

# Internet und IT-Security im Unternehmen

Juristische Informationen für die Unternehmensleitung

2. Auflage







# 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 Unternehmen 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.



## 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. die Verletzung des Telekommunikationsgeheimnisses, das missbräuchliche Abfangen von Daten oder die Verletzung 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.

Im Auftrag der Informations- und Kommunikationstechnik-Stabstelle des Bundes hat A-SIT (Zentrum für sichere Informationstechnologie - Austria) das Österreichische Informationssicherheitshandbuch im Jahr 2007 aktualisiert. Das Handbuch befasst sich im Wesentlichen mit IT-Sicherheit und Querschnittstellen zum Schutz von Informationen unabhängig von ihrer Darstellungsform.

Das Handbuch richtet sich sowohl an die öffentliche Verwaltung als auch an die Wirtschaft und versteht sich als Sammlung von Leitlinien und Empfehlungen. Es stellt eine Ergänzung zu den bestehenden Regelungen und Vorschriften (wie z.B. Datenschutzrecht) dar.

Ergänzend hat die österreichische Wirtschaftskammer Ende 2009 das aktuelle IT-Sicherheitshandbuch veröffentlicht. Dieses Handbuch umfasst Themen wie Risikomanagement, Datensicherung, Internetzugang, Virenschutz, Computersicherheit, personelle, bauliche und infrastrukturelle Maßnahmen und Einhaltung rechtlicher Vorgaben.

Folgende Aspekte stehen im Vordergrund:

### 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.

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.

Das Österreichische Informationssicherheitshandbuch beschäftigt sich auch mit der Datensicherung und sieht dabei folgende Maßnahmen vor:

- **regelmäßige Datensicherung,**
- **Entwicklung eines Datensicherungskonzeptes,**
- **Festlegung des Minimaldatensicherungskonzeptes,**
- **Beschaffung eines geeigneten Datensicherungssystems,**
- **Sicherungskopie der eingesetzten Software,**
- **Verpflichtung der Mitarbeiter zur Datensicherung.**

### **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**

Der österreichische Corporate Governance Kodex wurde am 1. Oktober 2002 veröffentlicht. Er stellt den Maßstab für gute Unternehmensführung und Unternehmenskontrolle am österreichischen Kapitalmarkt dar und wird jährlich anhand nationaler und internationaler Entwicklungen modernisiert. Seit dem Unternehmensrechts-Änderungsgesetz 2008 haben alle börsennotierten Unternehmen den Corporate Governance Bericht verpflichtend zu erstellen, der insbesondere auch eine Erklärung über etwaige Abweichungen vom Kodex vorsieht (sog. Comply or Explain – Prinzip). Der Kodex richtet sich grundsätzlich an börsennotierte Unternehmen, kann aber auch von anderen als Leitlinie ordnungsgemäßer und transparenter Unternehmensführung herangezogen

werden. Die Unternehmen können sich dem Kodex freiwillig unterwerfen.

Der Kodex betrifft vor allem die Arbeitsweise der Leitungsorgane, ihre Zusammenarbeit und die Kontrolle ihres Verhaltens. Dabei wird nicht nur eine optimale Unternehmensführung, sondern auch eine allgemeine Überwachung dieser Führung, Kontrolle und Transparenz beschrieben, wozu auch eine optimale IT-Security des Unternehmens gehört. Im Kapitel „Transparenz und Prüfung“ werden insbesondere die Aufstellung des Corporate Governance Berichts, die Rechnungslegung und die Kommunikationseinrichtungen geregelt. Danach hat die Gesellschaft bei der Erstellung ihres Corporate Governance Berichts die Pflichtangaben gemäß § 243 b UGB und bei Erstellung ihres Konzernabschlusses die internationalen Rechnungslegungsstandards (wie z.B. IAS 34, IFRS und US-GAAP) zu beachten. Der Kodex besagt weiters, dass das Unternehmen über die gesetzlichen Mindestforderungen hinaus eine externe Kommunikation etablieren soll, die Informationsbedürfnisse zeitnah und ausreichend deckt, wie z.B. Verfügungstellung von Finanz- und Konzernberichten auf der Webseite der Gesellschaft, unverzügliche Bekanntmachung von Insider-Informationen, die die Gesellschaft unmittelbar betreffen oder Darstellung eines Finanzkalenders auf der Webseite der Gesellschaft. Bei der Etablierung dieser Maßnahmen hat das Unternehmen auch die IT-Sicherheit zu beachten und die entsprechenden Vorkehrungen zu treffen.

