja die Mail inhaltlich untersucht. Das ist bei privaten Mails grundsätzlich unzulässig und verletzt das Telekommunikationsgeheimnis. Auch bei geschäftlichen Mails soll das Inhalts-scanning nach Stichwörtern unzulässig sein, weil es sich um eine unzulässige Verhaltens- und Leistungskontrolle handeln soll (Hanau/Hoeren, private Internetnutzung durch Arbeitnehmer, 2003, Seite 66, Bundesbeauftragter für Datenschutz, 19. Tätigkeitsbericht 2001/2002, Seite 74).

Diese Auffassung teilt der Verfasser nicht. Zumindest dürfte ein überwiegendes Interesse des Arbeitgebers am Schutz vor Viren das Interesse des geschäftlich handelnden Arbeitnehmers bezüglich einer, in seltenen Fällen eintretenden Verhaltens- oder Leistungskontrolle überwiegen. Denn einen Virus kann man sich alle paar Wochen einfangen, ein einmal unterlassenes Scannen von Emails kann jedoch zu enormen Schäden in der Firma des Empfängers führen. Wägt man diese Interessen gegeneinander ab, stellt die Erhebung dieser Daten daher keine systematische Überprüfung dar, die Rückschlüsse auf das Verhalten und/oder die Leistung des Arbeitnehmers zulässt.

Insgesamt bedarf beim Scannen jeglicher Kenntnisnahme von Absender, Empfänger, Dauer der Nachricht, Inhalt der Nachricht und Zeitpunkt der vorherigen Einwilligung des Nutzers.

Technischer Hinweis: Im übrigen kann der zentrale Virenskan auch nicht jeden Virus ausschalten. Ist die Mail verschlüsselt, kann der Virus erst am Arbeitsplatz des Empfängers der verschlüsselten Mail geprüft und erkannt werden.

#### 14. Löschen von Mails bzw. Mailanhängen:

Grundsätzlich dürfen dem Benutzer eines Mailedienstes keinerlei Mails, und daher erst einmal keine verseuchten Emails, vorenthalten werden. Die zur Zeit herrschende Meinung (die Meinungsbildung dauert an) spricht sich aber dafür aus, dass virenbehaftete Mails nicht zugestellt werden müssen (Rieß in Rosnagel, Recht der Multimedienetze, Stand Juni 2003, Teil 6.4, Randnummer 35; die Datenschutzbeauftragten des Bundes und der Länder (Orientierungshilfe der 63. Konferenz der Datenschutzbeauftragten, Nrn. II i III 2c; Bundesdatenschutzbeauftragter, datenschutzrechtliche Grundsätze bei der dienstlichen/privaten Internet- und Email-Nutzung am Arbeitsplatz, Stand März 2003, Nr. 2.4 – <http://www.bfd.bund.de/information/Leitfaden.pdf>.)

Danach sollen insbesondere html-Seiten als Mail-body, Dateien mit den Erweiterungen \*.exe, \*.bat, \*.com oder gepackte Dateien wie \*.zip, \*.arj, \*.lha gelöscht werden dürfen.

Auch dieses Vorgehen muss aber den Mailempfängern vor der Löschung bekannt gegeben werden, damit die widersprechen können. Vor einer rechtlichen Regelungen durch die Gerichte wird daher immer empfohlen, den Nutzer vor dem Löschen mit einzubeziehen, damit man sich nicht eines strafbaren Verstoßes gegen das Fernmeldegeheimnis (§ 206 Abs. 2 Nr. 2 StGB) oder einer strafbaren Datenveränderung (303 a StGB) schuldig macht.

#### 15. Verhältnismäßigkeit:

Nach dem Grundsatz der Verhältnismäßigkeit muss auch bei Maßnahmen der Datensicherheit immer das am wenigsten einschneidende Mittel gewählt werden.

Deswegen dürfte es unzulässig sein, dem Adressaten eine virenbehaftete Mail nur manuell weiterzuleiten. Denn dann muss der Administrator den Header und damit den Absender zur Kenntnis nehmen. Damit verstößt man gegen das Telekommunikationsgeheimnis.

### **Eine mögliche Alternative stellt die sogenannte Quarantänelösung dar:**

Die virenverseuchten Mails werden zunächst in einem gesonderten Ordner abgelegt. Darüber wird der Adressat informiert sowie darüber, wie die Mail für ihn zugänglich ist.

