

## Firmenleitung in der Pflicht

Gesetzgeber verschärft Anforderungen an IT-Sicherheit in Firmen

Das Jahr 2005 wird einen entscheidenden Richtungswechsel mit sich bringen: IT Security wird aus Haftungsgründen zunehmend zur Chefsache. Denn der Gesetzgeber nimmt das Firmenmanagement verstärkt in die Pflicht, für einen sicheren Datenverkehr zu haften. Gesetzliche Auflagen durch Sarbanes Oxley, Basel II oder das neue Urheberrecht treiben diesen Trend. Was viele Firmen noch gar nicht bewußt ist: Sind in einer Firma die notwendigen IT-Sicherheitsstrukturen nicht oder nur unzureichend implementiert, riskieren die Verantwortlichen - häufig der Geschäftsführer oder Vorstand - die Haftung der Firma und der eigenen Person. Sie müssen sogar unter Umständen mit ihrem Privatvermögen für entstandene Schäden aufkommen. Anders als im Strafrecht haftet der Verantwortliche für die IT im Zivilrecht auf für Fahrlässigkeit.

Es gibt ganz unterschiedliche Rechtsverletzungen, die über den digitalen Kommunikationsverkehr auftreten können. So hat die Novellierung des Urheberrechts dazu geführt, daß Firmen mit Schadensersatzklagen rechnen müssen, wenn ihre Mitarbeiter Musik- und Filmdateien aus dem Internet herunterladen oder nicht lizenzierte Software auf ihren PCs nutzen. Aber auch strafrechtliche Tatbestände wie die Verbreitung von kinderpornographischem Material oder Verstöße gegen den Datenschutz, wie die Veröffentlichung von geheimen Kunden- oder Mit-

arbeiterinformationen, können Firmen in Bedrängnis bringen.

Die Folgen reichen von Geldstrafen, wie die Zahlung von Schadensersatz, Schmerzensgeld oder Bußgeldern. Im Falle einer Schädigung Dritter drohen Unternehmen Gerichtsverfahren mit einhergehender Überprüfung ihrer IT-Sicherheitsvorkehrungen unter Einbeziehung von Sachverständigen. Hat ein solcher Vorfall Wettbewerbsbezug, so drohen zudem kostenpflichtige Abmahnungen von Konkurrenten. Firmen, die aufgrund ihres Geschäftsgebärens mangelhafte IT-Sicherheitsstrukturen erkennen lassen, können zudem ihre Gewerbeurteilung verlieren. Kommt es zum Versicherungsfall, drohen Untersuchungen des Versicherers und die Verweigerung der Versicherungsleistung bei fahrlässiger Unterlassung von IT-Sicherheitsmaßnahmen.

Mit dem am 1. Mai 1998 in Kraft getretenen Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) wurde die Pflicht zur Schaffung eines unternehmensinternen Risikofrüherkennungssystems im Recht der Aktiengesellschaft eingeführt. Der Vorstand hat danach geeignete Maßnahmen zu treffen, damit Entwicklungen, die den Fortbestand der Gesellschaft gefährden, frühzeitig erkannt werden.

### Banken und Investoren fordern

Zu diesen Maßnahmen zählt auch eine funktionierende IT-Sicher-

heitsinfrastruktur. Wirtschaftsprüfer sind verpflichtet, solche Risikofrüherkennungssysteme zu evaluieren, und sie kontrollieren zunehmend genauer die IT-Sicherheitssysteme in den Firmen. Sind diese nicht ordnungsgemäß eingerichtet worden und entstehen Schäden, so droht dem Vorstand schlimmstenfalls eine Haftung mit seinem Privatvermögen sowie eine außerordentliche Kündigung seines Anstellungsverhältnisses. Neben dem Gesetzgeber interessieren sich verstärkt auch andere Instanzen für die Güte von IT-Sicherheitsmaßnahmen in Firmen: Mit dem Inkrafttreten der Basel-II-Richtlinien im Jahr 2005 kontrollieren Banken im Rahmen ihrer sogenannten Ratings Risikovorkehrungen für IT-Systeme in Unternehmen. Sehr ähnlich gehen Investoren bei der Risikobewertung von Firmen vor, und auch Vergabestellen nehmen immer häufiger den Nachweis einer ausreichenden IT-Sicherheitsinfrastruktur in ihre Ausschreibungsbedingungen auf.

In den Vereinigten Staaten werden laxere IT-Sicherheitsvorkehrungen noch schärfer geahndet als in den EU-Ländern, aber es ist wohl nur eine Frage der Zeit, bis dieser Trend auch an die Ufer Europas schwappen wird.

(Von Steve Purdham)