Gemäß § 82 AktG und § 22 Abs 1 GmbHG sind Kapitalgesellschaften allgemein verpflichtet ein internes Kontrollsystem (IKS) zu führen. Das IKS muss den Anforderungen des Unternehmens entsprechen und individuelle, aufeinander abgestimmte und sich ergänzende Methoden und Maßnahmen für die Organisation eines Unternehmens vorsehen, die dazu dienen, Fehler zu verhindern und die Einhaltung vorgegebener Normen zu gewährleisten, um insbesondere

- **die Vollständigkeit und Richtigkeit der geschäftlichen Aufzeichnungen zu sichern,**
- **die vorhandenen Vermögenswerte zu sichern,**
- **die betriebliche Leistungsfähigkeit zu steigern,**
- **die Geschäftsführung bei ihrer Überwachungsaufgabe zu unterstützen.**

Das IKS umfasst alle dafür von der Geschäftsleitung angeordneten organisatorischen Methoden und Maßnahmen. Die Elemente des IKS sind:

- **Risikobeurteilung,**
- **Kontrollumfeld,**
- **Kontrolltätigkeiten,**
- **Information und Kommunikation.**

Es ist also ein unternehmensweites Risikomanagement zu installieren. Teil der Risikoprävention ist dabei der Schutz der IT-Infrastruktur, also die Sicherstellung der IT-Security.

Die Unternehmensleitung ist dafür verantwortlich, wirksame Maßnahmen zum Schutz der IT-Infrastruktur zu treffen (wie z.B. Datensicherung gegen Datenverlust, Datenmissbrauch) und ein entsprechendes Risikomanagement einzurichten. Sollten Geschäftsführer bzw. Vorstände diese Pflicht verletzen und das Unternehmen dadurch Schaden erleiden, könnten sie gegenüber ihrem Unternehmen persönlich haften.

Aber auch Unternehmensmitarbeiter können bei Verstößen gegen die Anforderungen der IT-Sicherheit gegebenenfalls wegen Verletzung ihrer arbeitsvertraglichen Pflichten in Anspruch genommen werden.

Nach der durch das Unternehmensrechts-Änderungsgesetz 2008 neu eingeführten Vorschrift § 243a UGB müssen nunmehr kapitalmarktorientierte Gesellschaften die wichtigsten Merkmale des IKS und des Risikomanagement auch in ihrem Lagebericht anführen.

**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.

Aus der Sarbanes-Oxley Act ergibt sich auch die Verpflichtung von europäischen Tochterunternehmen sog. „Whistleblowing“-Hotlines als internes Kontrollsystem zu führen, bei denen Mitarbeiter interne Missstände aufzeigen können bzw. müssen. In Österreich sind die von der Datenschutzkommission aufgestellten Anforderungen an die Genehmigung der Whistleblowing-Systeme zu beachten.

Wirtschaftsprüfer können bei börsennotierten Aktiengesellschaften das Testat im Rahmen der Jahresabschlussprüfung verweigern, wenn die IT-Sicherheitsstandards unzureichend sind. Das Anfang Juni 2008 in Kraft getretene Unternehmensrechts-Änderungsgesetz, das die EU-Abschlussprüferrichtlinie (so etwas wie ein „Euro-SOX“) in österreichisches Recht umsetzt, verschärft die Anforderungen an Abschlussprüfer. Zudem ist die Wirksamkeit des internen Kontroll- und Risikomanagementsystems kapitalmarktorientierter Unternehmen nach der daraus resultierenden Änderung des Corporate Governance Kodex von 2009 durch den Aufsichtsrat oder einen von ihm bestellten Prüfungsausschluss besser zu kontrollieren. Auch wenn nach diesen Gesetzesänderungen 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. Abzuwarten sein wird, welche Standards der Vorstand einer Aktiengesellschaft bei der seit dem Aktienrechts-Änderungsgesetz 2009 neu eingeführten Fernabstimmung (§§ 126, 102 Abs 3 Z 3 AktG) im Rahmen der Hauptversammlung in puncto IT-Sicherheit einzuhalten haben wird.