Sein weiterer Zugriff kann dann durch Einsatz eines lokalen Virenschanners oder durch Haftungsregelungen arbeitsrechtlicher Art geregelt werden. Vorteil ist, dass dieses Verfahren ausschließlich automatisch abläuft und daher datenschutzrechtlich unbedenklich ist, weil auch der Administrator keine Kenntnis von Header oder Inhalt nimmt. Außerdem hat es der Nutzer selbst in der Hand, zu entscheiden, ob er abrufen oder nicht. Er trägt daher auch die Haftung.

Ausreichend dürfte es auch sein, dem Nutzer die Möglichkeit zu geben, im Voraus in einem benutzerspezifischen Profil festzulegen, wie er mit virenbehafteten Emails umzugehen wünscht, ob also entsprechende Emails gelöscht, gesäubert oder ganz normal zugestellt werden sollen. Auch hier kann die Zustellung vom Einsatz eines lokalen Antiviren-Programms oder der Übernahme der Haftung abhängig gemacht werden.

Ist eine der vorgenannten Möglichkeiten ergriffen worden, oder ist die Zustimmung aller Nutzer zum Virenschanning und zum Filtern eingeholt worden, steht der Überprüfung von Mails und der Abwehr von Spam und Viren nichts mehr im Wege.

## **XII. Strafrecht:**

Eine Darstellung der Verantwortlichkeit des Geschäftsführers wäre nicht vollständig, wenn man nicht auch die strafrechtliche Verantwortung erörtern würde.

Dazu hat der Bundesgerichtshof in der „Erdal-Entscheidung“ eine 4-Stufen-Theorie entwickelt, die die Handlungspflichten des Geschäftsführers herausarbeitet.

Grundlage der Entscheidung war, dass die Firma Erdal ein Lederspray herausgegeben hatte, von dem bekannt geworden war, dass es Gesundheitsschäden verursachen sollte. Die insgesamt sechs Geschäftsführer der Firma hielten eine Besprechung ab, in der sich zwei Geschäftsführer darüber aussprachen, das Produkt vom Markt zu nehmen.

Die anderen vier setzten sich mit ihrer Auffassung durch, dass es ausreiche, einen Aufkleber aufzubringen, wonach dem Kunden geraten wurde, das Spray nur mit einem ausreichenden Abstand von 30 cm vom Körper einzusetzen.

In der Folgezeit konnten geschädigte Kunden nachweisen, dass ihre Schädigungen auf den Gebrauch des Sprays zurückzuführen waren. Sie erstatteten Strafanzeige wegen Körperverletzung. Der Staatsanwalt erhob Anklage. Alle sechs Geschäftsführer und nicht nur die vier, die die Mehrheit ausgemacht hatten, wurden wegen Körperverletzung vom Bundesgerichtshof in letzter Instanz rechtskräftig verurteilt.

Zur Begründung führte der Bundesgerichtshof aus, dass die Verantwortlichkeit eines Geschäftsführers im strafrechtlichen Bereich hoch sei. Er könne sich nicht hinter der Organisation seiner Firma oder anderen Mitarbeitern verstecken. Damit ein Geschäftsführer sich nicht strafbar macht, muss er vielmehr folgende vier Schritte einhalten:

1. Er muss gegen die beabsichtigte Maßnahme stimmen.
2. Er muss darauf bestehen, dass der Beschluss im Protokoll mit den Mehrheitsentscheidungen aufgenommen wird.
3. Wird der nach seiner Auffassung unzulässige Beschluss umgesetzt, muss er bei den Gesellschaftern vorstellig werden und auf eine Anweisung an die Geschäftsführer dringen, diesen Beschluss nicht auszuführen.
4. Entsprechen die Gesellschafter dem nicht, muss der Geschäftsführer **sein Geschäftsführeramt niederlegen und den Vertrag kündigen**. Nur durch diese Handlungen kann der Geschäftsführer erreichen, dass er sich nicht strafbar macht.

Bleibt er z. B. in der Firma, obwohl er den Gesellschaftern Vorhaltungen gemacht hat, führt er ja selbst wieder als Organ der GmbH die Beschlüsse aus. Dann kann es ihm nicht zur Straffreiheit verhelfen, dass er vorher dagegen gestimmt hat, weil sein späteres Verhalten, nämlich das Verbleiben als Geschäftsführer und Umsetzen dieser Beschlüsse wiederum strafrechtliche Relevanz besitzt.

