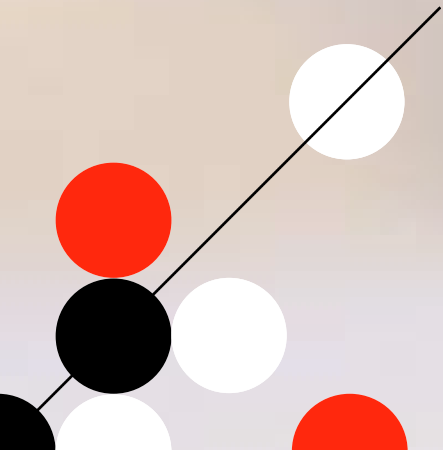


Internet und IT-Security im Unternehmen

Juristische Informationen für die Unternehmensleitung





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) Schadenersatzverpflichtungen 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 die Geschäftsleitung wie auch der Verwaltungsrat 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 Konsumentenschutz-Regelungen einzuhalten sind und wie eine elektronische Rechnung rechtswirksam gestellt werden kann.

Diese Broschüre 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 dieser Broschüre 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**

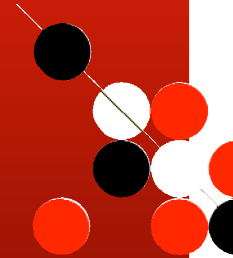
Bei Nichtbeachtung drohen als Sanktionen u.a. zivilrechtliche Schadenersatzansprüche von Geschädigten gegen das Unternehmen, Geldbussen, ökonomische Nachteile wie z.B. ein schlechteres Kreditrating, Verlust des Versicherungsschutzes oder der Ausschluss bei der Vergabe öffentlicher Aufträge.

Verwaltungsräte und Geschäftsführer 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 unbefugte Datenbeschaffung, die Verletzung des Post- oder Fernmeldegeheimnisses oder die Verletzung des Fabrikations- oder Geschäftsgeheimnisses.

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 Geschäftsverkehr** 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.



II

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 der „Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung“ (BinfV) umfasst die Informatiksicherheit „Massnahmen zum Schutz der Integrität und Verfügbarkeit der Informatiksysteme sowie zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Nachweisbarkeit der Daten, die in diesen Systemen gespeichert, verarbeitet und übertragen werden.“

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.

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 gegen Virenausbrüche und Angriffe von Hackern geschützt werden.

b) Sicherstellung der Unversehrtheit/Integrität

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 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.

2. Rechtliche Pflichten zur IT-Security

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

a) Anforderungen an die Unternehmensleitung und andere Beteiligte

Gemäss Art. 716a Abs.1 OR ist der Verwaltungsrat unter anderem zwingend für die Oberleitung der Gesellschaft, die Festlegung der Organisation und die Oberaufsicht verantwortlich. Aufgrund der hohen Abhängigkeit von einer funktionierenden IT-Infrastruktur stellt die IT-Security einen wichtigen Bestandteil des Risikomanagements dar und ist somit bereits von strategischer Bedeutung. In Zukunft (Inkrafttreten voraussichtlich am 1. Januar 2008) sind im Anhang zur Jahresrechnung Angaben über die Durchführung einer Risikobeurteilung vorgesehen. Die Organisationspflicht des Verwaltungsrates erstreckt sich auch auf die IT-Security, für welche er um eine angemessene, branchenübliche Organisation besorgt sein muss und zwar nicht nur in personeller, sondern auch in technischer und konzeptioneller Hinsicht. Schliesslich erfordert die Pflicht zur Oberaufsicht, dass die Umsetzung der Vorgaben überprüft und verfolgt werden, z.B. durch Einholung von Berichten. Eine Verletzung von Sorgfaltspflichten durch den Verwaltungsrat oder Dritte, welche mit der Geschäftsführung (Umsetzung der IT-Security Vorgaben durch den Verwaltungsrat) betraut wurden, kann eine Haftung gegenüber der Gesellschaft zur Folge haben. Für die Beurteilung, ob eine Verletzung vorliegt, besteht die Möglichkeit, dass ein Richter Corporate Governance Empfehlungen (vgl. auch unten Ziffer 5.e.) als Mindeststandards anwendet.

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 Werkvertrag oder Auftrag in Betracht.