Öffentliche Auftraggeber könnten im Rahmen der Leistungsbeschreibung bei IT-relevanten Aufträgen einen Nachweis über die IT-Sicherheit fordern. 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 könnte sogar die gewerberechtliche Befähigung 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 infi-



zierten 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.

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 Datenschutzgesetzes 2000, idF BGBl I Nr 135/2009 (DSG) zu beachten. Hierbei ist besonderes Augenmerk darauf zu richten, dass auch eine Datenübermittlung innerhalb des Konzerns dem DSG entsprechen muss, insbesondere, wenn Daten an eine Konzerngesellschaft außerhalb der EU übermittelt werden.

§ 14 DSG sieht bestimmte Maßnahmen zur Gewährleistung der Datensicherheit vor, wie z.B.:

- |                     |                        |                          |
|---------------------|------------------------|--------------------------|
| • Zutrittskontrolle | • Zugriffskontrolle    | • Auftragskontrolle      |
| • Zugangskontrolle  | • Verwendungskontrolle | • Maßnahmendokumentation |

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 § 14 DSG vom Auftraggeber ausgewählt werden. Die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse sind in dem entsprechenden Auftrag schriftlich festzulegen. Zudem muss der Auftraggeber sich von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen des Auftragnehmers überzeugen.

Wer vorsätzlich personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich gemacht geworden sind oder die er sich widerrechtlich verschafft

hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schützwürdiges Interesse hat, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen (§ 51 DSGVO) § 52 DSGVO sieht eine Geldstrafe bis zu EUR 25.000 vor, wenn jemand Daten vorsätzlich in Verletzung des Datengeheimnisses übermittelt oder für andere Zwecke verwendet.

Außerdem besteht seit der DSGVO-Novelle 2010 nach § 24 Abs 2a DSGVO eine gesetzliche Pflicht zur Benachrichtigung des Betroffenen, falls das Unternehmen Kenntnis von einer systematischen und schwerwiegenden unrechtmäßigen Verwendung personenbezogener Daten Dritten erlangt. Dies soll vor allem der Vermeidung von Vermögensschäden der Betroffenen dienen. 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**

Das DSGVO stellt Datensicherheitsmaßnahmen und die Geheimhaltung der personenbezogenen Daten in den Vordergrund. Der Verwender hat sicherzustellen, dass die Daten vor zufälliger und unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind. Das DSGVO macht die Datensicherung zur gesetzlichen Pflicht. Danach gilt Datensicherung als notwendiges Instrument für den Schutz personenbezogener Daten.

Sofern ein Unternehmen kein regelmäßiges Backup seiner Daten und seiner IT-Systeme durchführt, ist im Falle eines durch Datenverlust entstehenden Schadens ein „haftungsreduzierendes Mitverschulden“ zu befürchten. 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, könnte aufgrund dieses grob fahrlässigen Außerachtlassens von Sicherheitsvorkehrungen auch ein Verlust des Versicherungsschutzes drohen.

### **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 beachtet werden.

In Betrieben ohne Betriebsrat unterliegt die Einführung und Verwendung von Kontrollmaßnahmen und technischen Einrichtungen der Zustimmung der betroffenen Arbeitnehmer. Eine solche Zustimmung kann in der Regel gekündigt werden.

