

Teil - I

Gesetzliche Anforderungen an IT-Sicherheit

Unternehmensrisiken (Einleitung Abschnitt-1)

Jedes Unternehmen ist Risiken¹ ausgesetzt oder geht Risiken bewusst manchmal auch unbewusst ein.

Risiken können entstehen in den unterschiedlichsten Bereichen eines Unternehmens. Vorstände und Geschäftsführer von juristischen Personen haben per Gesetz die Verpflichtung Risiken zu erkennen und Gegenmaßnahmen zu treffen.

KonTraG

In Deutschland bildet das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) aus dem Jahre 1998 die Grundlage zum Aufbau eines Risikomanagements. Der §91 Abs. 2 AktG besagt:

"Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit der Fortbestand der Gesellschaft gefährdende Entwicklung früh erkannt werden."

Das ist der gesetzliche Mindestrahmen für Aktiengesellschaften und hat auf andere juristische Personen entsprechenden Einfluss.

¹ Das Wort Risiko bedeutet Wagnis, Gefahr und wurde im 16. Jahrhundert aus dem italienischen in den deutschen Sprachgebrauch übernommen.

Basel II

Banken müssen nach den Festlegungen von Basel II (europäische Zentralbanken legen das Verfahren ab 2005 fest) bei der Zentralbank einen bestimmten Sicherungsbetrag für einen vergebenen Firmenkredit hinterlegen. Je schlechter das Rating der Firma, um so höher der zu hinterlegende Sicherungsbetrag. Neben einer Reihe von Einflussgrößen wird auch die IT und deren Sicherheit im Rating eine Rolle spielen.

Aus diesen beiden Komponenten heraus hat sich in der Praxis der Begriff Risikomanagement entwickelt. Es lassen sich folgende Teilbereiche unterscheiden:

Risikoidentifikation

Alle Einzelrisiken werden systematisch erfasst und kontinuierlich fortgeschrieben. Dabei ist es hilfreich, verschiedene geeignete Risikofelder zu definieren.

Risikoanalyse

Hier werden die identifizierten Einzelrisiken hinsichtlich ihrer Eintrittswahrscheinlichkeit und ihrer qualitativen Auswirkungen auf den Unternehmenserfolg bewertet.

Risikobewältigung

Folgende Maßnahmenbündel bieten sich als Schutz gegen Risiken an:

- Risikovermeidung
- Risikoverminderung
- Risikoüberwälzung
- Risikoakzeptanz
- Risikofelder

Unternehmensrisiken können in folgende Risikofelder eingeteilt werden:

- Operative Risiken
- Produktionsrisiken
- Qualitätsrisiken

- Mitarbeiter
- Informationstechnologie (IT)

Strategische Risiken

- Marktanteile
- Kunden
- Lieferanten
- Wettbewerber
- Ersatz

Finanzielle Risiken

- Umsatz
- Liquidität
- Rating
- Kapitalumschlag
- Börsenkurs

Externe Risiken

- Infrastruktur
- Technische Veränderungen
- Werkspionage, Sabotage, Krieg
- Physikalische Gefahren (Stromausfall, Feuer, Wasser, Rauchgas, Wind, Erdbeben)

Risikocontrolling

Das gesamte Risikomanagement muß funktionsfähig und effizient arbeiten, das ist die Aufgabe des Risikocontrollings.

Maßnahmen

Die Maßnahmen, die konkret getroffen werden, können sich von technischen über organisatorische und personelle Maßnahmen ziehen und über Verträge mit Lieferanten, Dienstleistern und Versicherungen weitergeführt werden.

Haftungsrisiken für IT-Verantwortliche (Abschnitt-2 Einleitung)

Zu den IT-Verantwortlichen eines Unternehmens gehören:

- Vorstand
- Geschäftsführer
- Behördenleiter
- IT-Leiter
- IT-Mitarbeiter

Die Informationstechnik birgt ausreichend Gefahren, die das gesamte Unternehmen betreffen und dessen Existenz bedrohen können. Jede Person im IT-Bereich kann je nach Lage des Einzelfalles persönlich haftbar gemacht werden für Schäden, die dem Unternehmen aus der IT entstehen können.

Gegenmaßnahme: Somit ist es dringend geraten, im Hinblick auf eine mögliche Eigenhaftung, geeignete Maßnahmen zu ergreifen um einer Gefährdung der unternehmenseigenen Informationssysteme sowie der dazugehörigen Daten vorzubeugen.

Beispielfall "unbewusste Verbreitung von Viren" (Abschnitt 7.5)

Eine Steuerberatersozietät setzt zum Erstellen und Bearbeiten ihres Schriftverkehrs ein Textverarbeitungssystem kombiniert mit einer Datenbankanwendung in einem Netzwerk ein. Ein Steuerberater erhält von seinem Mandanten eine Diskette mit der Bitte, den gespeicherten Text zu überarbeiten und an steuerrechtlich Notwendigkeiten anzupassen.

Der auf dieser Diskette gespeicherte Bootvirus gelangt auf diese Weise in das Netzwerk der Sozietät und zerstört eine Reihe von Texten. Der Betrieb bricht zusammen und es kostet die Sozietät sehr viel unproduktive Zeit das IT-System wieder herzustellen.

In einem solchen Fall wird man differenzieren müssen. Grundsätzlich trifft zunächst den zuständigen IT-Leiter die Verantwor-

tung für aktuelle Virenerkennungs- und Entseuchungsprogramme zu sorgen. Darüber hinaus hat er sämtliche Mitarbeiter der Sozietät regelmäßig über die Gefahren von Computerviren aufzuklären und sie zu entsprechenden Vorsorgemaßnahmen anzuhalten. Kommt der IT-Leiter dieser Pflicht nicht nach, so handelt er in Anbetracht der Bedeutung der Datenverarbeitung für den Betrieb, welche ein besonders sorgfältiges und aufmerksames Verhalten der Mitarbeiter erfordert, grob fahrlässig und haftet dem Arbeitgeber persönlich für den daraus entstehenden Schaden.

Kommt hingegen der IT-Leiter nach und verstößt der Steuerberater gegen diese Belehrung und überspielt die Diskette seines Mandanten ohne vorherige Überprüfung auf das System, so handelt er grob fahrlässig, da er trotz mehrfacher Hinweise seiner Pflicht nicht nachgekommen ist.

Ein „Haftungsloch“ entsteht somit nur dann, wenn beide IT-Leiter und Steuerberater nur leichte Fahrlässigkeit vorzuwerfen ist. Dies kann vor allem bei neuen, noch unerfahrenen Mitarbeitern der Fall sein, die aus Zeitmangel noch nicht in die Virenerkennungssoftware des Unternehmens eingewiesen sind und deshalb den Anforderungen an die Datensicherheit nicht entsprechen haben.