IT-Security muss ernst genommen werden – von allen Beteiligten auch in ihrem eigenen Interesse!

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 werden in Zukunft überprüfen müssen, ob eine Risikobeurteilung im Sinne von Art. 663b Ziff. 12 nOR vorgenommen wurde.

Öffentliche Auftraggeber können 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 werden.

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 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 mit Spyware fremde Daten gesammelt werden.

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 Schadenersatz 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 Bundesgesetzes über den Datenschutz (DSG), zu beachten. Art. 7 DSG verlangt angemessene technische und organisatorische Massnahmen.

In Art. 9 der Datenschutzverordnung sind folgende Massnahmen beschrieben:

- **Zugangskontrolle**
- **Personendatenträgerkontrolle**
- **Transportkontrolle**
- **Bekanntgabekontrolle**
- **Speicherkontrolle**
- **Benutzerkontrolle**
- **Zugriffskontrolle**
- **Eingabekontrolle**

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. So muss der Auftraggeber gemäss Art. 14 Abs. 1 DSG darum besorgt sein, dass die Daten nur so bearbeitet werden, wie er es selbst tun dürfte. Der Auftragsdatenverarbeiter sollte deshalb nach seinen getroffenen technischen und organisatorischen Massnahmen unter besonderer Berücksichtigung 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.

c) Datensicherung

Obwohl es keine ausdrückliche, spezifische Pflicht zur Datensicherung gibt, so ist eine solche praktisch unabdingbar, weshalb von Unternehmen auch eine regelmässige Datensicherung erwartet wird.

Sofern ein Unternehmen kein regelmässiges Backup seiner Daten und seiner IT-Systeme durchführt, ist ihm im Falle eines durch Datenverlust entstandenen Schadens ein Selbstverschulden vorzuwerfen. Etwaige Schadenersatzansprüche gegen Dritte, die an sich für den Datenverlust verantwortlich sind, sind somit nicht oder nur in stark begrenztem Umfang durchsetzbar. Überdies droht der Verlust eines allfällig vorhandenen Versicherungsschutzes.

d) Arbeitsrecht und Arbeitsschutz

Im Rahmen der IT-Compliance sind die Mitwirkungsrechte der Arbeitnehmer bzw. Arbeitnehmervertretung hinsichtlich der Einrichtung und des Betriebs von IT-Systemen zu beachten. Ihnen stehen weitgehende Informationsrechte zu und in Fragen der Arbeitssicherheit sowie des Arbeitnehmerschutzes überdies Mitwirkungsrechte. Arbeitsplätze, Arbeitsablauf und Arbeitsumgebung sind an gesicherte arbeitswissenschaftliche Erkenntnisse auszurichten. Im Rahmen der IT-Compliance müssen also die Rechte der Arbeitnehmer gewahrt und die geltenden Arbeitsschutzvorschriften beachtet werden.

e) Handlungsanleitungen und Best Practice-Vorgaben

Auch wenn es sich um keine für Unternehmen verbindliche Richtlinie handelt, stellt das „IT-Grundschutz-Kataloge“ des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI, www.bsi.de/gshb/index.htm) eine wichtige Handlungsanleitung für die praktische Umsetzung von IT-Compliance-Anforderungen dar. Anhand dieser Grundschutz-Kataloge und der Werkzeuge, die vom BSI zur Verfügung gestellt werden, können Unternehmen ein angemessenes IT-Sicherheitsniveau erreichen. Die 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) und die Risikoanalyse auf der Basis von IT-Grundschutz (BSI-Standard 100-3). Weiterhin lassen sich die ISO-Standards 13335, 17799 und 27001 sowie die „IT Infrastructure Library“ (ITIL) 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 4.0 veröffentlicht worden ist (kostenlos abrufbar unter www.itgi.org).

f) Einhaltung von Prüfungsstandards

Die Schweizer Treuhand-Kammer hat im Schweizer Prüfungsstandard 401 verschiedene Grundsätze und Erläuterungen zu Prüfungshandlungen im Umfeld von Systemen der Informations- und Kommunikationstechnologie erlassen. Insbesondere wird auch auf die IT-Sicherheit hingewiesen, welche ein Risiko für die Zuverlässigkeit der Informationen darstellen kann.

