

Navigation

Rechtsgebiete

Einführung Internetrecht Teil 7 IT Sicherheit

IT-Sicherheit

Da die betrieblichen Abläufe, betrieblichen Daten, kurzum fast alle Vorgänge inzwischen als Daten erfasst und mit Computern bearbeitet werden, haben Datenschutz und Datensicherheit heute einen enormen Stellenwert. Je wichtiger die Daten für ein Unternehmen sind, desto anfälliger sind sie auch.

Wer braucht IT-Sicherheit?

Im Bereich IT-Sicherheit herrschen immer noch die gängigen Vorbehalte „betrifft uns nicht, brauchen wir nicht, zu teuer“ vor. IT-Sicherheit braucht jedoch jedes Unternehmen. Dabei trifft in diesem Bereich ganz besonders die Aussage zu, dass nicht „viel hilft viel“ IT-Schutz sicherstellt, sondern vielmehr, dass jedes Unternehmen ein ganz unterschiedliches, individuelles Sicherheitsbedürfnis und Konzept benötigt. Die Kosten für die technische und rechtliche Umsetzung sind damit regelmäßig wesentlich geringer, als allgemein befürchtet.

Technische IT-Sicherheit

Firewall, Virenschutz und Backup-Datensicherung sind weitestgehend verbreitet und angewendet. Wie gut diese Anwendungen durch aktuelle Virensignaturen und Updates gepflegt sind, dabei sieht es vielfach schon nicht mehr so gut aus. Gleiches gilt beim Einsatz von kabellosen Netzwerken WLAN. In beinahe jeder Straße kann mit einem handelsüblichen Notebook auf Daten in mindestens einem offenen Netzwerk zugegriffen werden, und damit beinahe sämtliche Daten auf den lokalen Speichermedien gelesen werden. Dabei ist hier IT-Sicherheit hier mit einfachen Mitteln möglich durch die Verschlüsselung der Funkübertragung.

IT-Sicherheit betrifft auch sämtliche mobilen Geräte. Das Handy speichert heutzutage meist auch die Termine seines Besitzers, das BlackBerry oder PDA speichert noch etliche Dokumente oder Kalkulationen mehr. Erst recht gilt dies für das Notebook. Nur die wenigsten haben ihre Geräte mit einem wirksamen Passwortschutz versehen oder wenden für ihre mobilen Geräte gar eine Verschlüsselung an. Und das, obwohl Handys und Notebooks zu den am häufigsten geklauten Gegenständen gehören.

Rechtliche IT-Sicherheit

Nicht nur sinnvoll, sondern unbedingt erforderlich ist daher für sämtliche im Einsatz befindlichen Geräte ein IT-Sicherheitsmanagement. Zunächst ist hierzu in jedem Unternehmen eine Bestandsaufnahme zu machen und eine Risikoabschätzung. Dementsprechend sind die technischen und rechtlichen Maßnahmen zu ergreifen und umzusetzen.

Die Hauptprobleme im Bereich IT-Sicherheit sind meistens mangelndes Bewusstsein und mangelnde Organisation. Die größten Gefahren gehen selten von gezielten Angriffen durch Hacker aus, auch wenn Industriespionage zu einem immer ernsteren Thema wird. Viren und Trojaner sind zwar selten gezielt eingesetzt, doch der Schaden umso größer, wenn die Datenverarbeitung im Unternehmen nicht mehr richtig oder gar nicht mehr funktioniert. Die größte Gefahr ist immer noch der Mensch selbst: durch fahrlässige Falschbedienung oder Nachlässigkeit der Mitarbeiter passieren noch immer die meisten Systemausfälle. Es ist daher ein Bewusstsein der Geschäftsführung und entsprechende Schulung der Mitarbeiter erforderlich, um hier IT-Sicherheit umzusetzen.