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

Auch wenn es sich um keine für Unternehmen verbindliche Richtlinie handelt, stellen das Österreichische Informationssicherheitshandbuch ([www.bka.gv.at/site/5743/default.aspx](http://www.bka.gv.at/site/5743/default.aspx)) und das IT-Sicherheitshandbuch der österreichischen Wirtschaftskammer ([www.portal.wko.at](http://www.portal.wko.at)) eine wichtige Handlungsanleitung für die praktische Umsetzung von IT-Compliance-Anforderungen dar. Anhand dieser Handbücher können Unternehmen ein angemessenes IT-Sicherheitsniveau erreichen. Die Standards des Österreichischen IT-Sicherheitshandbuches enthalten Empfehlungen zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen zur Informationssicherheit.

Der Grad der Sicherheit von IT-Systemen im Unternehmen wird überdies durch internationale Sicherheitsstandards definiert. Hier kommen insbesondere folgende Standards zur Anwendung: Die ISO-Standards 13335, 17799 und A7799 (dies ist der BS7799, der in der ISO bzw. der ÖNORM übernommen wurde) sowie die „IT Infrastructure Library“ (ITIL) können unter anderem als Best Practice-Vorgaben herangezogen werden. Auch eine Zertifizierung des Informationssicherheits-Managementsystems nach ISO 27001 ist möglich. Beachtet werden weiters das British Standard 7799 und das IT Grundschriftbuch des Bundesamt für Sicherheit in der Informationstechnologie in Deutschland. 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 4.0 veröffentlicht worden ist (kostenlos abrufbar unter [www.itgi.org](http://www.itgi.org)).

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

Die Kammer der Wirtschaftstreuhänder Österreich (KWT) hat verschiedene Prüfungsstandards wie z.B. KFS/DV1 (Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Informationstechnologie) mit verstärktem Bezug auf Datensicherheit und Datenschutz und KFS/DV2 (Richtlinie zur Prüfung der IT im Rahmen von Jahresabschlussprüfungen) herausgegeben, die bei Abschlussprüfungen zu beachten sind ([www.kwt.or.at](http://www.kwt.or.at)).

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

§§ 190, 212, 216 UGB iVm §§ 125 ff BAO enthalten Anforderungen an die Führung der Handelsbücher und die Aufbewahrung der Unterlagen.

Der Unternehmer kann zur ordnungsgemäßen Buchführung und zur Aufbewahrung seiner Geschäftsbriefe Datenträger benützen. Nach § 190 Abs 5 UGB 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. Die inhaltliche Übereinstimmung der Wiedergabe mit den auf den maschinell lesbaren Datenträgern geführten Unterlagen muss durch das jeweilige Archivierungsverfahren sichergestellt sein.

Der Unternehmer hat seine Bücher sieben Jahre lang geordnet aufzubewahren. Es ist sicherzustellen, dass auch bei einer Erneuerung der IT-Infrastruktur oder einer Datenmigration das Unternehmen den Vorschriften des UGB gerecht wird.

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

Das Bankwesengesetz (BWG) sowie § 30 Wertpapieraufsichtsgesetz (WAG) 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 Finanzmarktaufsicht (FMA) beeinträchtigt werden. In entsprechenden Rundschreiben der FMA werden diese Anforderungen konkretisiert sowie Mindestanforderungen an das Risikomanagement 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 Kommunikationsgeheimnisses oder die Verletzung von Datenschutzvorschriften in Bereicherungsabsicht - sind mit Geld- oder Freiheitsstrafe bedroht.

### b) Verwaltungsübertretung

Verstöße gegen öffentlich-rechtliche Regelungen, wie das Datenschutzgesetz, können eine Verwaltungsübertretung darstellen und Geldstrafen 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 schadenersatzpflichtig 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, im Extremfall eine Abmahnung oder Entlassung nach sich ziehen.

Auch ein Verstoß gegen ein Verbot der privaten E-Mail- und Internetnutzung (siehe Kapitel IV.) kann einen Entlassungsgrund darstellen. So hat zum Beispiel der Oberste Gerichtshof in seiner Entscheidung (OGH 05.11.1997, ARD 4937/33/98) ausgesprochen, dass die private Verwendung des Computers und von Computerprogrammen des Arbeitgebers einen Entlassungsgrund darstellt, wobei es nicht darauf ankommt, ob der Arbeitnehmer dabei weisungswidrig auch fremde Software installiert hat, oder ob die Installation privater Programme überdies geeignet war, Viren einzubringen.