g) Anforderungen an die Buchhaltung

Art. 957 bis 963 OR beinhalten Anforderungen an die Führung der Geschäftsbücher und die Aufbewahrung der Unterlagen. Die Buchführungspflicht knüpft an die Pflicht zum Eintrag ins Handelsregister und bedingt ihrerseits die Aufbewahrungspflicht. Letztere soll sicherstellen, dass die Geschäftsbücher und Unterlagen verfügbar sind und als Beweismittel vorgelegt werden können. Die Aufbewahrungspflicht umfasst diejenigen Bücher, die nach Art und Umfang des Geschäftes nötig sind, um die Vermögenslage und die mit dem Geschäftsbetriebe zusammenhängenden Schuld- und Forderungsverhältnisse sowie die Ergebnisse der einzelnen Geschäftsjahre festzustellen. Die Bücher müssen so geführt und aufbewahrt werden, dass die Übereinstimmung mit den zugrunde liegenden Geschäftsvorfällen gewährleistet ist. Während die Betriebsrechnung und Bilanz schriftlich und unterzeichnet aufbewahrt werden müssen, können die übrigen Unterlagen auch in elektronischer Form gespeichert aufbewahrt werden, sofern sie jederzeit lesbar gemacht werden können, und haben alsdann die gleiche Beweiskraft. Gemäss Art. 2 der Geschäftsbücherverordnung sind die Grundsätze ordnungsgemässer Buchführung und Datenverarbeitung einzuhalten, welche sich subsidiär nach den allgemein anerkannten Regelwerken und Fachempfehlungen richten. Die Aufbewahrung muss so erfolgen, dass keine Änderungen des Inhaltes vorgenommen werden können, ohne dass sich dies feststellen lässt. Die Informationsträger sind regelmässig auf Integrität und Lesbarkeit zu prüfen.

Die Aufbewahrungsfrist beträgt zehn Jahre und beginnt mit dem Ablauf des Geschäftsjahres, in dem die letzten Eintragungen vorgenommen wurden, die Buchungsbelege entstanden sind und die Geschäftskorrespondenz ein- oder ausgegangen ist.



h) Besondere Anforderungen an Banken und Finanzdienstleister

Trotz der grossen wirtschaftlichen Bedeutung der Banken und Finanzdienstleister gibt es in der Schweiz im Unterschied zum EU-Ausland keine spezifischen gesetzlichen Vorschriften zu den Sicherheitsvorkehrungen für den Einsatz elektronischer Datenverarbeitung. Vielmehr sieht die Verordnung über die Banken und Sparkassen eine allgemeine Pflicht zur Festlegung eines angemessenen Risikomanagements vor. Die Eidgenössische Bankenkommission (EBK) schreibt überdies in ihrem Rundschreiben „Interne Überwachung und Kontrolle“ vor, dass die interne Revision mindestens jährlich eine umfassende Risikobeurteilung durchführt. Das Outsourcing gewisser IT-Leistungen (Datenaufbewahrung, Betrieb und Unterhalt von Datenbanken, Betrieb von Informationstechnologie-Systemen) wird ferner vom Rundschreiben „Auslagerung von Geschäftsbereichen“ erfasst. Dieses setzt angemessene technische und organisatorische Massnahmen gegen das unbefugte Bearbeiten von Kundendaten voraus. Ebenso muss dafür gesorgt werden, dass die Vertraulichkeit, die Verfügbarkeit und die Richtigkeit der Daten gewährleistet und die Systeme gegen unbefugte oder zufällige Verluste geschützt sind.

4. Sanktionen bei Verstoss gegen IT-Compliance-Anforderungen

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

a) Strafrechtliche Sanktionen

Vorsätzliche Verstösse – wie das unbefugte Beschaffen von Daten, die Verletzung des Fernmeldegeheimnisses oder das unbefugte Beschaffen von Personendaten- sind mit Geld- oder Freiheitsstrafe bedroht.

b) Übertretungen

Verstösse gegen öffentlich-rechtliche Regelungen, wie das Datenschutzrecht, können eine Ordnungswidrigkeit darstellen und Bussen nach sich ziehen.

c) Haftung der Unternehmensleitung

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

d) Haftung von Arbeitnehmern

Arbeitnehmer, besonders IT-Sicherheits-Verantwortliche, können gegenüber ihrem Arbeitgeber schadenersatzpflichtig sein, wenn sie schuldhaft ihre Arbeitsleistung schlecht erbracht und dadurch den Arbeitgeber geschädigt haben. Verstossen sie gegen IT-Compliance-Anforderungen, kann das, je nach Grad des Verstosses, eine Verwarnung oder fristlose Kündigung nach sich ziehen. Beispielsweise hat das Bundesgericht die fristlose Kündigung eines Mitarbeiters gutgeheissen, welcher die gesamte elektronische Post des Direktors auf seinen Briefkasten umgeleitet hatte (BGE 130 III 28).

