

# Internet und IT-Security im Unternehmen

Juristische Informationen für die Unternehmensleitung

D







# Internet und IT-Security im Unternehmen

Juristische Informationen für die  
Unternehmensleitung

Ohne den Einsatz von Informationstechnologie ist die Führung eines Unternehmens heute kaum mehr denkbar. Die Nutzung des Internets bietet jede Menge Möglichkeiten: von der fast grenzenlosen Recherche über die schnelle Übermittlung von Dokumenten, Bildern, Software oder Musik, bis zum Abschluss von Rechtsgeschäften wie beispielsweise der Online-Bestellung von Waren. E-Mails führen als Kommunikationsmedium zu fast ständiger Erreichbarkeit und neuen Reaktionsgeschwindigkeiten. Der Informationsaustausch innerhalb von Unternehmen und die Kommunikation mit Kunden, Partnern oder Zulieferern wird dadurch erheblich beschleunigt.

Allerdings bietet die Informationstechnologie nicht nur Vorteile: Die E-Mail- und Internet-Nutzung durch Mitarbeiter kann zu datenschutzrechtlichen Problemen im Unternehmen führen. Der Missbrauch von IT-Infrastruktur oder Datendiebstahl hat unter Umständen nicht nur strafrechtliche Konsequenzen, sondern kann auch (zivilrechtliche) Schadensersatzverpflichtungen gegen das Unternehmen begründen.

Im Rahmen der Corporate Governance ist IT-Security und IT-Compliance für die Geschäftsleitung von großer Bedeutung. Sie stellt sicher, dass Geschäftsführer, Vorstand oder Aufsichtsrat den einschlägigen rechtlichen Anforderungen gerecht werden können und ihren Pflichten nachkommen.

Für den Bereich des E-Commerce ist relevant, wie Verträge über das Internet geschlossen werden, welche Verbraucherschutz-Regelungen einzuhalten sind und wie eine elektronische Rechnung rechtswirksam gestellt werden kann.

Dieser Leitfaden gibt einen Einblick in wichtige juristische Themengebiete, die für den Einsatz von IT-Infrastruktur und Internet in Unternehmen relevant sind. Dabei liegt der Schwerpunkt auf IT-Security. Die nachfolgenden Kapitel enthalten juristische Informationen für die Geschäftsleitung, jedoch keine konkrete Handlungsanweisung oder -anleitung. Diese Hinweise sind lediglich allgemeiner Art und können weder eine Untersuchung des jeweiligen Einzelfalls noch eine Rechtsberatung durch eine interne Rechtsabteilung bzw. einen Rechtsanwalt ersetzen.

Auch wenn die Autoren schon seit vielen Jahren im Bereich des IT- und Internet-Rechts sowie der IT-Security tätig sind und sorgfältig recherchiert haben, übernehmen sie für die Richtigkeit und Vollständigkeit dieses Leitfadens keine Haftung.

# I Die Themen im Überblick

Die **Sicherstellung der IT-Security** ist originäre Pflicht und Aufgabe der Unternehmensleitung.

Sie umfasst insbesondere:

- **Wirksame Schutzmaßnahmen gegen Angriffe von außen, z.B. durch Hacker, Viren oder sog. Botnets (ferngesteuerte Netzwerke von infizierten Computern)**
- **Einhaltung der datenschutzrechtlichen Pflichten**
- **Regelmäßige Erstellung von Backups**
- **Berücksichtigung von Handlungsanleitungen, Best Practice-Vorgaben und Wirtschaftsprüfungsstandards**

Bei Nichtbeachtung drohen als **Sanktionen** u.a. zivilrechtliche Schadensersatzansprüche von Geschädigten gegen das Unternehmen, Geldbußen, ökonomische Nachteile wie z.B. ein schlechteres Kreditrating, Verlust des Versicherungsschutzes oder der Ausschluss bei der Vergabe öffentlicher Aufträge.

**Geschäftsführer, Vorstände und Aufsichtsräte können zudem persönlich in die Haftung genommen werden.**

Der **Missbrauch von IT-Infrastruktur** und der **Datendiebstahl** können nach mehreren Vorschriften strafbar sein. Dazu zählen z.B. das Ausspähen von Daten, die Verletzung des Post- oder Fernmeldegeheimnisses oder der Verrat von Geschäfts- und Betriebsgeheimnissen.

Ein heikles Thema für die Beziehungen zwischen der Geschäftsleitung und den Mitarbeitern eines Unternehmens (und ihren Vertretungsorganen) stellt die **Nutzung des vom Unternehmen zur Verfügung gestellten E-Mail-Accounts und Internetzugangs für private Zwecke** dar. Hierbei kommt es darauf an, die Weichen richtig zu stellen.

Bei der Teilnahme am **elektronischen Rechtsverkehr** können ebenso verbindliche Verträge geschlossen werden, wie außerhalb des Internets. Zur Gewährleistung der Authentizität und der Integrität elektronischer Willenserklärungen und Dokumente sowie bei der elektronischen Rechnungsstellung kann auf die **elektronische Signatur** zurückgegriffen werden.



# IT-Security und IT-Compliance im Unternehmen

*Im Rahmen der Corporate Governance soll die Unternehmensleitung und -überwachung transparent gemacht werden, um das Vertrauen in die Unternehmensführung zu stärken. Der Vorstand bzw. die Geschäftsführung hat die Einhaltung der gesetzlichen Bestimmungen zu gewährleisten, auf deren Beachtung durch die Konzernunternehmen hinzuwirken und für ein angemessenes Risikomanagement und -controlling im Unternehmen zu sorgen. Die Sicherstellung der IT-Security und der IT-Compliance bilden dabei wichtige Bausteine.*

## 1. Generelle Anforderungen an die IT-Security

Das Schlagwort „IT-Security“ umfasst nicht nur Schutzmaßnahmen der Unternehmen gegen Angriffe auf ihre IT-Infrastruktur, sondern schließt auch zahlreiche rechtliche Aspekte ein.

Nach dem „Gesetz über das Bundesamt für die Sicherheit in der Informationstechnik“ (BSIG) bedeutet „Sicherheit in der Informationstechnik“ (...) „die Einhaltung bestimmter Sicherheitsstandards, die durch Sicherheitsvorkehrungen die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen

1. in informationstechnischen Systemen oder Komponenten oder
2. bei der Anwendung von informationstechnischen Systemen oder Komponenten.“

### a) Sicherstellung der Verfügbarkeit

Der Schutz vor Informationsverlust, Informationsentzug, Informationsblockade und Informationszerstörung muss gewahrt werden. Wichtige Kunden- oder Geschäftsdaten müssen während der üblichen Arbeitszeiten permanent verfügbar sein, damit der fortlaufende Geschäftsbetrieb nicht beeinträchtigt wird.

So können einem Urteil des Bundesgerichtshofs vom 12. Dezember 2000 (Az. XI ZR 138/00) zufolge Kunden von Online-Banking erwarten, dass sie zu dem Online-Service „rund um die Uhr“ Zugang haben.

Eine Klausel, durch die der Anbieter eines Online-Services die Haftung für sämtliche technisch oder betrieblich bedingten zeitweiligen Zugangsstörungen - auch im Fall eigenen groben Verschuldens - ausschließen wollte, hielt der Bundesgerichtshof für unwirksam.

Unternehmen sind verpflichtet, ihre IT-Infrastruktur zu den üblichen Geschäftszeiten zur Verfügung zu stellen. Sofern Unternehmen ihren Kunden Online-Services anbieten, sollten sie deren Verfügbarkeit entweder in Service Level Agreements (SLA) regeln oder den Zugang – mit Ausnahme üblicher Wartungsintervalle – „rund um die Uhr“ gewährleisten. Dabei muss eine regelmäßige Datensicherung vorgenommen und die IT-Infrastruktur insbesondere gegen Schad-Software („Malware“), Virenausbrüche und Angriffe von Hackern geschützt werden. Die Maßstäbe hierfür werden ohne Zweifel durch den permanenten technologischen Fortschritt gesetzt. Daher kann es z.B. erforderlich sein, wegen der ständig zunehmenden mobilen Telekommunikation und Virtualisierung der IT-Systeme Echtzeitschutz im Rahmen von kollektiven Sicherheitsnetzwerken in Anspruch zu nehmen.

### b) Sicherstellung der Unversehrtheit

Unternehmen müssen ihre IT-Infrastruktur gegen ungewollte Informationsveränderungen schützen. Unbefugte dürfen unter keinen Umständen Daten verändern können. Besonders sensible Daten - wie Buchhaltungsunterlagen oder elektronisch gespeicherte rechtsverbindliche Erklärungen -, müssen ausreichend gegen externe Angriffe geschützt sein. Hinzu kommt der Schutz der Integrität von Dokumenten gegen unbefugte Änderungen - beispielsweise durch die sog. elektronische Signatur.

### c) Sicherstellung der Vertraulichkeit

Vertrauliche Unternehmensinformationen sollten nicht von Dritten ausgespäht werden können. Dies betrifft insbesondere drei Arten von Daten:

- **personenbezogene Daten, die dem Datenschutz unterliegen,**
- **Inhalte der Telekommunikation und deren nähere Umstände, die durch das Fernmeldegeheimnis geschützt sind, sowie**
- **Geschäfts- und Betriebsgeheimnisse von Unternehmen.**

Der Zugriff auf derartige Daten und Informationen darf nur berechtigten Personen möglich sein. Im Rahmen der IT-Security sind sowohl Zugriffsbeschränkungen als auch Schutzvorrichtungen gegen das Ausspähen von Daten durch Externe ebenso wie gegen Datenmissbrauch durch Interne und Datenlecks einzurichten.