Doch es geht nicht nur um finanzielle Verluste durch PC-Stillstand. Vielmehr noch ist IT-Sicherheit eine gesetzlich vorgeschriebene Pflicht. Das Handelsgesetzbuch und Bundesdatenschutzgesetz, das GmbH-Gesetz und auch das Informations- und Kommunikationsdienstegesetz regulieren die Pflicht zur Einführung eines entsprechenden Risikomanagements. Weitestgehend fehlt auch noch immer das Bewusstsein, dass die Folgen ohne ein entsprechendes Risikomanagement nicht nur das Unternehmen betreffen, sondern auch eine persönliche Haftung des Unternehmers normiert ist.

Der persönlichen Haftung kann vorgebeugt werden, indem für die IT-Sicherheit ein IT-Sicherheitsmanagement eingeführt ist. Dies betrifft zunächst eine schriftlich dokumentierte Erklärung der Mitarbeiter, was sie im Unternehmen mit der IT umzugehen haben. Darf der Mitarbeiter das Internet und Email auch privat nutzen? Dürfen USB-Sticks und mobile Geräte angeschlossen werden? Wie dürfen Daten ausgetauscht werden? Gibt es hierfür verschieden Kategorien? Wer ist regulär und im Notfall verantwortlicher Ansprechpartner?

Diese Regelungen werden in einer sog. IT-Security-Policy getroffen und von den Mitarbeitern gegengezeichnet. Nur so ist nachweislich ein Risikomanagement eingeführt, dass nicht nur zu einem besseren Ranking bei der Bank führt, sondern ganz besonders zu Rechtssicherheit und Haftungsminimierung des Unternehmers.

Weiterlesen:

[zum vorhergehenden Teil des Buches](#)

[zum folgenden Teil des Buches](#)

Links zu allen Beiträgen der Serie [Einführung Internetrecht](#)

Kontakt: info@brennecke-rechtsanwaelte.de

Stand: 02/07

Wir beraten Sie gerne persönlich, telefonisch oder per Mail. Sie können uns Ihr Anliegen samt den relevanten Unterlagen gerne unverbindlich als PDF zumailen, zufaxen oder per Post zusenden. Wir schauen diese durch und setzen uns dann mit Ihnen in Verbindung, um Ihnen ein unverbindliches Angebot für ein Mandat zu unterbreiten. Ein Mandat kommt erst mit schriftlicher Mandatserteilung zustande.

Wir bitten um Ihr Verständnis: Wir können keine kostenlose Rechtsberatung erbringen.

Das Referat IT-Recht wird bei Brennecke & Partner Rechtsanwälte betreut von:



Tilo Schindele, Rechtsanwalt, Stuttgart

Rechtsanwalt Schindele begleitet IT-Projekte von der Vertragsgestaltung und Lastenheftdefinition über die Umsetzung bis hin zur Abnahme oder Gewährleistungs- und Rückabwicklungsfragen.

Tilo Schindele ist Dozent für IT-Recht und Datenschutz bei der DMA Deutsche Mittelstandsakademie.

Er bietet Seminare und Vorträge unter anderem zu folgenden Themen an:

- Praxistipps zum rechtssicheren Einsatz von E-Mails im Unternehmen
- Rechtssicherheit im Internet: - Praktische Rechtstipps für Unternehmer von AGB über Disclaimer und E-Mails bis zu web2.0
- Allgemeine Geschäftsbedingungen zu Vertragsschluss, Laufzeit und Umzug in Telekommunikationsverträgen

Kontaktieren Sie Rechtsanwalt Tilo Schindele unter:

Mail: tilo.schindele@brennecke-rechtsanwaelte.de

Telefon: 0721-20396-28

Datenschutzerklärung

Mehr Beiträge zum Thema finden Sie unter:

[Rechtsinfos/ IT-Recht/ Internetrecht/ Viren](#)

[Rechtsinfos/ Datenschutzrecht/ IT-Security](#)

[Rechtsinfos/ IT-Recht/ IT-Security](#)

[Rechtsinfos/ Haftungsrecht](#)

© 2002 - 2020

 [Standorte - Ihr Rechtsanwalt vor Ort](#)

 [Kontakt](#)

[Datenschutzerklärung](#)