### XIII. Verantwortlichkeit der Unternehmensleitung

Nach den vorstehend geschilderten Möglichkeiten kann es keinem Zweifel unterliegen, dass die Unternehmensleitung verantwortlich ist, ein IT-Sicherheitskonzept einzuführen.

#### 1. Zehn Risikobereiche:

Wer das unterlässt, muss mit Risiken in folgenden Bereichen rechnen:

##### 1.1 Schadensersatz und Schmerzensgeld

Bei datenschutzrechtlichen Verletzungen wird mittlerweile auch Schmerzensgeld zugebilligt, § 253 BGB

##### 1.2 Bußgelder

Im Datenschutz drohen Bußgelder bis 250.000,00 €.

### 1.3 Haftstrafe oder Geldstrafe

Verstöße gegen das Fernmeldegeheimnis oder Vorschriften des Bundesdatenschutzgesetzes führen zu einer Geld- oder Haftstrafe. Das gilt insbesondere bei unbefugter Überwachung wegen Verletzung des Telekommunikationsgeheimnisses und dem unbefugten Löschen von Daten, zum Beispiel durch Email-Filtering.

### 1.4 Gewerberecht/Wettbewerbsrecht

Verstöße gegen IT-Sicherheitsvorschriften können zu Abmahnungen der Konkurrenz führen und im schlimmsten Fall bei notorischer Gefährdung anderer sogar zu dem Einschreiten des Gewerbeamtes.

### 1.5 Ansehensverlust

Wer seinem Geschäftspartner verseuchte Mails übersendet, verliert an Ansehen und mittelfristig möglicherweise einen Geschäftspartner.

### 1.6 Datenschutzbehörden

### 1.7 Beweisprobleme im Prozess

Im Prozess, insbesondere beim Arbeitsgericht, dürfen Daten nur dann verwendet werden, wenn sie in rechtlich zulässiger Weise erhoben worden sind.

### 1.8 Versicherung

Versicherungen zahlen nicht, wenn aufgrund eines erheblichen Verstoßes gegen die Pflicht zur IT-Sicherheit verfahren worden ist und deswegen der Schaden aufgetreten ist.

### 1.9 Banken

Beim Rating nach Basel II kann auch mangelnde IT-Sicherheitsstruktur zu einer Höherstufung im Risiko und damit zu Kosten für Unternehmen führen.

### 1.10 Urheberrechtsverstöße

Wenn schwarz kopiert wird, haftet auch das Unternehmen dem Verletzten auf Schadensersatz, wenn die Schädigung hätte vermieden werden können.

### 1.11 Jugendschutz

Laden sich minderjährige Auszubildende unzulässige Inhalte aus dem Internet, kann auch dafür der Arbeitgeber verantwortlich sein.

## 2. Pflichten der Unternehmensleitung

2.1 Verantwortlich ist „die Unternehmensleitung“. Der Geschäftsführer eines größeren Unternehmens kann aber nicht alles selbst machen. Er ist deswegen berechtigt zur **Delegation**. Wenn er delegiert, ist er aber noch nicht aller Pflichten ledig. Er muss vielmehr diejenige Person, auf die die Aufgabe übertragen wurde noch **überwachen**. Außerdem muss er diese Person in die Lage versetzen, die ihr übertragenen Aufgaben auch tatsächlich zu erfüllen.

Er muss ihr deswegen ausreichende **Schulung** und **Sachmittel** zur Verfügung stellen. Das gilt insbesondere für die Datenschutzbeauftragten. Zu empfehlen ist aber auch die Einführung eines **IT-Sicherheits-Beauftragten**.

## 2.2

Die Haftung des Geschäftsführers erstreckt sich dann nicht nur auf das Vermögen der Gesellschaft, sondern, weil er ihm persönlich obliegende Pflichten verletzt hat auf sein **Privatvermögen**.

## 2.3 Schädigung des Unternehmens

Bei grob fahrlässiger Verletzung der Pflichten zur IT-Sicherheit kann sogar der Schädiger, der eigentlich den Schaden zu tragen hätte, den Einwand des Mitverschuldens (§ 254 BGB) erheben mit der Folge, dass das Unternehmen selbst von dem vorsätzlichen (!) Schädiger nicht den vollen Schadensersatz bekommt.