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



## 1. „IT-Grundrecht“

Das Bundesverfassungsgericht in Deutschland hat bereits 2008 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.

Eine entsprechende Entwicklung ist in Österreich noch nicht zu vermelden. Die Neuformulierung des Grundrechts auf Datenschutz in § 1 DSGVO durch die DSGVO-Novelle 2010 sorgte nur für bessere Verständlichkeit ohne inhaltliche Änderungen. Eine Rechtsprechung nach dem deutschen Vorbild für das Auditing datenschutzkonformer Datenanwendungen bleibt abzuwarten.

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

Obwohl bereits im Jahre 2008 ein Ministerialbericht zum Thema Online-Durchsuchung in Österreich vorgelegt wurde, hat eine gesetzliche Regelung noch keinen Eingang in die Strafprozessordnung gefunden. Die technische Durchführung der Online-Durchsuchung ist demnach noch unklar. Aller Voraussicht nach werden von Fall zu Fall individuelle Einzelanfertigungen als „Ermittlungssoftware“ programmiert. 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. Es ist aber davon auszugehen, dass technische Selbstschutzmöglichkeiten wie Antiviren-Programme eingesetzt werden dürfen, 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 § 11 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 Österreich 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 eine E-Mail-Verschlüsselung zur Wahrung der Vertraulichkeit rechtlich geboten ist oder empfohlen wird, wie etwa bei der öffentlichen Auftragsvergabe oder bei der elektronischen Übermittlung von Sozialdaten. Dies gilt insbesondere für den Schutz von Betriebs- und Geschäftsgeheimnissen, personenbezogenen Daten, Sozialdaten sowie des Bankgeheimnisses und des Kommunikationsgeheimnisses. 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. Der Einsatz von E-Mail-Verschlüsselungstechnologien ist somit für Unternehmen, Kaufleute, Behörden und Selbstständige in vielen Bereichen rechtlich zwingend geboten.

# 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.*

## 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 Datenschutzgesetzes (DSG). Bei den Kontrollbefugnissen des Arbeitgebers sind insbesondere die Persönlichkeitsrechte der Arbeitnehmer zu beachten, wie z.B. Recht auf Privatsphäre (§§ 16, 1328a ABGB), Grundrecht auf Achtung des Privat- und Familienlebens (Art 8 EMRK), Grundrecht auf Wahrung des Briefgeheimnisses und des Bildnisschutzes (§§ 77, 78 UrhG), Grundrecht auf Datenschutz (§1 DSG) und Schutz personenbezogener Daten.

Der Arbeitgeber ist zur Kontrolle der Nutzung befugt, wenn er die private Nutzung von E-Mails generell ausgeschlossen hat. In diesem Fall darf der Arbeitgeber darauf vertrauen, dass E-Mails nur dienstlich verwendet werden. Das gilt auch, wenn ein Arbeitnehmer Internet oder E-Mail-Account unerlaubt privat nutzt. (Zu etwaigen Missbrauchsfällen siehe Kapitel VI. Ziffer 2.)

## 2. Private Nutzung

Wird die private Nutzung erlaubt, ist für die datenschutzrechtliche Beurteilung des Versendens von E-Mails zunächst zu unterscheiden, ob der E-Mail-Dienst durch einen externen Internetprovider oder durch den Arbeitgeber selbst geleistet wird. Im ersten Fall gelten die Sonderdatenschutzbestimmungen des Telekommunikationsgesetzes (TKG) (wie z.B. Wahrung des Kommunikationsgeheimnisses) neben dem DSG, im zweiten Fall ausschließlich das DSG.