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 Schadenersatzsprüchen des Geschädigten ausgesetzt.

f) Weitere Konsequenzen

Zudem droht die Reduzierung oder der Verlust von Schadenersatzansprüchen gegenüber Dritten aufgrund Selbstverschuldens, der Verlust von Versicherungsschutz oder der Ausschluss von einer öffentlichen Auftragsvergabe.

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 die Vorgaben des Datenschutzgesetzes (DSG). Der Arbeitgeber ist zur Kontrolle der Nutzung nur befugt, soweit die Kontrolle der Zweckbestimmung des Arbeitsverhältnisses dient oder zur Wahrung berechtigter Interessen des Arbeitgebers erforderlich ist und Interessen des Arbeitnehmers nicht überwiegen. Die Kontrolle darf nicht ausschliesslich der Überwachung des Verhaltens von Mitarbeitern dienen, sondern muss vielmehr aus anderen Gründen erforderlich sein. Das gilt auch, wenn ein Arbeitnehmer Internet oder E-Mail-Account unerlaubt privat nutzt.

2. Private Nutzung

Wird die private Nutzung erlaubt, stellt sich überdies die Frage, ob der Arbeitgeber Fernmeldedienste im Sinne des Fernmeldegesetzes anbietet. Gemäss Art. 3 lit. b FMG ist der Fernmeldedienst die fernmeldetechnische Übertragung von Informationen für Dritte. Dies wird selbst für den selteneren Fall verneint, in welchem der Arbeitgeber selbst Zugangsprovider ist, da die Mitarbeiter als Teil des Unternehmens und nicht als Dritte verstanden werden. Somit untersteht der Arbeitgeber nicht dem Fernmeldegesetz, selbst wenn die private Nutzung von E-Mail erlaubt wurde. Allerdings besteht unabhängig davon das verfassungsmässige Fernmeldegeheimnis, welches gemäss Bundesgericht auch für den E-Mail Verkehr auf dem Internet gilt (BGE 126 I 50). Eine Einsicht in private E-Mails ist ohne Einwilligung des Mitarbeiters somit nur mit richterlicher Genehmigung zum Zwecke der Strafverfolgung erlaubt. Im Übrigen gelten die Regeln der Briefpost analog auch für den E-Mail-Verkehr. Ist eine E-Mail im Betreff als „privat“ gekennzeichnet oder geht die private Natur sonst wie aus dem Betreff hervor, darf sie von Dritten nicht gelesen werden. Im Zweifelsfall muss dies mit dem Angestellten geklärt werden. Ein weiterer Aspekt, der in diesem Zusammenhang zu berücksichtigen ist, stellt die Archivierung von E-Mails dar, welche oftmals bereits bei Eingang einer E-Mail erfolgt. Da die ordnungsgemässe Aufbewahrung eine rasche Auffindbarkeit voraussetzt, kommen bei Archivlösungen oft Suchmaschinen zum Einsatz. Dies hat zur Folge, dass private E-Mails ungewollt durchforstet werden können. Diese Möglichkeit muss bei Einsatz eines solchen Archivierungssystems dem Mitarbeiter ebenfalls eröffnet werden. Es bleibt dem Mitarbeiter dann unbenommen, auf die private Nutzung zu verzichten.