Den beim Unternehmen verbleibenden Anteil trägt dann wieder der Geschäftsführer.

## 2.4

Grob fahrlässige Verletzung von Pflichten führt schließlich zum Verlust des Versicherungsschutzes.

All diese Pflichtverletzungen des Geschäftsführers berechtigten die Gesellschaft in der Regel – und nur in Ausnahmefällen nach vorheriger Abmahnung- zur Kündigung und Abberufung als Geschäftsführer.

## 2.5 Kontrolldichte

Häufig unterschätzt wird auch die Anzahl der Stellen, die IT-Sicherheit überprüfen. Das sind der Datenschutzbeauftragte, falls eingesetzt der IT-Sicherheitsbeauftragte, ein Betriebsrat, Konkurrenten (Abmahnung), die Staatsanwaltschaft bei Verstößen gegen Strafvorschriften (Telekommunikationsgeheimnis, Löschen von Daten), Banken, Investoren, Vergabestellen der öffentlichen Hand, Wirtschaftsprüfer (bei der Aktiengesellschaft), die Datenschutzbeauftragten der Länder, die Gewerbeaufsicht und die berufsständischen Kammern.

Besonders hingewiesen sei auf die Banken und Investoren, die im Rahmen der Beurteilung eines Kredites die Wahrscheinlichkeit des Fortbestandes des Unternehmens prognostizieren müssen.

Für diese Frage stellt das Betreiben eines funktionierenden IT-Sicherheitskonzeptes natürlich eine grundlegende Voraussetzung dar.

Einen Teledienst betreibt bereits, wer den Mitarbeitern das private Mailen vom Arbeitsplatz aus erlaubt.

## 2.6 Beispiel: Rechtliche Pflichten bei einem Teledienst:

Wer einen Teledienst einrichtet, muss angemessene technische Vorkehrungen zur Sicherheit des von ihm angebotenen Teledienstes gewährleisten. Dazu gehören folgende Punkte:

- Schutz des Telekommunikationsgeheimnisses
- Schutz personenbezogener Daten
- Schutz programmgesteuerter Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe
- Schutz gegen Störungen

- Schutz vor äußeren Angriffen
- Schutz vor Einwirkungen von Katastrophen

Bei europarechtlichen Richtlinien sind bei elektronischer Kommunikation auch noch folgende Sicherheitsstandards zu beachten:

Weitergabekontrolle durch Verschlüsselungs- und Überwachungssoftware.  
Verfügbarkeitskontrolle durch Filtersoftware gegen Viren.

### 3. Anforderungen an IT-Security-Software:

Daraus ergeben sich folgende Mindestanforderungen an einer IT-Securitysoftware:

- Datenverkehr scannen
- Logfiles speichern
- Inhalte filtern
- Zugriff auf Websites blockieren

### 4. Organisatorische Maßnahmen der Unternehmensleitung

Die Einführung einer Software allein reicht nicht aus, um die Pflichten der Geschäftsführung zu erfüllen.

4.1 Nach dem Gesetz über die Kontrolle und Transparenz im Betrieb (KontraG) ist vielmehr ein Konzept geschuldet. Das sollte **schriftlich** vorliegen, damit man im Falle eines Vorwurfes durch Gesellschafter oder die vorstehend genannten Kontrollstellen den Beweis führen kann, die richtigen Maßnahmen ergriffen zu haben.

4.2 Beteiligung der Mitarbeiter, insbesondere Betriebsrat, aber auch jeden Einzelnen. Ist IT-Sicherheit nicht akzeptiert, wird sie auch nicht gelebt.

4.3 Das Sicherheitskonzept ist dynamisch und muss mit dem Ausbau/Umbau der EDV-Anlage und den technischen Entwicklungen fortgeschrieben werden.

4.4 Eine IT-Nutzungsordnung für den Betrieb muss erstellt werden, damit kein Mitarbeiter sich entschuldigen kann, wenn er gegen diese verstößt. Deswegen muss die zu Beweis Zwecken unterschrieben werden.

4.5 Verbot privater Nutzung des Internet

4.6 Sicherung elektronischer Beweise bei Verstößen durch die Mitarbeiter (NFS-Network Forensic Services).

4.7 Strukturelle Maßnahmen zur laufenden Überwachung (Filtering); unbedingt vorher mit dem Betriebsrat absprechen und auch im Betrieb bekannt machen.