### d) Sicherstellung der Authentizität

Schließlich ist die Authentizität der handelnden Personen sicherzustellen. Insbesondere wenn Geschäftskontakte ausschließlich online erfolgen, kennen sich die Vertragsparteien nicht unbedingt persönlich. E-Mail-Absender können fingiert sein, Webseiten können gar kein oder ein falsches Impressum enthalten.

Mittels der elektronischen Signatur lässt sich sicherstellen, dass es sich bei dem Vertragspartner auch um die Person handelt, für die er sich ausgibt. Zusätzlich sollte elektronische Post aber auch auf ihrem Weg zum Empfänger durch geeignete Verschlüsselungstechnologie für unbefugte Augen unlesbar gemacht werden.

## 2. Rechtliche Pflichten zur IT-Security

IT-Security ist nicht Selbstzweck, sondern rechtliche Verpflichtung der Unternehmensleitung.

### a) Anforderungen an die Unternehmensleitung und andere Beteiligte

Das „Gesetz zur Kontrolle und Transparenz im Unternehmensbereich“ (KonTraG) aus dem Jahre 1998 hat die Anforderungen für Vorstände von Aktiengesellschaften und die Geschäftsführung großer Kapitalgesellschaften an Kontrolle und Transparenz verschärft:

- Der Vorstand bzw. die Geschäftsführung muss geeignete Maßnahmen treffen und insbesondere ein Überwachungssystem einrichten, um für den Fortbestand der Gesellschaft gefährdende Entwicklungen frühzeitig zu erkennen.
- Es ist ein unternehmensweites Risikomanagement zu installieren. Teil der Risikoprävention ist dabei der Schutz der IT-Infrastruktur, also die Sicherstellung der IT-Security.
- Im Rahmen des Lageberichts von Kapitalgesellschaften (mit Ausnahme sog. „kleiner Kapitalgesellschaften“) ist darauf einzugehen – und vom Abschlussprüfer zu kontrollieren –, ob die Chancen und Risiken der künftigen Entwicklung des Unternehmens zutreffend dargestellt sind. Die IT-Risiken sind dabei zu benennen.
- Die Unternehmensleitung ist dafür verantwortlich, wirksame Maßnahmen zum Schutz der IT-Infrastruktur zu treffen und ein entsprechendes Risikomanagement einzurichten. Sollten Geschäftsführer bzw. Vorstände diese Pflicht verletzen und das Unternehmen dadurch Schaden erleiden, haften sie gegenüber ihrem Unternehmen persönlich. Dies gilt gleichermaßen für den Aufsichtsrat einer Aktiengesellschaft im Falle eines Verstoßes gegen seine Pflicht zur Überwachung der Geschäftsführung.

Aber auch Unternehmensmitarbeiter können bei Verstößen gegen die Anforderungen der IT-Sicherheit gegebenenfalls wegen Verletzung ihrer arbeitsvertraglichen Pflichten in Anspruch genommen werden. Sofern bei der Umsetzung von IT-Sicherheitsmaßnahmen externe Unternehmen beauftragt worden sind, kommt bei entsprechenden Pflichtverletzungen eine Haftung aus Dienst-, Werk- oder Geschäftsbesorgungsvertrag in Betracht.

Der IT-Security muss also von allen Beteiligten – auch in ihrem eigenen Interesse – höchste Priorität eingeräumt werden!

### **b) Vermeidung öffentlich-rechtlicher Konsequenzen und ökonomischer Nachteile**

Die Sicherstellung der IT-Security ist auch zur Vermeidung ökonomischer Nachteile für Unternehmen von erheblicher Bedeutung.

Im Juni 2004 hat der Basler Ausschuss für Bankenaufsicht die „Neue Basler Eigenkapitalvereinbarung“ verabschiedet, die unter dem Stichwort „Basel II“ die Kapitalanforderungen an Kreditinstitute stärker als bisher vom eingegangenen Risiko abhängig macht. Bei der Finanzierung von Unternehmen sind besonders versteckte organisatorische Risiken zu beachten. Für Unternehmen, die stark von der Funktionsfähigkeit ihrer IT-Infrastruktur abhängig sind, ist die IT-Sicherheit für das Rating und damit auch für die Kreditkonditionen von großer Bedeutung.

Auch der US-amerikanische Sarbanes-Oxley Act (SOX) hat auf europäische Unternehmen Einfluss, wenn sie an einer amerikanischen Wertpapierbörse notiert sind oder ein solches Unternehmen als Muttergesellschaft haben. Diese Unternehmen müssen u.a. ein Kontrollsystem für Finanzdaten vorhalten, mit dem auch Anforderungen an IT-Systeme impliziert werden, da in aller Regel Finanzdaten elektronisch verarbeitet werden. Verstöße gegen SOX können Auswirkungen auf das Börsen-Listing sowie Bußgelder oder sogar Gefängnisstrafen für die verantwortlichen Manager nach sich ziehen.

Wirtschaftsprüfer können bei börsennotierten Aktiengesellschaften das Testat im Rahmen der Jahresabschlussprüfung verweigern, wenn die IT-Sicherheitsstandards unzureichend sind. Das Ende Mai 2009 in Kraft getretene Bilanzrechtsmodernisierungsgesetz, das die EU-Abschlussprüferrichtlinie (so etwas wie ein „Euro-SOX“) in deutsches Recht umsetzt, verschärft die Anforderungen an Abschlussprüfer, so dass sie ihre Prüfung börsennotierter Gesellschaften aller Voraussicht nach künftig strenger durchführen werden. Zudem ist die Wirksamkeit des internen Kontroll- und Risikomanagementsystems kapitalmarktorientierter Kapitalgesellschaften durch den Aufsichtsrat oder einen von ihm bestellten Prüfungsausschuss besser zu kontrollieren. Auch wenn nach dieser Gesetzesänderung die Entscheidung über Einrichtung, Art und Umfang eines Risikomanagementsystems weiter im Aufgabenbereich der Geschäftsführung bzw. des Vorstands liegt, wurden die Anforderungen an die IT-Compliance und IT-Security nochmals erhöht und damit die Haftung von Vorstand und Aufsichtsrat verschärft.

Öffentliche Auftraggeber fordern im Rahmen der Leistungsbeschreibung bei IT-relevanten Aufträgen einen Nachweis über die IT-Sicherheit. Anbieter, die dies nicht nachweisen können, laufen Gefahr, dass ihr Angebot wegen Nichterfüllung der Leistungsbeschreibung oder aufgrund mangelnder Zuverlässigkeit schon bei der ersten Prüfung ausgeschlossen wird.

Bei besonders schwerwiegenden Verstößen gegen die Grundsätze der IT-Security kann sogar die gewerberechtliche Zuverlässigkeit des Unternehmens in Frage gestellt werden und eine Gewerbeuntersagung erfolgen.

## **3. Konkrete Maßnahmen zur IT-Security und IT-Compliance**

Nachfolgend werden einige konkrete Maßnahmen zur Sicherstellung der IT-Security und IT-Compliance in Unternehmen vorgestellt. Dieser Maßnahmenkatalog basiert primär auf rechtlichen Erwägungen und ist nicht abschließend. Seine Umsetzung sollte zwischen der Unternehmensleitung, der IT-Abteilung, der Rechtsabteilung und gegebenenfalls externen Beratern des Unternehmens (z.B. IT-Systemhäuser, externe Datenschutzbeauftragte, Rechtsanwälte oder Wirtschaftsprüfer) abgestimmt werden.

### **a) Schutz vor Hackern, Viren, Trojanern, Spyware, Botnets etc.**

Aus den in Ziffer 2 dargestellten Gründen folgt bereits, dass Unternehmen zur Sicherstellung der IT-Security wirksame Maßnahmen gegen Angriffe von außen implementieren müssen. Der Schutz gegen Hacker, also fremde Dritte, die in Computersysteme des Unternehmens eindringen und dabei Daten ausspähen, verändern oder zerstören, ist erforderlich, um die Verfügbarkeit, Unversehrtheit und Vertraulichkeit der IT-Infrastruktur sicherzustellen und personenbezogene Daten zu schützen. Dies gilt auch für Angriffe durch Schad-Software wie Viren oder Würmer sowie durch Trojaner, welche es einem Dritten ermöglichen, die Kontrolle über ein EDV-System zu übernehmen. Über die Errichtung von sog. „Botnets“ (Netzwerke von infizierten Computern) gelingt es sog. „Botmasters“ mit kriminellen Zielen immer häufiger, fremde Computer für

sich zu nutzen, um z. B. Spam oder Denial of Service-Attacken zu initiieren. Ebenso können sie mit Hilfe von Spyware fremde Daten sammeln.

Die Abwehr gegen den Befall durch Schad-Software ist aus zweierlei Gründen wichtig: Zum einem muss das Unternehmen seine eigene IT-Infrastruktur schützen, zum anderen muss es verhindern, selbst haftbar gemacht zu werden.