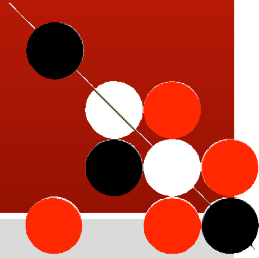
Dennoch ist eine Überwachung nicht gänzlich unmöglich. So darf zunächst eine permanente anonymisierte Auswertung der Protokollierung stattfinden. Diese hat die Überprüfung der Einhaltung des Nutzungsreglements zum Ziele, was natürlich ein solches Nutzungsreglement voraussetzt. Ein solches ist zwar nicht obligatorisch, jedoch sehr zu empfehlen, um Unsicherheiten zu vermeiden. Dagegen ist ein Überwachungsreglement zwingend vorgeschrieben, wenn die private Nutzung mittels personenbezogener Auswertung der Protokollierung überwacht werden will. Dieses Reglement muss der Belegschaft vorgängig zur Kenntnis gebracht werden und wird vorzugsweise schriftlich zusammen mit dem Nutzungsreglement erlassen. Das Überwachungsreglement muss darüber informieren, dass eine personenbezogene Auswertung möglich ist und dass die Resultate im Missbrauchsfall an den Personaldienst und an den Vorgesetzten weitergeleitet werden. Auch externe E-Mail-Empfänger und -Absender müssen darüber in Kenntnis gesetzt werden, z.B. in einer Fusszeile. Die personenbezogene Auswertung darf selbst nach Erlass dieses Reglements nur dann durchgeführt werden, wenn mittels der anonymisierten Auswertung ein Missbrauch festgestellt wurde, also ein Verstoss gegen das Nutzungsreglement.

Ein Verbot der privaten Nutzung von betrieblichen E-Mail-Accounts kann ebenfalls in Betracht gezogen werden und befreit den Arbeitgeber bspw. von rechtlichen Risiken des Einsatzes von Spamfiltern (sh. dazu das nachfolgende Kapitel IV.). 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. Letzteres ist nicht zu empfehlen, da dies wiederum die bereits aufgeführten Probleme nach sich ziehen kann.

IV.

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 ist Folgendes zu beachten:



In Art. 144^{bis} StGB (sh. unten V.4.) wird die unbefugte Datenbeschädigung unter Strafe gestellt. Während ein Unternehmen in Bezug auf betriebliche E-Mails als zur Löschung befugt betrachtet werden kann, trifft dies auf private E-Mails nicht zu. Bei einem Verbot der privaten Nutzung könnte diese Befugnis grundsätzlich angenommen werden, allerdings besteht eben auch die Möglichkeit, dass der Arbeitnehmer unaufgefordert private E-Mails zugeschickt erhält. In diesem Fall ist unklar, ob eine implizite Befugnis durch das Verbot ausreichend ist.

Jedenfalls dürfte das Ausfiltern von Viren unabhängig von einer Einwilligung bereits durch die drohende Gefahr eigener Datenbeschädigungen oder aufgrund weiterer eigener Pflichten zur Aufbewahrung bzw. zum Schutz der gespeicherten Informationen gerechtfertigt sein. Oftmals können Virenprogramme auch den Virus entfernen ohne die eigentlichen Daten zu löschen.

Dies trifft auf Spam-Filter nicht zu. Um einer möglicherweise drohenden Strafbarkeit beim Einsatz eines solchen vorzubeugen, bieten sich folgende Lösungsmöglichkeiten an:

- **Dem Arbeitnehmer wird die private Nutzung seines dienstlichen E-Mail-Accounts untersagt (vgl. hierzu näher Kapitel III. 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.**

V

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. Unbefugte Datenbeschaffung

Art. 143 StGB stellt die unbefugte Beschaffung 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. Vorausgesetzt wird, dass die Verfügungsmacht über die Daten in Bereicherungsabsicht für sich selbst oder für einen Dritten unmittelbar erlangt wird. Reine Kenntnisnahme der Daten reicht somit nicht aus. Fehlt eine Beschaffung oder eine Bereicherungsabsicht, könnte lediglich ein unbefugtes Eindringen in ein Datenverarbeitungssystem vorliegen.

2. Unbefugtes Eindringen in ein Datenverarbeitungssystem („Hacking“)

Gemäss Art. 143 StGB macht sich strafbar, wer ohne Bereicherungsabsicht auf dem Wege der Datenübertragungseinrichtung unbefugt in ein fremdes und gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt.

3. Datenbeschädigung

Art. 144bis StGB stellt die unbefugte 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. Ebenfalls unter Strafe steht die Herstellung, Einführung und das Zugänglichmachen von Programmen, welche zum Zwecke der unbefugten Datenbeschädigung verwendet werden sollen.