Die Kontrolle von Inhaltsdaten ist bei erlaubter privater Nutzung ohne Einwilligung des Arbeitnehmers (zusätzlich zu einer Betriebsvereinbarung gem § 96 Abs 1 Z 3 ArbVG) nicht zulässig. Wenn aber eine Vereinbarung über die eingeschränkte Zulässigkeit der Privatnutzung von E-Mails vorliegt, ist zur Überwachung eine umfassende Protokollierung des E-Mails-Verkehrs auf dem Mailserver notwendig. Datenschutzrechtlich ist die Protokollierung nach § 9 DSG zu beurteilen. Eine Datenverwendung ist nur erlaubt, wenn der Arbeitnehmer seine Zustimmung ausdrücklich erteilt hat (§ 9 Z. 6 DSG).

Besteht aber keine Vereinbarung hinsichtlich der Privatnutzung von E-Mails, so wird angenommen, dass diese im „ortsüblichen“ Ausmaß zulässig ist und zwar abhängig von den konkreten Umständen des Einzelfalls während oder außerhalb der Arbeitszeit. Eine umfassende Protokollierung ist auch hier nötig.

Es ist also empfehlenswert, mit jedem einzelnen Mitarbeiter (unter dem Gesichtspunkt der Gleichbehandlung) eine einheitlich gestaltete Vereinbarung zu treffen. (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 Betriebsrat.)

Das Verbot der privaten Nutzung von betrieblichen E-Mail-Accounts kann den Arbeitgeber von rechtlichen Risiken des Einsatzes von Spamfiltern befreien (siehe 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.

# 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. Eine gesetzliche Verpflichtung zum Schutz gegen Viren gibt es nicht, jedoch haften Unternehmen für Schäden, die sie durch Fahrlässigkeit verursachen. Ein Versenden von Viren wegen fehlendem Virenschutz muss nach dem heutigen Stand der Technik als fahrlässig betrachtet werden.*

*Aus rechtlichen Gründen sind besondere Voraussetzungen zu beachten:*

## 1. Strafbarkeit des Ausfilterns von E-Mails

§ 119 StGB stellt eine Verletzung des Telekommunikationsgeheimnisses unter Strafe. Dieser Straftatbestand erfasst das Benützen einer Vorrichtung, die an einer Telekommunikationsanlage oder an einem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, in der Absicht, sich oder einem anderen Unbefugten vom Inhalt einer im Wege einer Telekommunikation oder eines Computersystems übermittelten und nicht für ihn bestimmten Nachricht Kenntnis zu verschaffen. Unter diesen Tatbestand fällt das unbefugte Lesen von E-Mails, sowie deren Unterdrückung, etwa in Form der absichtlichen Nichtweiterleitung an einen Empfänger. Nicht nur das Lesen, sondern auch bereits unbefugtes Öffnen von E-Mails wird durch diesen Straftatbestand sanktioniert. Die Benützung eines Sniffers erfüllt auch den objektiven Tatbestand des § 119 StGB.

## 2. Zulässigkeit des Ausfilterns von E-Mails

Nach TKG müssen Dienstanbieter 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. Problematisch bleibt nach gegenwärtiger Rechtslage der Fall, dass ein Unternehmen Spam-E-Mails, also unverlangt zugesendete Werbe-E-Mails, löscht. Die vorsätzliche Unterdrückung bzw. Nichtweiterleitung von E-Mails kann gemäß § 119 StGB strafbar sein. Ob allerdings auch ein Spam-Filter bereits als ein solches Computerprogramm oder eine Vorrichtung anzusehen ist, ist fraglich, wird allerdings in der Literatur teilweise bejaht. Der Gesetzgeber hat in den Materialien zu § 119 StGB zum Ausdruck gebracht, dass der Täter ein Unbefugter sein muss, und daher z.B. Systemadministratoren, die befugterweise E-Mails analysieren, von der Strafbarkeit ausgenommen sind. Wesentlich ist, dass der Sender und der Empfänger jeweils für sich befugt sind, vom Inhalt der Nachricht Kenntnis zu nehmen. Im Fall also eines außenstehenden, nicht an der Kommunikation beteiligten Internetproviders, der Filtersoftware einsetzt, muss dagegen davon ausgegangen werden, dass grundsätzlich sowohl die Einwilligung des Senders als auch die des Empfängers für das Ausfiltern von E-Mails erforderlich ist. Die Einholung der Einwilligung des Absenders zur Benutzung von Filtersoftware ist in der Praxis kaum möglich. Im Ergebnis ist die Verwendung von Filtersoftware durch einen Internetprovider jedoch ohne solche Einwilligung straffrei. Um gegebenenfalls einer drohenden 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 ungeschoren zu löschen.**