In mehreren Urteilen der letzten Jahre (z.B. Landgericht Hamburg vom 25. Januar 2006 – Az. 308 O 58/06 und vom 15. Juli 2008 – Az. 310 O 144/08) wurde entschieden, dass der Inhaber eines Internetanschlusses für eine damit begangene Rechtsverletzung einstehen muss, auch wenn er selbst die Handlungen gar nicht vorgenommen hat. Denn als Inhaber des Anschlusses ist er rechtlich und tatsächlich in der Lage, entsprechende Prüf- und Kontrollmaßnahmen zu treffen, und muss dafür sorgen, dass sein Anschluss nicht für Rechtsverletzungen genutzt werden kann.

Ähnlich hat das Oberlandesgericht Düsseldorf in Beschlüssen vom 27. Dezember 2007 (Az. I-20 W 157/07) und vom 11. Mai 2009 (Az. 20 W 146/08) entschieden. Demnach trifft den Betreiber eines WLAN-Funknetzes die Pflicht, dieses abzusichern. Wer – so das OLG Düsseldorf – ein WLAN verwendet, hat zumindest Sicherungsmaßnahmen zu ergreifen, die eine Standardsoftware erlaubt, wie z.B. die Einrichtung von Benutzerkonten mit Passwort und eine Verschlüsselung. Unterlässt ein Betreiber solche technischen Schutzmaßnahmen, hat er für Rechtsverletzungen wie etwa Urheberrechtsverletzungen einzustehen, die Unbekannte über sein Funknetz begehen.

Wird ein Unternehmenscomputer z. B. über ein Botnet dafür missbraucht, Viren oder Spam an Dritte zu versenden oder eine Denial of Service-Attacke zu initiieren, muss das Unternehmen für Unterlassung und Schadensersatz einstehen. Dieser Fall kann bei unzureichenden Sicherungsmaßnahmen (z.B. veralteter Virenschutz) des IT-Systems durchaus eintreten.

Der Einsatz und die Wartung entsprechender Virenschutz-Software ist zwingende Voraussetzung, um die Anforderungen an die IT-Compliance zu erfüllen und die Haftung gegenüber Dritten zu minimieren.

### **b) Datenschutz**

Sofern personenbezogene Daten verarbeitet werden – was in aller Regel der Fall ist, wenn Namen von Mitarbeitern, Kunden oder persönliche E-Mail-Adressen gespeichert werden – sind die Anforderungen des Datenschutzrechts, insbesondere diejenigen des Bundesdatenschutzgesetzes (BDSG), zu beachten. § 9 BDSG regelt technische und organisatorische Maßnahmen, die Unternehmen zu treffen haben. In einer Anlage zu § 9 Satz 1 BDSG sind folgende Maßnahmen näher beschrieben:

• Zutrittskontrolle	• Zugriffskontrolle	• Eingabekontrolle	• Verfügbarkeitskontrolle
• Zugangskontrolle	• Weitergabekontrolle	• Auftragskontrolle	• Datentrennung

Sofern Unternehmen die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten an ein anderes Unternehmen durch die sog. Auftragsdatenverarbeitung auslagern, bleiben sie für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Der Auftragsdatenverarbeiter muss nach seinen getroffenen technischen und organisatorischen Maßnahmen unter besonderer Berücksichtigung von § 11 BDSG vom Auftraggeber ausgewählt werden. Die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse sind in dem entsprechenden Auftrag schriftlich festzulegen. Zudem muss der Auftraggeber sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen des Auftragnehmers überzeugen. Das Ergebnis ist zu dokumentieren.

Sollten die Anforderungen nach §§ 9 oder 11 BDSG nicht eingehalten werden oder sollte eine sonstige unzulässige Datenerhebung, -verarbeitung oder -nutzung erfolgen, etwa weil der Betroffene hierzu keine Einwilligung erteilt hat, drohen nach § 43 BDSG erhebliche Geldbußen (bis zu € 300.000). Zudem können nach § 7 BDSG Schadensersatzansprüche geltend gemacht werden.

Außerdem besteht seit dem 1. September 2009 nach § 42a BDSG eine gesetzliche Pflicht zur Benachrichtigung der zuständigen Datenschutzaufsichtsbehörde sowie des Betroffenen, falls bestimmte Arten personenbezogener Daten Dritten unrechtmäßig (ggf. auch „nur“ auf Grund einer Sicherheitspanne) zur Kenntnis gelangt sind und schwerwiegende Beeinträchtigungen der Rechte oder schutzwürdigen Interessen des Betroffenen drohen. Bei



einer anderweitig nicht sicher erreichbaren Vielzahl von Betroffenen kann sogar eine öffentliche Mitteilung in überregionalen Medien erforderlich werden. Der Einsatz von Technologien zur Verhinderung von Datenlecks (sog. „Data Leak Prevention“) kann solchen peinlichen Pressemitteilungen wirksam vorbeugen.

### **c) Datensicherung**

Nach einem Urteil des Oberlandesgerichts Hamm vom 1. Dezember 2003 (Az. 13 U 133/03) gehört es „im gewerblichen Anwenderbereich heute zu den vorauszusetzenden Selbstverständlichkeiten, dass eine zuverlässige, zeitnahe und umfassende Datenroutine die Sicherung gewährleistet“.

Das heißt: Eine Sicherung muss täglich erfolgen, eine Vollsicherung mindestens einmal wöchentlich. Sofern ein Unternehmen kein regelmäßiges Backup seiner Daten und seiner IT-Systeme durchführt, ist ihm im Falle eines durch Datenverlust entstehenden Schadens ein „haftungsüberdeckendes Mitverschulden“ vorzuwerfen. Etwaige Schadensersatzansprüche gegen Dritte, die an sich für den Datenverlust verantwortlich sind, sind somit nicht oder nur in stark begrenztem Umfang durchsetzbar. Sollte ein Datenverlust erfolgen und die Daten mangels ausreichender Backups nicht wiederhergestellt werden können, droht aufgrund dieses grob fahrlässigen Außerachtlassens von Sicherheitsvorkehrungen auch ein Verlust des Versicherungsschutzes.

### **d) Arbeitsrecht und Arbeitsschutz**

Im Rahmen der IT-Compliance sind die Mitbestimmungsrechte des Betriebsrats hinsichtlich der Einrichtung und des Betriebs von IT-Systemen zu beachten. So stehen dem Betriebsrat z. B. Mitbestimmungsrechte bei der Einführung und Anwendung von technischen Einrichtungen zu, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Arbeitsplätze, Arbeitsablauf und Arbeitsumgebung sind an gesicherten arbeitswissenschaftlichen Erkenntnissen auszurichten. Im Rahmen der IT-Compliance müssen also die Rechte des Betriebsrats gewahrt und die geltenden Arbeitsschutzvorschriften, wie z. B. die Bildschirmarbeitsverordnung, beachtet werden.

### **e) Handlungsanleitungen und Best Practice-Vorgaben**

Auch wenn es sich um keine für Unternehmen verbindliche Richtlinie handelt, stellen die „IT-Grundschutzkataloge“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI, [www.bsi.de](http://www.bsi.de)) eine wichtige Handlungsanleitung für die praktische Umsetzung von IT-Compliance-Anforderungen dar. Anhand dieser Grundschutzkataloge und der Werkzeuge, die vom BSI zur Verfügung gestellt werden, können Unternehmen ein angemessenes IT-Sicherheitsniveau erreichen. Die IT-Grundschutz-Standards des BSI enthalten Empfehlungen zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen mit Bezug zur Informationssicherheit. Sie umfassen Managementsysteme für Informationssicherheit (BSI-Standard 100-1), die IT-Grundschutz-Vorgehensweise (BSI-Standard 100-2), die Risikoanalyse auf der Basis von IT-Grundschutz (BSI-Standard 100-3) und Notfallmanagement (BSI-Standard 100-4). Weiterhin lassen sich die Iso-Standards 13335, 27001 und 27002 sowie die „IT Infrastructure Library“ (ITIL), eine über Jahrzehnte gewachsene Sammlung von Best Practices zum IT Service Management, als Best Practice-

Vorgaben heranziehen. Auch eine Zertifizierung des Informationssicherheits-Managementsystems nach ISO 27001 ist möglich. Als weiterer Standard kann auf die „Control Objectives for Information and related Technology“ (COBIT) zurückgegriffen werden. Hierbei handelt es sich um ein international anerkanntes Framework zur IT-Governance, welches vom IT-Governance Institute (ITGI) mittlerweile in der Version 4.1 veröffentlicht worden ist (kostenlos abrufbar unter [www.itgi.org](http://www.itgi.org)).

#### **f) Einhaltung von Prüfungsstandards**

Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) hat verschiedene Prüfungsstandards wie z.B. IDW PS 330 (Abschlussprüfung bei Einsatz von Informationstechnologie), IDW PS 331 (Abschlussprüfung bei teilweiser Auslagerung der Rechnungslegung auf Dienstleistungsunternehmen) und IDW PS 880 (Die Prüfung von Softwareprodukten) herausgegeben, die bei Abschlussprüfungen zu beachten sind.

