

Datenschutz ist Chefsache!

### **Warum das so ist, kann man an fünf Fingern abzählen:**

#### ■ **Schadenersatzforderungen**

Viren, Trojaner, Spam - das Trio infernale moderner Kommunikation. Elektronische Parasiten sind jedoch nicht nur ärgerlich, sondern können richtig teuer werden. Immer wieder nämlich gelingt es Kriminellen, die IT- Systeme eines Unternehmens zu unterwandern, um von hier aus Viren oder Spam-E-Mails zu verschicken.

Haftbar hierfür ist das Unternehmen, wenn mangelnde Kontrolle zur Virenverbreitung beitrug.

Deshalb genügt es nicht, für einen möglichst umfassenden Schutz der Systeme zu sorgen - man muss diesen Schutz auch überwachen und protokollieren können. Ohne eine lückenlose Beweisführung ist man den Vorwürfen in einem möglichen Prozess schutzlos ausgeliefert, ist die Entkräftung solcher Anschuldigungen kaum möglich. Die Folge: Unternehmen akzeptieren aufgrund des drohenden Imageverlusts im Falle einer Verurteilung oder im Falle eines langen Verfahren unangemessen hohe außergerichtliche Vergleiche.



#### **Die persönliche Haftung**

Sollte es zu solch einem Prozess kommen, können Unternehmen Schadenersatz beim Vorstand oder beim Geschäftsführer geltend machen. Ihm nämlich obliegt die Durchführung aller erforderlichen Maßnahmen. Hierbei sind die Regelungen im Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) und im Bundesdatenschutzgesetz (BDSG) zu beachten.



### Die unterschiedlichen Gesetze

Verantwortungsvoller Umgang mit der IT- Sicherheit ist nichts anderes als die Basis für viele weitere Vorgänge, die über das Wohl eines Unternehmens entscheiden. Immerhin stehen die unterschiedlichen Vorschriften, wie sie durch die Reform des Aktien- und Bilanzrechtes, durch das Gesetz zur Transparenz und Publizität (TransPuG) oder im KonTraG zu erfüllen sind, im direkten Zusammenhang mit der Datensicherheit. Hierbei überschreitet der globale Markt längst auch die nationalen Grenzen, weshalb selbst us-amerikanische Richtlinien beachtet werden müssen - auch von deutschen Unternehmen.



### Die Kreditaufnahme

Banken achten bei der Einschätzung der Kreditwürdigkeit schon lange auf die IT-Sicherheit eines Unternehmens. Das ist verständlich und nachvollziehbar - und wurde denn auch durch Basel II nochmals verdeutlicht. Deshalb zahlt sich ein zeitgemäßer Umgang mit Daten- und IT-Sicherheit doppelt aus. Denn wo ein mangelhafter Umgang zu schlechten Ratings und somit zu schlechten Darlehenskonditionen führt, machen sich Investitionen in die IT- Sicherheit im positiven Sinn auch bei der Fremdkapitalaufstockung bezahlt.



### Der Jahresabschluss

Alle Jahre wieder nehmen ihre Wirtschaftsprüfer die verschiedenen Geschäftszahlen sowie alle anderen Daten in Augenschein - was auch teure IT-Prüfungen beinhaltet. Im Vorteil ist hier, wer seinen Wirtschaftsprüfern eine zertifizierte IT- Sicherheitsinfrastruktur belegen kann. Das spart Zeit - und Geld.