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

# VT

## 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 Compliance-Anforderungen an die IT-Security siehe Kapitel II. Ziffer 4)*

### 1. Abfangen von Daten

§ 119a StGB stellt das missbräuchliche Abfangen von Daten unter Strafe. Geschützt werden nur solche Daten, die im Wege eines Computersystems 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. Hier handelt es sich um ein Privatanklagedelikt.

### 2. Verletzung des Kommunikationsgeheimnisses

Gemäß § 93 TKG unterliegt der Inhalt der Telekommunikation und ihre näheren Umstände dem Kommunikationsgeheimnis, wozu insbesondere auch die Tatsache zählt, ob jemand an einem bestimmten Telekommunikationsvorgang beteiligt ist oder war. Das Kommunikationsgeheimnis erstreckt sich zudem auf die näheren Umstände erfolgloser Verbindungsversuche. Nach § 119 StGB ist eine unbefugte Mitteilung über den Inhalt privater E-Mail-Korrespondenz an andere oder die Unterdrückung der Weiterleitung privater E-Mails strafbar. 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. Datenbeschädigung

§ 126a StGB stellt die rechtswidrige Veränderung, Löschung, Unterdrückung oder Unbrauchbarmachung von Daten unter Strafe. Darunter fallen automationsunterstützt verarbeitete, übermittelte oder überlassene Daten, über die der Täter nicht oder nicht allein verfügen darf. 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. Die Installation eines Backdoorprogramms erfüllt auch den Tatbestand des § 126a StGB. Liegt aber eine schwere Störung der Funktionsfähigkeit des Computerprogramms durch die Installation vor, ist der objektive Tatbestand des § 126b StGB einschlägig.

### 4. Störung der Funktionsfähigkeit eines Computersystems

§ 126b StGB sanktioniert die Störung der Funktionsfähigkeit eines Computersystems. Darunter fallen Computersysteme, über die der Täter nicht oder nicht alleine verfügen darf. Die schwere Störung wird vor allem durch Dateneingabe bzw. Datenübermittlung verursacht. Viren-Attacken können als Störung der Funktionsfähigkeit eines Computersystems strafbar sein. Damit sollen auch Denial of Service (DoS)-Angriffe

erfasst werden. In der Neufassung der Vorschrift seit 01.01.2008 wird für den Fall einer längere Zeit andauernden Funktionsstörung eine Freiheitsstrafe von bis zu fünf Jahren angedroht.

## 5. Fälschung beweisheblicher Daten

§ 225a StGB stellt die Fälschung beweisheblicher Daten unter Strafe. Demnach ist es verboten, durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten falsche Daten herzustellen oder echte Daten zu verfälschen, die im Rechtsverkehr zum Beweis eines Rechtes, eines Rechtsverhältnisses oder einer Tatsache gebraucht werden können.

## 6. Widerrechtlicher Zugriff auf ein Computersystem

§ 118a StGB stellt den widerrechtlichen Zugriff auf ein Computersystem unter Strafe. Der nicht über das System verfügungsberechtigte Täter muss zunächst eine Sperre (Passwort beim System oder bei einzelner Datei, Firewall) überwinden und dies muss in der Absicht erfolgen, Daten einem Dritten zugänglich zu machen oder sich einen Vermögensvorteil zu verschaffen oder einem anderen einen solchen Nachteil zuzufügen. Der Täter muss auch tatsächlich in das System eindringen und innerhalb des Systems tätig werden können. Unter Computersystem versteht man sowohl Netzwerke als auch einzelne PC's oder Notebooks. Auch das Hacking, bei dem der Hacker für ihn nicht bestimmte Daten lediglich zur Kenntnis nimmt, ohne diese zu verändern, fällt unter § 118a 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 Backdoor-Trojanern, ActiveX-Control und Phishing.