4. Urkundenfälschung

Art. 251 StGB stellt das Fälschen und Verfälschen einer Urkunde sowie die Benutzung einer gefälschten Urkunde unter Strafe. Gemäss Art. 110 StGB sind Urkunden Schriften, die bestimmt und geeignet sind, eine rechtlich relevante Tatsache zu beweisen, wobei diese auch auf Bild- oder Datenträger aufgezeichnet sein können. Somit unterstehen beweistaugliche elektronisch gespeicherte Daten dem strafrechtlichen Schutz. Neben der Veränderung solcher Daten steht auch deren Löschen als Urkundenunterdrückung im Sinne von Art. 254 StGB unter Strafe.

5. Störung von Betrieben, die der Allgemeinheit dienen

Nach Art. 239 StGB ist strafbar, wer den Betrieb einer öffentlichen Verkehrsanstalt, zu welchen der Wortlaut des Gesetzes z.B. auch die Telefonbetriebe zählt, hindert, stört oder gefährdet. Es kann sich dabei auch um private Unternehmen handeln, wobei dann die Konzessionspflicht ein wichtiges Indiz darstellen kann. Die Störung muss von einer gewissen Dauer sein. Analog der Telefonbetriebe dürften auch die Internetprovider bzw. deren Netzwerkbetreiber unter den Schutz fallen und somit z.B. auch solche Denial-of-Service Angriffe von einer gewissen Zeitdauer, welche deren Grunddienstleistungen beeinträchtigen.

6. Verletzung des Fabrikations- und Geschäftsgeheimnisses/ Wirtschaftlicher Nachrichtendienst/unlauterer Wettbewerb

Art. 162 StGB stellt den Verrat von Fabrikations- und Geschäftsgeheimnissen unter Strafe. Mitarbeiter machen sich strafbar, wenn sie unbefugt Fabrikations- und Geschäftsgeheimnisse an Dritte weitergeben oder durch Verrat eines Dritten erlangte Fabrikations- und Geschäftsgeheimnisse für sich oder einen anderen (z.B. die Unternehmung) ausnützen. Werden Fabrikations- und Geschäftsgeheimnisse für Dritte aus dem Ausland zugänglich gemacht, handelt es sich überdies um wirtschaftlichen Nachrichtendienst im Sinne von Art. 273 StGB. Schliesslich kann wegen unlauteren Wettbewerbes mit Gefängnis oder Busse bis zu Fr. 100'000.- bestraft werden, wer ausgekundschaftete oder sonstwie unrechtmässig erlangte Fabrikations- und Geschäftsgeheimnisse verwertet oder anderen mitteilt.

7. Datenschutzdelikte

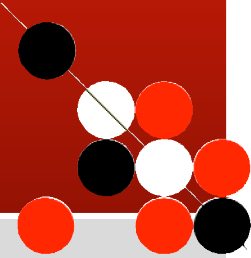
Verstösse gegen das Datenschutzgesetz können gemäss Art. 34 und 35 DSG mit Haft oder Busse bestraft werden. Dazu zählt beispielsweise die vorsätzliche falsche bzw. unvollständige Auskunft oder die unbefugte Bekanntgabe geheimer, besonders schützenswerter Personendaten oder Persönlichkeitsprofile. Weiter sieht das Strafgesetzbuch für das unbefugte Beschaffen von besonders schützenswerten, nicht frei zugänglichen Personendaten oder Persönlichkeitsprofilen aus einer Datensammlung eine Geldstrafe oder Freiheitsstrafe vor (Art. 179^{novies} StGB).

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), Schadenersatzansprüchen 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.

Elektronischer Rechtsverkehr

VI.

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 dieser juristischen Informationen für die Geschäftsleitung 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. 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 ein Indiz 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 bzw. 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 Bundesgesetz über die

elektronische Signatur 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 Bundesgesetz über die elektronische Signatur entspricht gemäss Art. 14 Abs. 2^{bis} OR der eigenhändigen Unterschrift, welche für die Schriftform vorausgesetzt ist. Allerdings ist zu berücksichtigen, dass dies nur für die einfache Schriftlichkeit gilt und nicht für Eigenschriftlichkeit, wie sie z.B. gemäss Art. 493 Abs. 2 OR für die Bürgschaft natürlicher Personen mit einem Haftungsbetrag bis Fr. 2'000.- verlangt wird.