#### **g) Anforderungen an die Buchhaltung**

§§ 239 und 257 HGB beinhalten Anforderungen an die Führung der Handelsbücher und die Aufbewahrung der Unterlagen. Die Grundsätze ordnungsgemäßer Buchführung (GoB) sind einzuhalten. Nach §239 Abs. 4 Satz 2 HGB muss bei der Führung der Handelsbücher und der sonst erforderlichen Aufzeichnungen auf Datenträgern insbesondere sichergestellt sein, dass die Daten während der Dauer der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können. Zu beachten sind dabei die „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme“ (GoBS) der Finanzverwaltung. Die inhaltliche Übereinstimmung der Wiedergabe mit den auf den maschinell lesbaren Datenträgern geführten Unterlagen muss durch das jeweilige Archivierungsverfahren sichergestellt sein.

Die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“ (GDPdU) regeln die Anforderungen an Unternehmenssoftware, sodass die betriebswirtschaftlichen Daten vom Betriebsprüfer erfasst werden können. Daher sollte die einzusetzende Software durch einen fachlich versierten Wirtschaftsprüfer auf die Einhaltung der Grundsätze überprüft und entsprechend zertifiziert worden sein, um bei der nächsten (elektronischen) Betriebsprüfung durch das Finanzamt keine böse Überraschung zu erleben.

Je nach Art der Unterlagen beträgt die Aufbewahrungsfrist sechs bzw. zehn Jahre. Es ist sicherzustellen, dass auch bei einer Erneuerung der IT-Infrastruktur oder einer Datenmigration das Unternehmen den GoBS und den GDPdU gerecht wird.

#### **h) Besondere Anforderungen an Banken und Finanzdienstleister**

§ 25a Kreditwesengesetz (KWG) sowie § 33 Wertpapierhandelsgesetz (WpHG) enthalten besondere Organisationspflichten für Banken und Finanzdienstleister. Danach müssen angemessene Sicherheitsvorkehrungen für den Einsatz der elektronischen Datenverarbeitung getroffen werden. Sofern Bereiche auf ein anderes Unternehmen ausgelagert werden, die für die Durchführung der Bankgeschäfte oder Finanzdienstleistungen wesentlich sind, dürfen weder die Ordnungsmäßigkeit dieser Geschäfte oder Dienstleistungen noch die Steuerungs- oder Kontrollmöglichkeiten der Geschäftsleitung, noch die Prüfungsrechte und Kontrollmöglichkeiten der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) beeinträchtigt werden. In entsprechenden Rundschreiben der BaFin werden diese Anforderungen konkretisiert sowie Mindestanforderungen an das Risikomanagement (MaRisk) aufgestellt. Banken und Finanzdienstleister müssen diese organisatorischen Pflichten beachten -insbesondere beim Outsourcing von IT-Leistungen.

## **4. Sanktionen bei Verstoß gegen IT-Compliance-Anforderungen**

Beim Verstoß gegen Compliance-Anforderungen an die IT-Security können folgende Sanktionen drohen, die allerdings von Fall zu Fall unterschiedlich sind:

#### **a) Strafrechtliche Sanktionen**

Vorsätzliche Verstöße – wie das Ausspähen von Daten, die Verletzung des Fernmeldegeheimnisses oder die Verletzung von Datenschutzvorschriften in Bereicherungsabsicht - sind mit Geld- oder Freiheitsstrafe bedroht.



### **b) Ordnungswidrigkeit**

Verstöße gegen öffentlich-rechtliche Regelungen, wie das Datenschutzrecht oder das KWG, können eine Ordnungswidrigkeit darstellen und Bußgelder nach sich ziehen.

### **c) Haftung der Unternehmensleitung**

Vorstands- oder Aufsichtsratsmitglieder sowie Geschäftsführer oder geschäftsführende Gesellschafter sind der Gesellschaft persönlich zum Ersatz des Schadens verpflichtet, welcher der Gesellschaft aufgrund schuldhafter Pflichtverletzung ihrer Organmitglieder entsteht. Bei Aktiengesellschaften können unter gewissen Voraussetzungen selbst Minderheitsaktionäre, auch wenn sie nur ein Prozent des Grundkapitals auf sich vereinigen, die Durchsetzung solcher Schadensersatzansprüche einklagen.

### **d) Haftung von Arbeitnehmern**

Arbeitnehmer, besonders IT-Sicherheitsverantwortliche, können gegenüber ihrem Arbeitgeber schadensersatzpflichtig sein, wenn sie schuldhaft ihre Arbeitsleistung schlecht erbracht und dadurch den Arbeitgeber geschädigt haben. Verstoßen sie gegen Compliance-Anforderungen an die IT-Security, kann das, je nach Grad des Verstoßes, eine Abmahnung oder fristlose Kündigung nach sich ziehen. So hat zum Beispiel das Arbeitsgericht Aachen mit Urteil vom 16. August 2005 (Az. 7 Ca 5514/04) die fristlose Kündigung eines Systemadministrators ohne vorherige Abmahnung als rechtmäßig angesehen, weil dieser – mit umfassenden Zugriffsrechten ausgestattet – aus Neugierde interne E-Mail-Korrespondenz zwischen seinem Vorgesetzten und einer anderen Führungskraft eingesehen hatte. Das Landesarbeitsgericht München hat in einem Urteil vom 8. Juli 2009 (Az. 11 Sa 54/09) diese Rechtsprechung bestätigt und entschieden, dass sich ein Unternehmen darauf verlassen können muss, dass seine Systemadministratoren die eingeräumten Zugriffsrechte nicht missbrauchen, und im Falle eines Verstoßes fristlos kündigen darf.

### **e) Haftung des Unternehmens**

Auch das Unternehmen selbst kann im Einzelfall gegenüber Dritten haftbar sein. Dies gilt aufgrund Organisationsverschuldens, wenn keine ausreichenden Schutzvorrichtungen getroffen wurden, die beispielsweise den Missbrauch der IT-Infrastruktur durch Externe verhindern. Sofern dadurch Dritte geschädigt werden – weil über das IT-System des Unternehmens Spam oder Viren versendet wurden – ist das Unternehmen Unterlassungs- und Schadensersatzsprüchen des Geschädigten ausgesetzt.

### **f) Weitere Konsequenzen**

Zudem droht die Reduzierung oder der Verlust von Schadensersatzansprüchen gegenüber Dritten aufgrund überwiegenden Mitverschuldens, der Verlust von Versicherungsschutz, der Ausschluss von der öffentlichen Auftragsvergabe oder sogar die Gewerbeuntersagung.

# III

## III. Gewährleistung der Vertraulichkeit und Integrität von IT-Systemen

### 1. Urteil des Bundesverfassungsgerichts zum „IT-Grundrecht“

Mit seinem Urteil vom 27. Februar 2008 (Az. 1 BvR 370/07) hat das Bundesverfassungsgericht ein neues Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme geschaffen, das in der Öffentlichkeit als „IT-Grundrecht“ bezeichnet wird. Es ist dann anzuwenden, wenn ein Zugriff auf IT-Systeme es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten.

Zwar werden von dem Grundrecht nicht Server, Großrechenanlagen und die Steuerung technischer Geräte erfasst, denn hierüber verfügt der Arbeitnehmer nicht selbstbestimmt, aber beispielsweise ein dem Arbeitnehmer überlassenes Notebook, elektronischer Terminkalender und Mobiltelefon.

Um den Grundrechtsschutz seiner Mitarbeiter und anderer Nutzer der IT-Infrastruktur auf Integrität der IT-Systeme zu gewährleisten, wird von einem Unternehmen verlangt werden müssen, ausreichende Überwachungsmaßnahmen einzurichten. Die Anforderungen an Unternehmen zur Gewährleistung der IT-Sicherheit und IT-Compliance sind durch das Urteil des Bundesverfassungsgerichts gestiegen. Hiernach sind nicht nur Vorkehrungen gegen wirtschaftliche Schäden und Risiken wie Datenverluste zu treffen, sondern auch zur Gewährleistung der Vertraulichkeit und Integrität der IT-Systeme.

### 2. Online-Durchsuchung („Bundestrojaner“)

Durch das Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 25. Dezember 2008 wurde eine Befugnis des Bundeskriminalamtes zur Online-Durchsuchung eingeführt. Allerdings bestehen über diese Online-Durchsuchung durch den Einsatz eines „Bundestrojaners“ unzutreffende Vorstellungen. So behauptet ein Anbieter von Internet-Sicherheitslösungen, durch den Einsatz seiner Software würde ein solcher Bundestrojaner „vermutlich erkannt“. Durch den neu eingeführten § 20k Bundeskriminalamtgesetz wird dem Bundeskriminalamt gestattet, „mit technischen Mitteln in informationstechnische Systeme einzugreifen und aus ihnen Daten zu erheben“. Wie dies geschieht, sei es durch den Einsatz eines Trojaners oder durch andere Arten eines Angriffs auf den zu durchsuchenden Computer, ist gesetzlich nicht näher geregelt. Das Bundeskriminalamt wird also von Fall zu Fall entscheiden, wie es die Online-Durchsuchung durchführt, und hierzu aller Voraussicht nach häufig individuelle Einzelanfertigungen als „Ermittlungssoftware“ programmieren. Daher lassen sich zur Zeit keine seriösen Aussagen darüber treffen, ob und in welchem Umfang Internet-Sicherheitslösungen Schutz gegen solche Software („Bundestrojaner“) bieten. Allerdings sind Anbieter von Internet-Sicherheitslösungen nicht zum aktiven Mitwirken beim Zugriff auf gespeicherte Daten verpflichtet, so dass sie nicht etwa eine „Backdoor“ für den „Bundestrojaner“ bereitstellen müssen. Vielmehr geht das Bundesverfassungsgericht in seinem o.g. Urteil zum IT-Grundrecht trotz der staatlichen Befugnis einer Online-Durchsuchung davon aus, dass technische Selbstschutzmöglichkeiten wie Antiviren-Programme eingesetzt werden, um einen Zugriff von außen zu verhindern.