## 7. Missbrauch von Computerprogrammen und Zugangsdaten

Gemäß § 126c StGB sind Herstellung, Beschaffung und Besitz von Crackprogrammen, Zugangscodes und Passwörtern strafbar, wenn dies zum Zwecke des Verschaffens eines illegalen Zuganges erfolgt. Sanktioniert wird damit das Herstellen, Einführen, Verbreiten, Veräußern, sonst Zugänglichmachen, Sichverschaffen oder Besitzen von „Hacker-Tools“. Demnach stellt § 126c StGB die Vorbereitungshandlungen ua für die Straftatbestände des §§119, 126a StGB unter Strafe.

## 8. Verletzung von Geschäfts- und Betriebsgeheimnissen

§ 122 StGB sowie § 11 UWG stellt die Verletzung von Geschäfts- und Betriebsgeheimnissen und die Betriebsspionage 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 §§ 51, 52 DSGVO eine Freiheitsstrafe bis zu einem Jahr oder eine Geldstrafe 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 (siehe Kapitel VI. 1- 6). Sofern ein Unternehmen von eigenen Mitarbeitern geschädigt wird, kann es mit arbeitsrechtlichen Maßnahmen (Abmahnung, Entlassung), Schadensersatzansprüchen und gegebenenfalls einer Strafanzeige reagieren. Sollte ein Mitarbeiter das IT-System seines Arbeitgebers zur Durchführung solcher strafbaren 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.

# VTI

## Elektronischer Geschäftsverkehr

*Sofern Unternehmen unter Einsatz von E-Mail und Internet am Geschäftsverkehr 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 Vertragsschluss.

### 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. 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 Geschäftsverkehr sicherzustellen, also um einer Verfälschung des Inhalts vorzubeugen und um 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 (SigG) sowie der Signaturverordnung (SiGV) näher geregelt. Man unterscheidet zwischen der „einfachen“ und der „sicheren“ elektronischen Signatur.

Nur die Verwendung der sicheren elektronischen Signatur gemäß § 4 Signaturgesetz erfüllt die sog. „elektronische Form“, die gemäß § 886 ABGB 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. So bedarf die Bürgschaftserklärung eines Unternehmens nach dem UGB ebenfalls der Schriftform.

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 E-Commerce-Gesetz (ECG) müssen sie über ihren Namen, ihre Anschrift, ihre Firmenbuchnummer (sofern vorhanden ist) und das Firmenbuchgericht, 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 es 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 nach Fernabsatzgesetz (FernAG) und Konsumentenschutzgesetz (KSchG) 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 ab Erhalt der Ware bzw. bei Dienstleistungen ab Vertragsschluss widerrufen.

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

Seit 1. Januar 2007 sind alle protokollierten Unternehmen, also Einzelunternehmer, OG, KG, Genossenschaft, AG, GmbH sowie die Europäische Genossenschaft (SCE) und die Europäische Gesellschaft (SE) nach § 14 UGB verpflichtet, die bisher 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, Firmenbuchnummer und -gericht.

# VIII 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 Österreich erstellt, ist der Einsatz einer fortgeschrittenen oder einer sicheren elektronischen Signatur erforderlich, die den Vorgaben des Signaturgesetzes entsprechen muss. Die elektronischen Rechnungen inklusive elektronische Signatur sind für die Dauer von sieben Jahren aufzubewahren (z.B. auf CD oder DVD). Der Ausdruck auf Papier reicht nicht aus. 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



Rechtsanwältin Dr. Bettina Windisch-Altieri, Windisch Law Offices, Wien

Stand: April 2010 – 2. Auflage – Version 2.0





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)**