Notfallplan für denkbare Fälle, wie zum Beispiel Durchsuchung durch die Staatsanwaltschaft oder Entdecken strafbarer Inhalte auf dem Arbeitsplatz seines Arbeitnehmers.

Die Einführung einer IT-Security-Software ist daher nur ein Schritt, wenn auch der wesentliche, um die Haftung des Geschäftsführers auszuschließen. Damit ist die technische Seite des Problems gelöst. Zwingend müssen aber auch organisatorische Anstrengungen unternommen werden, um das Unternehmen und die Unternehmensleitung vor unangenehmen Folgen zu schützen.

#### **XIV. Zusammenfassung:**

Nach alledem steht fest, dass der Geschäftsführer einer GmbH erhebliche Verpflichtungen im Bereich des Internet hat. Sie erstrecken sich sowohl auf den Schutz der Mitarbeiter und Dritter, aber auch auf den Schutz der Vermögensinteressen seiner Gesellschafter.

Verletzt er diese Pflichten, macht er sich den Mitarbeitern, Dritten oder Gesellschaftern gegenüber möglicherweise schadensersatzpflichtig.

Angesichts des fortschreitenden Einsatzes von EDV im Geschäftsleben und den dadurch größer werdenden Risiken von Angriffen und unbeabsichtigten Schädigungen steigen daher die Anforderungen an die Sorgfaltspflichten des Geschäftsführers. Dem entspricht auch die Einstellung der Rechtsprechung, die in den letzten 20 Jahren die Verantwortlichkeit des Geschäftsführers Stück für Stück heraufgesetzt hat.

Die Anschaffung einer modernen und jederzeit aktuellen IT-Sicherheitsstruktur ist daher die effektivste Maßnahme des Selbstschutzes des Geschäftsführers, weil er damit das größte Problem der Unternehmen absichert.

Er vermeidet damit eigene Haftung und fördert den Erhalt und den Erfolg des eigenen Unternehmens.

Hagen, im September 2004

## **Anhang zum Arbeitsvertrag**

### **Verhalten im Unternehmensnetzwerk und Internet**

Das reibungslose Funktionieren des Netzwerkes und die Abwehr von Angriffen von Außen sind von entscheidender Bedeutung für unser Unternehmen.

Deshalb ergeht folgende Anweisung:

#### **Verhalten im Netzwerk:**

1. Bitte halten Sie Ihr Passwort wirklich geheim. Sorgen Sie daher dafür, daß es auch von anderen Mitarbeitern nicht eingesehen werden kann und verraten Sie es auch nicht freiwillig.  
Sobald Ihnen Ihr Passwort abhanden gekommen ist oder nur der Verdacht besteht, daß andere Mitarbeiter oder Dritte Kenntnis vom Passwort erlangt haben könnten, wollen Sie dies bitte unverzüglich Ihrem Vorgesetzten mitteilen.
2. Wenn Sie Ihren Arbeitsplatz nicht nur für wenige Sekunden verlassen, fahren Sie den Rechner bitte runter und sorgen Sie dafür, dass kein anderer Mitarbeiter in der Zeit Ihrer Abwesenheit Zugriff auf Ihren Rechner hat.
3. Rufen Sie innerhalb des Netzes nur solche Bereiche auf, die für die Durchführung der Ihnen zugewiesenen Aufgaben notwendig sind. Das Aufrufen anderer Bereiche des Netzes ist auch dann untersagt, wenn keine Sperren eingebaut sind.
4. Es ist streng verboten, Fremdsoftware oder Spiele einzuspielen. Diese Software kann Viren enthalten und zu unersetzbaren Schäden an Software und Daten des Unternehmens oder Dritter zu führen.
5. Es ist streng untersagt im Netzwerk vorhandene Software, Datenbanken oder Daten ohne ausdrückliche Anweisung zu kopieren und/oder solche Kopien außer Hauses zu bringen. Die im Unternehmen vorhandene Software, Datenbanken und Daten sind Betriebsgeheimnisse, deren Verbringung außer Hauses, auch als Kopie, ganz oder in Teilen, eine Straftat gemäß § 17 UWG darstellt.

#### **Zusätzliche Vorschriften für den Email-Verkehr und Internet:**

1. Es ist streng verboten, sowohl innerhalb als auch außerhalb des Unternehmens, Emails mit privatem Inhalt zu versenden.