### 3. Schutz gegen Datenlecks (Data Leak Prevention)

Wie z.T. schon an anderer Stelle in diesem Leitfaden erwähnt, gibt es verschiedene rechtliche Verpflichtungen für Unternehmen aller Größen, angemessene Maßnahmen zum Schutz gegen Datenlecks (oder Datensicherheitspannen) zu treffen. Sie sollen sicherstellen, dass elektronisch gespeicherte Daten nicht verloren gehen oder gestohlen werden können, bzw. nicht zur Kenntnis oder in den Besitz unautorisierter Dritter gelangen. Die entsprechenden rechtlichen Anforderungen finden sich insbesondere in den Bereichen IT-Security, Datenschutz, gewerblicher Rechtsschutz, Geheimhaltungsvereinbarungen, Buchprüfung und Arbeitsrecht. Ein Mangel an Compliance auf diesen Gebieten kann zum Verlust von Rechtsschutz für betriebswichtiges Know-How oder geistiges Eigentum führen und Schadensersatzforderungen, Vertragsstrafen oder Geldbußen auslösen. Deshalb liegt der Einsatz einer wirksamen Data Leak Prevention Technologie eindeutig im Unternehmensinteresse. Im einzelnen sei hierzu noch auf folgendes hingewiesen:

Wenn etwa Sicherheitspannen dazu führen, dass betriebliches Know-How ungewollt an die Öffentlichkeit gelangt, kann dieses Know-How den Charakter eines „Betriebs- oder Geschäftsgeheimnisses“ und damit den wettbewerbsrechtlichen Know-How-Schutz gemäß § 17 des Gesetzes gegen den unlauteren Wettbewerb (UWG) verlieren.

Ein ungewollter Abfluss vertraulicher Informationen im Rahmen einer Sicherheitspanne kann ferner zu vertraglichen Ansprüchen Dritter führen, mit denen das Unternehmen, bei dem diese eingetreten ist, eine Vertraulichkeitsvereinbarung (Non-Disclosure Agreement, NDA) abgeschlossen hatte. Voraussetzung ist natürlich, dass gerade die von der Sicherheitspanne betroffenen Daten bzw. Informationen von der Vertraulichkeitsvereinbarung umfasst waren. Häufig werden in Vertraulichkeitsvereinbarungen auch Vertragsstrafen für den Fall einer unautorisierten Preisgabe geschützter Informationen an Dritte vereinbart. Ist die Sicherheitspanne allerdings trotz eines umfassenden IT-Sicherheitssystems eingetreten und kann dem betroffenen Unternehmen seine fahrlässige Verursachung auch sonst nicht vorgeworfen werden, so sollten sich vertragliche Ansprüche aus einer Vertraulichkeitsvereinbarung jedenfalls insoweit erfolgreich abwehren lassen, wie sie einen schuldhaften Verstoß gegen die Vertraulichkeitsvereinbarung voraussetzen. Mit Blick auf Vertragsstrafenklauseln ist zu beachten, dass diese häufig die Beweislastumkehr zulasten des Verpflichteten vorsehen, so dass von einer Sicherheitspanne betroffene Unternehmen ggf. beweisen müssen, dass sie diese nicht fahrlässig verursacht haben. Gerade dann zeigt sich aber, welchen Wert umfassende Maßnahmen zur IT- und Datensicherheit – und der Nachweis darüber – haben.

Eine Sicherheitslücke in einem in Deutschland befindlichen IT-System löst unter Umständen zusätzliche Benachrichtigungspflichten nach US-amerikanischem Recht aus. Es kommt vor, dass in Europa ansässige Unternehmen, bei denen eine Sicherheitspanne eintritt, von Betroffenen (oder deren Anwälten) in den USA benachrichtigt und – unter Vorbehalt der Geltendmachung aller Rechte einschließlich Schadensersatz und Mitteilung an die zuständigen Behörden – zur Einhaltung der anwendbaren „security breach notification laws“ angehalten werden.

### 4. Verpflichtung zur Verschlüsselung von E-Mails

Es bestehen zahlreiche Fallgestaltungen, bei denen entweder eine gesetzliche Verpflichtung besteht, E-Mail-Verschlüsselungstechnologien einzusetzen, wie etwa bei der öffentlichen Auftragsvergabe oder bei der elektronischen Übermittlung von Sozialdaten, oder bei denen eine E-Mail-Verschlüsselung zur Wahrung der Vertraulichkeit rechtlich geboten ist oder empfohlen wird. Dies gilt insbesondere für den Schutz von Betriebs- und Geschäftsgeheimnissen, personenbezogenen Daten, Sozialdaten sowie des Bankgeheimnisses und des Fernmeldegeheimnisses. Unternehmen und insbesondere Kreditinstitute und Finanzdienstleistungsinstitute haben zudem angemessene technische IT-Sicherheitsmaßnahmen zu etablieren, zu denen auch E-Mail-Verschlüsselungstechnologien zählen. Schließlich gibt es im E-Mail-Verkehr mit und von Behörden Fallgestaltungen, bei denen E-Mails verschlüsselt werden müssen. (Dies ist ein Kernelement des geplanten „Bürgerportalgesetzes“, das auch Unternehmen als elektronisch mit der Verwaltung korrespondierende „Staatsbürger“ betreffen dürfte.) Der Einsatz von E-Mail-Verschlüsselungstechnologien ist somit für Unternehmen, Kaufleute, Behörden und Selbstständige in vielen Bereichen rechtlich zwingend geboten.

# IV

## E-Mail- und Internet-Nutzung durch Mitarbeiter

*Die Nutzung von E-Mail und Internetzugang durch die Mitarbeiter eines Unternehmens für dessen eigene Zwecke wirft keine besonderen Rechtsprobleme auf. Anders sieht es jedoch aus, wenn es um die Nutzung dieser Arbeitsmittel für private Zwecke der Mitarbeiter geht.*

*Hier besteht ein großes Spannungsfeld, das durch Rechtsunsicherheit gekennzeichnet ist. In seiner umfassenden Stellungnahme 2/2010 (<http://www.anwaltverein.de/downloads/stellungnahmen/SN-10/SN0210.pdf>) hat der Arbeitsrechtsausschuss des Deutschen Anwaltvereins unter anderem auf das große Bedürfnis nach Rechtssicherheit im Zusammenhang mit der Nutzung von Telefon, E-Mail und Internet am Arbeitsplatz hingewiesen und gefordert, dass ein neues Arbeitnehmerdatenschutzrecht einen eindeutigen Rahmen für die Zulässigkeit der privaten Nutzung der betrieblichen Kommunikationsmittel, der Zugriffsrechte des Arbeitgebers und deren Grenzen festlegen sollte.*

### 1. Betriebliche Nutzung

Für die betriebliche Nutzung des ihnen jeweils zugeteilten E-Mail-Accounts und des Internetzugangs durch die Mitarbeiter eines Unternehmens gelten lediglich die Vorgaben des Bundesdatenschutzgesetzes (BDSG), insbesondere dessen §§ 4, 4a, 28 Abs. 1 Nr. 1 und Nr. 2. Der Arbeitgeber ist danach zur Kontrolle der Nutzung befugt, soweit die Kontrolle der Zweckbestimmung des Arbeitsverhältnisses dient oder zur Wahrung berechtigter Interessen des Arbeitgebers erforderlich ist und Interessen des Arbeitnehmers nicht überwiegen. Das gilt auch, wenn ein Arbeitnehmer Internet oder E-Mail-Account unerlaubt privat nutzt. (Zu etwaigen Missbrauchsfällen sh. Kapitel VI. Ziffer 2.)

### 2. Private Nutzung

Wird die private Nutzung erlaubt, ist nach wohl herrschender Meinung in der juristischen Literatur (sowie nach dem in Kapitel V. Ziffer 2 näher dargestellten Beschluss des OLG Karlsruhe) der Arbeitgeber als Diensteanbieter im Sinne des Telekommunikations-gesetzes (TKG) bzw. des Telemediengesetzes (TMG) anzusehen. Werden erlaubte private und betriebliche Nutzung nicht technisch getrennt, ist die gesamte Nutzung als privat zu qualifizieren. Der Arbeitgeber ist nach § 88 TKG zur Wahrung des Fernmeldegeheimnisses verpflichtet und unterliegt den datenschutzrechtlichen Anforderungen der §§ 91 ff. TKG und §§ 11 ff. TMG. Danach ist ohne Einwilligung des Arbeitnehmers eine Verarbeitung von Verbindungsdaten letztlich nur zu Abrechnungszwecken, aus Gründen der Systemsicherheit und zur Störungsbeseitigung zulässig. Ein Zugriff auf Inhaltsdaten zur Kontrolle des vereinbarten Nutzungsrahmens ist ohne Einwilligung unzulässig.