Im Entwurf zur Schweizerischen Zivilprozessordnung sind elektronische Datenträger als Urkunden im Beweisverfahren vorgesehen, unabhängig davon, ob es sich um eine ursprünglich digitale Datei oder ein eingescanntes Papierdokument handelt. Beim allenfalls nötigen Echtheitsbeweis der Urkunde dürfte einer qualifizierten Signatur entscheidende Bedeutung zukommen.

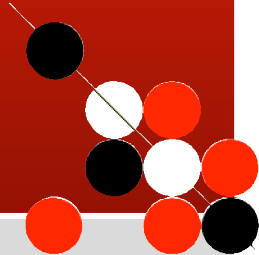
4. Anforderungen an den elektronischen Geschäftsverkehr

Nachdem ursprünglich die Einführung eines Bundesgesetzes über den elektronischen Geschäftsverkehr geplant war, hat der Bundesrat die Arbeiten mit der Begründung eingestellt, dass ein solches nicht nötig sei. Für den elektronischen Abschluss eines Vertrages gelten die normalen vertragsrechtlichen Regeln, welche übereinstimmende gegenseitige Willensäußerungen voraussetzen. Dies ist auf elektronischem Wege genau so möglich, wie auf dem traditionellen. Für Verträge, welche der Schriftform bedürfen, sieht Art. 14 Abs. 2^{bis} OR die Gleichstellung der qualifizierten elektronischen Signatur mit der eigenhändigen Unterschrift vor. Spezielle Informationspflichten hielt der Bundesrat für unnötig, da es im Interesse des Anbieters sei, den Kunden transparent zu informieren. Ansonsten setze er sich dem Risiko aus, dass eine Einigung bestritten werde. Auch auf die Einführung eines allgemeinen Widerrufsrechts wurde verzichtet und das EU-Recht als Vorbild ausdrücklich ausgeschlossen. Gerade für Rechtsgeschäfte im Internet muss aber auf den internationalen Charakter hingewiesen werden und damit einher gehend das Risiko, dass ein ausländisches Gericht nicht das im Vergleich relativ unbürokratische Schweizer Recht anwenden könnte. Aus diesem Grund empfiehlt es sich, eine Gerichtsstandsklausel und vor allem eine Rechtswahlklausel in den Vertrag einzufügen.

VII

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 Mehrwertsteuerbetrag auch als Vorsteuer verrechnen kann, ist die Vorlage einer ordnungsgemässen Rechnung erforderlich. Das leistende Unternehmen ist dazu gesetzlich verpflichtet. Neben der Rechnungsversendung per Post besteht gesetzlich auch die Möglichkeit der Versendung einer elektronischen Rechnung. Dabei handelt es sich um eine elektronische Datei, etwa im PDF-Format, die elektronisch übermittelt wird. Es müssen die Bestimmungen der Verordnung der Eidgenössischen Finanzdirektion über elektronisch übermittelte Daten und Informationen (EIDI-V) berücksichtigt werden, damit die Steuerverwaltung eine solche elektronische Rechnung anerkennt. So ist u. a. erforderlich, die Echtheit der Rechnungsherkunft und die Unversehrtheit des Rechnungsinhalts zu gewährleisten. Die Daten müssen während der Übertragung und Aufbewahrung mittels verifizierter Signatur gesichert sein. Überdies muss der ganze Vorgang dokumentiert werden und die Datensicherheit (Nachvollziehbarkeit von Änderungen, Zutritts- und Zugriffskontrollen etc.) muss gewährleistet sein. 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 in der EIDI-V geregelt sind, eingehalten werden, besteht die Gefahr, dass die Steuerverwaltung solche Rechnungen nicht anerkennt.

Rechtsanwalt Günter Untucht, Trend Micro, Director of Legal EMEA

Rechtsanwälte Dr. Peter K. Neuenschwander und Balz Meierhans, LL.M. (Edinburgh), Schweizer Neuenschwander & Partner

(www.SNPlegal.com)

Stand: Februar 2007



Trend Micro Deutschland GmbH
Central Europe
Lise-Meitner-Strasse 4
85716 Unterschleißheim
Tel.: +49 (0) 89 37479-700
Fax: +49 (0) 89 37479-799
www.trendmicro-europe.com