#### **Alternative:**

Jeder Mitarbeiter erhält eine eigene „private“ Email-Adresse, (z. B. [h.mustermann@mustermannmbh.de](mailto:h.mustermann@mustermannmbh.de)), die von anderen Mitarbeitern nicht eingesehen

werden kann. Diese privater Emailadresse ist ausschliesslich für den privaten Emailverkehr gedacht.

Hierüber darf keinerlei geschäftliche Kommunikation erfolgen.

Der Inhalt dieser Emails wird nicht überprüft. Die Emails werden aber, wie die geschäftlichen auch, in der nachstehend beschriebenen Weise auf störende Elemente untersucht.

Jegliche Erlaubnis zur Nutzung der privaten Emailadresse ist beschränkt auf einen üblichen, die Arbeitszwecke nicht einschränkenden Umfang und auch darüber hinaus jederzeit durch den Arbeitgeber frei widerruflich.

Der Widerruf bedarf keiner Begründung, kann deshalb nicht nur in Fällen des Missbrauchs ausgesprochen werden.

2. Alle Emails, die an die offiziellen Emailadressen (z. B. [Heinz.Mustermann@Mustermann.de](mailto:Heinz.Mustermann@Mustermann.de)) des jeweiligen Mitarbeiters gehen, werden auch die jeweiligen Arbeitsgruppen und Vorgesetzten weitergeleitet. Sie werden somit auch von allen anderen Arbeitsgruppenmitgliedern und Vorgesetzten gelesen.

Alle ankommenden Emails, geschäftliche und private, werden automatisch durch einen Virensch scanner durchsucht. Verseuchte Emails werden automatisch blockiert. Der Sender dieser Email erhält automatisch eine Benachrichtigung, dass diese Email nicht angenommen wurde.

Alle ankommenden Emails werden weiterhin automatisch auf sogenannte SPAMS durchsucht. Verdächtige Emails werden gekennzeichnet und dem Empfänger weitergeleitet.

Alle ankommenden Emails, die von einem verdächtigen Server (Blacklist) kommen, werden automatisch blockiert.

Der Sender dieser Email erhält automatisch eine Benachrichtigung, dass diese Email nicht angenommen wurde.

Alle ein- und ausgehenden Emails, sowohl geschäftlich, als auch privat, werden automatisch archiviert.

3. Jede Email hat sachlich zu sein und sich jeglicher abfälligen Meinungsäußerung zu enthalten. Insbesondere dürfen die Emails keinen beleidigenden, sexistischen, rassistischen oder politischen Inhalt aufweisen. Die vorstehende Aufzählung ist nicht abschließend.

4. Es ist streng untersagt, anonyme Emails und/oder deren Anhänge (Attachements) zu öffnen und weiter zu leiten. Dies gilt auch für Emails ohne Text, die mit einem Anhang versehen sind. Bei Eingang solcher Emails ist der zuständige Vorgesetzte sofort zu informieren.

5. Treten vermehrt Werbemails auf (Spam, UCE), ist ebenfalls der Vorgesetzte zu informieren.

6. Bewegungen im Internet sind auf das geschäftlich Notwendige zu beschränken. Es ist untersagt, Seiten aufzurufen und/oder herunter zu laden, die nicht unmittelbar mit der geschäftlichen Tätigkeit im Zusammenhang stehen.
7. Jeder Aufruf des Internets ist so kurz wie möglich zu halten.

**Allgemeines:**

1. Den Anweisungen der Vorgesetzten bezüglich der Nutzung des Netzwerks einschließlich des Internet ist strikt Folge zu leisten.
2. Jeder Verstoß oder versuchte Verstoß eines Mitarbeiters gegen vorstehenden Vorschriften ist dem Vorgesetzten unverzüglich zu melden.
3. Jeder erfolgreiche oder versuchte Angriff auf das Netzwerk unseres Unternehmens, sei es durch Mitarbeiter oder durch Angriffe von Außen, ist unverzüglich zu melden.

Verstöße gegen vorstehende Vorschriften können schwerste Schäden für unser Unternehmen hervorrufen. Jeder Arbeitnehmer, der gegen diese Vorschriften verstößt, muß daher mit arbeitsrechtlichen Konsequenzen bis hin zur fristlosen Kündigung rechnen.

....., den .....  
Unterschrift Geschäftsleitung

.....,den.....  
Arbeitnehmer