Dennoch sollte zum Schutz des Arbeitgebers eine Kontrolle von E-Mail-Nutzung und Internetzugang auch bei privater Nutzung erfolgen. Eine dahingehende Regelung kann er aber weder einseitig auf Grund seines Direktionsrechts noch mit der Arbeitnehmervertretung – etwa in Form einer Betriebsvereinbarung – treffen. (Letzteres kommt allenfalls für Aspekte einer damit zugleich möglichen Leistungskontrolle in Betracht.) Denn das Brief-, Post- und Fernmeldegeheimnis hat den Rang eines Individualgrundrechtes (Art. 10 des Grundgesetzes) und entzieht sich somit Einschränkungen durch eine Kollektivvereinbarung oder betriebliche Anweisungen.

Es bleibt also nur die Möglichkeit einer (unter dem Gesichtspunkt der Gleichbehandlung) einheitlich gestalteten **Vereinbarung mit jedem einzelnen Mitarbeiter**. (Wer sie nicht akzeptiert, hat dann auch keine private Nutzungsmöglichkeit.)



Diese Vereinbarung sollte mindestens das Folgende regeln:

- **Zielsetzung**
- **Umfang der E-Mail- und Internetnutzung**
- **Einwilligung in Protokollierung und Kontrolle**
- **Vertretungsregelung bei Ausscheiden oder längerer Krankheit des Mitarbeiters**
- **Leistungs- und Verhaltenskontrolle**
- **Datenschutz für E-Mail- und Internetnutzung**
- **Sanktionen**
- **Verhaltensgrundsätze (v.a. Beachtung der gesetzlichen Vorschriften)**

Wo allerdings die (gelegentliche) private Nutzung ohne eine solche vorherige Vereinbarung nur stillschweigend oder ausdrücklich (etwa durch einen Hinweis in Organisationsrichtlinien des Arbeitgebers) geduldet wird, kann daraus eine sog. "betriebliche Übung" erwachsen. Sie kann nur schwer – nämlich durch Änderungskündigungen – auf die Grundlage von Individualvereinbarungen umgestellt werden, in denen die bei erlaubter privater Nutzung unbedingt benötigten Regelungen getroffen werden.

Auch ein nachträgliches völliges Verbot der privaten Nutzung von betrieblichen E-Mail-Accounts ließe sich daher bei einer einmal entstandenen betrieblichen Übung kaum durchsetzen. Wenn jedoch ein solches Verbot wirksam geworden ist – aber auch wenn das Verbot schon bei erstmaliger Einführung von E-Mail im Unternehmen ausgesprochen worden ist –, muss seine Einhaltung durch Kontrollmaßnahmen bis hin zur Abmahnung und zu weiteren Konsequenzen durchgesetzt werden, um dem Entstehen einer (neuen) betrieblichen Übung vorzubeugen. (Dies ist dann wiederum ein Thema für den Betriebs- oder Personalrat.)

Das umfassende Verbot der privaten Nutzung von betrieblichen E-Mail-Accounts kann den Arbeitgeber zudem von rechtlichen Risiken des Einsatzes von Spamfiltern befreien (sh. dazu das nachfolgende Kapitel V.). Als Alternative für seine Mitarbeiter kann er ihnen den Internetzugang für die Nutzung ihrer privaten E-Mail-Accounts gestatten, sofern er es nicht auf sich nehmen will, ihnen ein zweites E-Mail-Account für die private Nutzung auf dem betrieblichen Server zu eröffnen. Das kann jedoch Probleme im Rahmen von Archivierungspflichten mit sich bringen.

Die erlaubte private Nutzung von betrieblichen E-Mail-Accounts hingegen kann den Arbeitgeber bzw. die für sein Handeln Verantwortlichen in die Nähe einer Strafbarkeit nach § 206 StGB bringen, wenn sie das danach geschützte Fernmeldegeheimnis ihrer Mitarbeiter verletzen sollten. Einen darauf gestützten Einwand hat allerdings das Verwaltungsgericht Frankfurt in einem Urteil vom 6. November 2008 (Az. 1 K 628/08.F (3)) nicht gelten lassen, nachdem die BaFin die Vorlage von E-Mails eines Mitarbeiters wegen Verdachts auf verbotenen Insiderhandel angeordnet hatte, obwohl dieser die Mail nach Kenntnisnahme selbst abgespeichert und archiviert hatte. Diese Entscheidung hat gezeigt, welche Sprengkraft für die arbeitsrechtlichen Beziehungen die erlaubte private Nutzung besitzt und wie groß der Regelungsbedarf für den Gesetzgeber ist.

# V

## Einsatz von Antiviren-Programmen und Spam-Filtern im Unternehmen

*In Kapitel II. wurde der notwendige Einsatz von Virenschutzprogrammen betont, der die IT-Security in Unternehmen sicherstellen kann. Aus rechtlichen Gründen sind besondere Voraussetzungen zu beachten.*

### 1. Strafbarkeit des Ausfilterns von E-Mails

§ 206 StGB stellt eine Verletzung des Post- oder Fernmeldegeheimnisses unter Strafe. Eine solche Verletzung liegt u. a. dann vor, wenn ein Unternehmen eine zur Übermittlung anvertraute Sendung unterdrückt. Der Begriff „des Unternehmens“ in dieser Strafvorschrift ist unterschiedlich zu deuten. Darunter fällt jede Betätigung im Geschäftsverkehr, die nicht ausschließlich hoheitlich erfolgt oder auf eine private Tätigkeit beschränkt ist. Unternehmen, die ihren Mitarbeitern auch die private E-Mail-Nutzung gestatten (vgl. Kapitel IV.), können sich der Verletzung des Post- oder Fernmeldegeheimnisses strafbar machen, wenn sie an einen Mitarbeiter adressierte E-Mails ausfiltern.

### 2. Zulässigkeit des Ausfilterns von E-Mails

Gemäß § 109 Abs. 1 Nr. 2 Telekommunikationsgesetz (TKG) müssen Diensteanbieter angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze der Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe treffen. Wie in Kapitel II. dargestellt, bestehen umfassende gesetzliche Anforderungen an die IT-Compliance. Daraus lässt sich ableiten, dass zumindest dann ein Ausfiltern von E-Mails zulässig ist, wenn eine E-Mail mit Viren behaftet ist. Diese könnte Störungen oder Schäden an den Telekommunikations- oder Datenverarbeitungssystemen des Unternehmens auslösen (so auch das OLG Karlsruhe in dem nachfolgend erwähnten Beschluss vom 10. Januar 2005).

Problematisch bleibt nach gegenwärtiger Rechtslage der Fall, dass ein Unternehmen Spam-E-Mails, also unverlangt zugesendete Werbe-E-Mails, löscht. So hatte das Oberlandesgericht Karlsruhe in einem Beschluss vom 10. Januar 2005 (Az. 1 Ws 152/04) entschieden, dass der Straftatbestand der Unterdrückung einer anvertrauten Sendung dann vorliegen kann, wenn der Arbeitgeber durch technische Eingriffe – Ausfiltern einer E-Mail – verhindert, dass die Nachricht den Empfänger vollständig und unverstümmelt erreicht.

Um drohender Strafbarkeit beim Einsatz von Spam-Filtern vorzubeugen, bieten sich folgende Lösungsmöglichkeiten an:

- **Dem Arbeitnehmer wird die private Nutzung seines dienstlichen E-Mail-Accounts untersagt (vgl. hierzu näher Kapitel IV. Ziffer 2).**
- **Der Arbeitnehmer stimmt dem Einsatz von Spam-Filtern zu.**
- **Die Spam-E-Mails werden in einen Quarantäne-Ordner verschoben, der betroffene Arbeitnehmer wird darüber informiert. Er hat so die Möglichkeit, die Spam-E-Mails entweder einzusehen oder sie ungesehen zu löschen.**

Nachdem für den Einsatz von Spam-Filtern bisher lediglich eine gerichtliche Entscheidung vorliegt und in der juristischen Literatur sehr unterschiedliche Auffassungen bestehen, sollte die Rechtsentwicklung beobachtet und die Rechtmäßigkeit des Einsatzes von Spam-Filtern in Unternehmen regelmäßig überprüft werden.

# Missbrauch von IT-Infrastruktur und Datendiebstahl



*Erfolgt ein Missbrauch von IT-Infrastruktur oder ein Datendiebstahl vorsätzlich, können strafrechtliche Konsequenzen eintreten. (Zur zivilrechtlichen und öffentlich-rechtlichen Verantwortlichkeit bei Verstößen gegen IT-Compliance-Anforderungen siehe Kapitel II. Ziffer 4)*

## 1. Ausspähen von Daten

§ 202a StGB stellt das Ausspähen von Daten unter Strafe. Geschützt werden nur solche Daten, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden. Erfasst werden auch nur solche Daten, die nicht für den Täter selbst bestimmt sind. Diese müssen gegen unberechtigten Zugang besonders gesichert sein. Das können z. B. softwaretechnische Schutzmaßnahmen wie Passwörter, Verschlüsselungen oder Zugangssicherungen der Hardware wie der mechanische Kopierschutz oder biometrische Verfahren sein. Eine alleinige Warnung, die Daten dürften nicht eingesehen werden, ist nicht ausreichend. Auch das Hacking, bei dem der Hacker für ihn nicht bestimmte Daten lediglich zur Kenntnis nimmt, ohne diese zu verändern, fällt aufgrund einer Gesetzesänderung vom August 2007 unter § 202a StGB; denn es ist bereits strafbar, sich oder einem anderen Zugang zu Daten zu verschaffen, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind. Damit wird das „Hacking“ unter Strafe gestellt, selbst wenn der Täter sich dadurch keine Daten verschafft. Zu diesen Attacken zählen unter anderem der Einsatz von Key-Logging-Trojanern, Sniffen oder Backdoorprogrammen.

## 2. Verletzung des Post- oder Fernmeldegeheimnisses

Gemäß § 88 TKG unterliegt der Inhalt der Telekommunikation und ihre näheren Umstände dem Fernmeldegeheimnis, wozu insbesondere auch die Tatsache zählt, ob jemand an einem bestimmten Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich zudem auf die näheren Umstände erfolgloser Verbindungsversuche.

Nach § 206 StGB ist es strafbar, wenn eine unbefugte Mitteilung über den Inhalt privater E-Mail-Korrespondenz an andere oder die Unterdrückung der Weiterleitung privater E-Mails gesendet wird. Sofern die private E-Mail-Nutzung untersagt ist, kann der Arbeitgeber grundsätzlich davon ausgehen, dass sämtliche E-Mail-Korrespondenz dienstlich veranlasst ist, und somit deren Vorlage verlangen. Ein direkter Zugriff des Vorgesetzten auf das Postfach des Mitarbeiters wird in der Regel unzulässig sein, weil der Mitarbeiter auch dienstlich veranlasste E-Mails erhalten kann, deren Inhalt dem Vorgesetzten nicht zur Kenntnis gelangen soll, z.B. Korrespondenz mit der Personalabteilung, dem Betriebsrat oder dem Betriebsarzt.

## 3. Datenveränderung

§ 303a StGB stellt die rechtswidrige Löschung, Unterdrückung, Unbrauchbarmachung oder Veränderung von Daten unter Strafe. Darunter fallen nur fremde Daten, an denen eine andere Person ein unmittelbares Recht auf Verarbeitung, Löschung oder Nutzung hat. Erfasst wird auch das „logische“ Verstecken von Daten, das zu einer Einschränkung der Verwendbarkeit führt. Dies kann beispielsweise durch die unbefugte Umbenennung von Dateien oder die Einfügung von Zugriffsbeschränkungen erfolgen.

#### 4. Computersabotage

§ 303b StGB regelt die Computersabotage. Darunter fallen unter anderem Störungen der Datenverarbeitung und erhebliche Beeinträchtigungen der reibungslosen Datenverarbeitung. Viren-Attacken können als Computersabotage strafbar sein. Nach einem Beschluss des Oberlandesgerichts Frankfurt am Main vom 22. Mai 2006 (Az. 1 Ss 319/05) stellte eine zweistündige Blockade der Internetseite von Lufthansa keine strafbare Computersabotage oder Datenveränderung dar, weil es sich hierbei nur um einen zeitlich befristeten Denial of Service (DoS)-Angriff handelte, der gesetzlich nicht erfasst war. Durch eine Änderung des § 303b StGB sind solche Denial of Service-Attacken seit August 2007 ebenfalls verboten. In besonders schweren Fällen wird eine Freiheitsstrafe von bis zu zehn Jahren angedroht.

#### 5. Vorbereitung des Ausspähens und Abfangens von Daten

Nach § 202c StGB ist die Vorbereitung von Taten nach §§ 202a oder 202b StGB strafrechtlich relevant, wenn der Täter Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten ermöglichen, oder Computerprogramme, deren Zweck die Begehung einer solchen Straftat ist, herstellt oder sich verschafft. Sanktioniert wird hierdurch das Herstellen, Überlassen, Verbreiten oder Verschaffen von „Hacker-Tools“, die nach Art und Weise ihres Aufbaus illegalen Zwecken dienen können. Allgemeine Programmier-Tools, -Sprachen oder sonstige Anwendungsprogramme fallen nicht unter diese Strafvorschrift, selbst wenn sie zum Hacken eingesetzt werden. In einem Beschluss vom 18. Mai 2009 (Az. 2 BvR 2233/07) hat das Bundesverfassungsgericht dies klargestellt und entschieden, dass Dual Use-Tools nicht unter § 202c StGB fallen. Werden Computerprogramme im Sinne dieser Vorschrift beschafft oder weitergegeben, um im Rahmen von Penetrations- und Sicherheits-Tests im Auftrag und somit im Einverständnis mit den über die überprüften Computersysteme Verfügungsberechtigten verwendet zu werden, fehlt es am Tatbestandsmerkmal des „unbefugten Handelns“, so dass insoweit auch Schadprogramme, deren objektiver Zweck in der Begehung von Computerstraftaten liegt, beschafft oder weitergegeben werden dürfen - und zwar auch dann, wenn aufgrund der Herkunft der Programme der Verdacht nahe liegt, dass andere Nutzer keine lauterer Absichten verfolgen.

#### 6. Fälschung beweisheblicher Daten

§ 269 StGB stellt die Fälschung beweisheblicher Daten unter Strafe. Demnach ist es verboten, im Rechtsverkehr beweishebliche Daten derart zu speichern oder zu verändern, dass sie bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde hervorbringen würden. Dieser Straftatbestand lässt sich als „elektronische Urkundenfälschung“ verstehen.

#### 7. Störung von Telekommunikationsanlagen

Nach § 317 StGB ist strafbar, wer den Betrieb einer öffentlichen Zwecken dienenden Telekommunikationsanlage dadurch verhindert oder gefährdet, dass eine hierfür dienende Sache zerstört, verändert oder unbrauchbar gemacht oder der Strom abgestellt wird. Dieser Straftatbestand ist z.B. dann erfüllt, wenn der E-Mail-Verkehr einer Behörde durch einen Viren-Angriff nicht nur kurzzeitig zum Erliegen kommt.



## 8. Verrat von Geschäfts- und Betriebsgeheimnissen

§ 17 UWG stellt den Verrat von Geschäfts- und Betriebsgeheimnissen und die Betriebsespionage unter Strafe. Mitarbeiter machen sich strafbar, wenn sie unbefugt Geschäfts- und Betriebsgeheimnisse an Dritte weitergeben. Ebenso macht sich strafbar, wer sich zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder um den Inhaber des Unternehmens zu schädigen, ein Geschäfts- oder Betriebsgeheimnis durch Anwendung technischer Mittel verschafft. Darunter fällt insbesondere das „Anzapfen“ von EDV-Anlagen und Datenfernleitungen.

## 9. Datenschutzdelikte

Verstöße gegen Datenschutzrecht können gemäß §§ 43, 44 BDSG eine Geldbuße, eine Geldstrafe oder eine Freiheitsstrafe bis zu zwei Jahren nach sich ziehen. Dazu zählt beispielsweise die unbefugte Erhebung, Verarbeitung, der Abruf oder die Erschleichung der Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, in Bereicherungs- oder Schädigungsabsicht.

Das Ausspähen von Daten und der Angriff auf die IT-Infrastruktur von Unternehmen können nach diversen Vorschriften strafbar sein. Sofern ein Unternehmen von eigenen Mitarbeitern geschädigt wird, kann es mit arbeitsrechtlichen Maßnahmen (Abmahnung, fristlose Kündigung), Schadensersatzansprüchen und gegebenenfalls einer Strafanzeige reagieren. Sollte ein Mitarbeiter das IT-System seines Arbeitgebers zur Durchführung solcher strafbarer Handlungen benutzen und so Dritte schädigen, kann das Unternehmen hierfür gegebenenfalls zivilrechtlich haftbar gemacht werden, falls es nicht ausreichende Sicherheitsvorkehrungen gegen einen solchen Missbrauch getroffen hat. Eine strafbare Verantwortlichkeit der Geschäftsführung für strafbare Handlungen eines Mitarbeiters, die dieser „privat“ begangen hat, scheidet in aller Regel mangels Vorsatz aus.

# VTIT

## Elektronischer Rechtsverkehr

*Sofern Unternehmen unter Einsatz von E-Mail und Internet am Rechtsverkehr teilnehmen, sollten sie sich darüber im klaren sein, dass sie dadurch in gleicher Weise rechtlich gebunden werden, wie bei anderen Rechtsgeschäften. Im Bereich des E-Commerce sind zahlreiche rechtliche Anforderungen und Bestimmungen zu beachten. Diese können im Rahmen dieses Leitfadens nur kurz skizziert werden und sind von Fall zu Fall eingehend rechtlich zu überprüfen.*

### 1. Vertragsabschluss über das Internet

Auch über E-Mail oder Internetseiten können rechtswirksame Verträge geschlossen werden, sofern der Vertrag keiner besonderen Formvorschrift unterliegt.

Der Austausch von E-Mails hinsichtlich Angebot und Annahme eines Kaufvertrages ist ebenso bindend, wie die Übersendung eines unterschriebenen Vertrages als PDF-Datei statt per Telefax. Auch die Bestellung von Waren, der Software-Download über einen Online-Shop oder der Zuschlag bei einem Internet-Auktionsverfahren führt zu einem wirksamen Vertragsabschluss.

### 2. Zugangs- und Beweisregelungen

Grundsätzlich gilt, dass die Person, die sich auf die Wirksamkeit einer empfangsbedürftigen Willenserklärung beruft, deren Zugang beweisen muss. So lässt sich z. B. ein Zeitschriften-Abonnement – sofern vertraglich nichts anderes vereinbart ist – per E-Mail kündigen. Allerdings muss der Absender der E-Mail, hier der Kündigende, deren Zugang nachweisen, sofern der Empfänger bestreitet, die E-Mail erhalten zu haben. Kann er dies nicht, ist die Kündigung unwirksam. Im Normalfall kann er diesen Beweis nicht erbringen. Ebenso wie ein Telefax-Sendebericht von der Rechtsprechung nicht als Beweis des Zugangs eines Telefax anerkannt wird, ist eine E-Mail-Empfangsbestätigung kein ausreichender Beweis. Einzig eine Lesebetätigung des Empfängers kann unter Umständen einen Anscheinsbeweis für deren Zugang begründen. Im Zweifelsfalle sollte der Absender einer Erklärung sich also deren Zugang per E-Mail bestätigen lassen.

### 3. Elektronische Signatur

Beim Austausch von E-Mails im Internet besteht die Gefahr, dass diese entweder nicht von der Person stammen, die sich als Absender ausgibt, oder diese E-Mails von unbefugten Dritten verändert worden sind. Um die Integrität und Authentizität im elektronischen Rechtsverkehr sicherzustellen, also um einer Verfälschung des Inhalts vorzubeugen und den Sender der E-Mail eindeutig identifizieren zu können, wurde das elektronische Signaturverfahren eingeführt. Eine elektronische Signatur ist ein mit einem geheimen Schlüssel erzeugtes elektronisches Dokument. Dieses hat eine kryptographische Prüfsumme, die mit dem öffentlichen Schlüssel des Urhebers überprüft werden kann. Die elektronische Signatur ist im sog. Signaturgesetz sowie der Signaturverordnung näher geregelt. Es gibt sie in drei unterschiedlichen Stufen, der „elektronischen Signatur“ der „fortgeschrittenen elektronischen Signatur“ und der „qualifizierten elektronischen Signatur“.

Nur die Verwendung der qualifizierten elektronischen Signatur nach dem Signaturgesetz, gemeinsam mit dem Namen des Ausstellers, erfüllt die sog. „elektronische Form“, die gemäß § 126a BGB der Schriftform gleichsteht. Allerdings ist zu berücksichtigen, dass einige Vorschriften weiterhin ausdrücklich die Schriftform erfordern und die elektronische Form explizit ausschließen.

Ein Beispiel ist die Bürgschaftserklärung, die in Schriftform erfolgen muss. Hingegen ist die Bürgschaftserklärung des Kaufmanns gemäß § 350 HGB formfrei, solange sie ein Handelsgeschäft betrifft.

Werden in einem Gerichtsverfahren private elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, vorgelegt, haben sie die gleiche Beweiskraft wie private Urkunden.

#### **4. Anforderungen an den elektronischen Geschäftsverkehr**

Unternehmen, die ihre Waren oder Dienstleistungen über den elektronischen Weg bzw. das Internet anbieten, unterliegen zahlreichen rechtlichen Anforderungen. Gemäß § 5 Telemediengesetz (TMG) müssen sie über ihren Namen, ihre Anschrift, ihre Handelsregisternummer, die zuständige Aufsichtsbehörde, ihre Umsatzsteueridentifikationsnummer oder Wirtschafts-Identifikationsnummer sowie über Möglichkeiten für eine schnelle elektronische Kontaktaufnahme informieren. Ferner sind sie dazu verpflichtet, technische Mittel zur Verfügung zu stellen, mit deren Hilfe der Kunde Eingabefehler vor Abgabe seiner Bestellung erkennen und berichtigen kann. Der Zugang einer Bestellung ist dem Kunden unverzüglich auf elektronischem Wege zu bestätigen. Des Weiteren muss dem Kunden möglich sein, die Vertragsbestimmungen einschließlich der Allgemeinen Geschäftsbedingungen bei Vertragsschluss abzurufen und in wiedergabefähiger Form zu speichern.

Sofern ein Unternehmen seine Waren oder Dienstleistungen gegenüber Verbrauchern anbietet, bestehen zusätzlich umfassende Informationspflichten. Zudem hat der Verbraucher ein Widerrufsrecht. Demzufolge kann der Verbraucher den Vertrag ohne Angaben von Gründen gegenüber dem Unternehmen innerhalb von zwei Wochen oder – falls die Widerrufsbelehrung in Textform erst nach Vertragsschluss erfolgt – einem Monat ab Erhalt der Ware bzw. bei Dienstleistungen ab Vertragsschluss widerrufen. Die Muster-Widerrufsbelehrung hat in den letzten Monaten wiederholt Änderungen erfahren und für Juni 2010 stehen weitere Änderungen an. Um von der gesetzlichen Schutzwirkung der Muster-Widerrufsbelehrung zu profitieren, ist Unternehmen, die Internet-Shops für Verbraucher betreiben, dringend zu empfehlen, dieses Muster in der jeweils aktuellen Fassung zu verwenden. Je nachdem, ob Waren geliefert und/oder Dienstleistungen erbracht werden, sind unterschiedliche im Muster vorgegebene Formulierungen zu verwenden und Gestaltungshinweise zu berücksichtigen.

#### **5. Unternehmensangaben auf geschäftlichen E-Mails**

Seit 1. Januar 2007 sind alle Unternehmen, die nach Handelsrecht oder gesellschaftsrechtlichen Vorschriften Pflichtangaben in ihre Geschäftsbriefe aufnehmen müssen, also Einzelkaufleute, OHG, KG, Partnerschaftsgesellschaft, Genossenschaft, AG und GmbH (einschließlich Unternehmersgesellschaft) sowie die Europäische Genossenschaft (SCE) und die Europäische Gesellschaft (SE), verpflichtet, die auf den Geschäftsbriefen gemachten Angaben auch in ihre E-Mail-Signatur zu übernehmen, die jeder ausgehenden E-Mail automatisch angefügt wird. Solche Pflichtangaben umfassen insbesondere Firma, Rechtsform und Sitz der Gesellschaft, Handelsregisterangaben und die Namen aller Geschäftsführer.

## Elektronische Rechnungsstellung

*Durch Electronic Invoicing, also die elektronische Rechnungsstellung für Warenlieferungen oder sonstige Leistungen, bietet sich Unternehmen ein erhebliches Kosteneinsparungspotential, meist sogar eine zusätzliche Prozessoptimierung. Ein Unternehmen – insbesondere wenn es digitale Güter wie Software oder elektronische Dienstleistungen wie Service Providing oder Remote-Pflege anbietet – kann einen Medienbruch vermeiden, wenn es die Rechnungen für seine Leistungen ebenfalls elektronisch statt auf dem Postwege versendet. Solche Rechnungen können direkt aus dem Warenwirtschaftssystem erstellt und versendet werden und sparen somit Personal- und Portokosten ein.*

Damit jedoch der Kunde den ausgewiesenen Umsatzsteuerbetrag auch als Vorsteuer verrechnen kann, ist die Vorlage einer ordnungsgemäßen Rechnung erforderlich. Das leistende Unternehmen ist dazu gesetzlich verpflichtet. Neben der Rechnungsversendung per Post, Telefax oder über das EDI-Verfahren besteht gesetzlich auch die Möglichkeit der Versendung einer elektronischen Rechnung. Dabei handelt es sich um eine elektronische Datei, etwa im PDF-Format, die per E-Mail übermittelt wird. Damit die Finanzverwaltung eine solche elektronische Rechnung anerkennt, ist u. a. erforderlich, die Echtheit der Rechnungsherkunft und die Unversehrtheit des Rechnungsinhalts zu gewährleisten. Wird die Rechnung in Deutschland erstellt, ist der Einsatz einer qualifizierten elektronischen Signatur erforderlich, die den Vorgaben des Signaturgesetzes entsprechen muss. Zudem müssen die elektronisch versendeten und empfangenen Rechnungen, einschließlich der gemäß der qualifizierten elektronischen Signatur erstellten Protokolle, ordnungsgemäß elektronisch archiviert werden. Zusätzlich muss der Rechnungsempfänger der elektronischen Übermittlung zugestimmt haben, was auch durch stillschweigende Annahme der elektronischen Rechnung zum Ausdruck gebracht werden kann.

Wenn nicht sichergestellt ist, dass die gesetzlichen Anforderungen an die elektronische Rechnungsstellung, wie sie insbesondere im Umsatzsteuergesetz und dem Signaturgesetz geregelt sind, eingehalten werden, besteht die Gefahr, dass die Finanzverwaltung solche Rechnungen nicht anerkennt.



Rechtsanwalt Günter Untucht, Trend Micro, Associate General Counsel & Director of EMEA Legal



Rechtsanwalt und Fachanwalt für Informationstechnologierecht Dr. Thomas Stögmüller, LL.M. (Berkeley), teclegal Habel Rechtsanwälte





Securing Your Web World

**Trend Micro Deutschland GmbH**

Zeppelinstraße 1  
85399 Hallbergmoos  
Tel.: +49 (0) 811 / 88 99 0 - 700  
Fax: +49 (0) 811 / 88 99 0 - 799

**[www.trendmicro.com](http://www.trendmicro.com)**