

### **Unternehmen unterschätzen Haftungsrisiken bei der IT- Sicherheit**

Geschäftsführer und Vorstände aber auch IT- Verantwortliche können persönlich haftbar gemacht werden, wenn sie in ihrem Unternehmen nicht ausreichend für IT- Sicherheit sorgen.

Darauf weist der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) hin.

So reiche die Installierung von Antiviren-Software, Spam- Filtern und Firewalls nicht aus. Denn auch höhere Gewalt wie Feuer und Überschwemmungen, technisches Versagen wie Softwarefehler und Stromausfall, Vorsatz wie Diebstahl und Hacking, sowie Organisationsdefizite wie unklare Vorschriften oder ungeschulte Mitarbeiter können zu IT- Schadensfällen führen.

Der BITKOM hat in einer Haftungsmatrix die unterschiedlichen rechtlichen Regelungen und ihre jeweiligen Verantwortlichen in den Unternehmen umfassend dargestellt. Haftungsrisiken bestehen danach für Vorstand, IT- Leitung und betriebl. Datenschutzbeauftragter, z. T. aber auch für einzelne Mitarbeiter.

Die gesetzlichen Regelungen zur IT- Sicherheit umfassen jedoch nicht nur das Haftungsrecht, sondern auch Steuer- und sogar Strafrecht, die Strafen reichen vom Bußgeld bis zur Gefängnisstrafe.

Um Sicherheits- und Haftungsrisiken vorzubeugen, sollten Unternehmer daher ein Sicherheitskonzept entwickeln lassen, dies verabschieden und auch intern kommunizieren. Ein solches Konzept müsse jedoch das ganze Unternehmen mit sämtlichen Geschäftsprozessen berücksichtigen.

#### **Matrix der Haftungsrisiken**

Ausgehend von besonders relevanten Pflichten bzw. Regelungsbedarf im Unternehmen bzgl. der Gewährleistung der IT- Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität) hat BITKOM den Leitfaden „Matrix der Haftungsrisiken“ erstellt. Dieser ist im folgenden Text auszugsweise und zusammengefasst dargestellt:

#### **Übersicht der Unternehmens-Pflichten und des Regelungsbedarfs nach Aufgabenbereichen:**

##### **Strategische Aufgaben**

- Sicherstellung einer bedarfs- und rechtskonformen IT- Nutzung
- Bestellung eines betrieblichen Datenschutzbeauftragten

##### **Konzeptionelle Aufgaben**

- Einführung eines Sicherheitskonzepts (inkl. Katastrophen- und Zugriffsschutz) und eines Datenschutzkonzeptes
- Ständige Aktualisierung des Sicherheits-/Datenschutzkonzeptes
- Regelungen beim Zugang von externen Dritten zu Datenverarbeitungssystemen
- Professionelle Beschaffung von IT- Systemen und Durchführung von IT- Projekten
- Sicherung von Vertraulichkeit und Geheimhaltung

##### **Operative Aufgaben**

- Ordnungsgemäße Abbildung der wirtschaftlichen Verhältnisse in der Buchführung
- Datenschutzrechtliche Konformität sicherstellen
- Einsatz von SPAM- und Viren-Filtern abwägen
- Regelung für die Nutzung von E-Mail und Internet am Arbeitsplatz
- Virenfreier Daten-/Datenträgeraustausch
- Verhinderung von Schädigung Dritter durch firmeneigene IT
- Durchführung regelmäßiger Backups
- Verwendung lizenzierter Software
- Einhaltung der Urheberrechte

## Verantwortliche und persönliche Haftung

Während für die **strategischen Aufgaben grundsätzlich der Vorstand** zuständig und verantwortlich ist, sind bei den konzeptionellen und operativen Aufgaben neben der Verantwortlichkeit der Geschäftsführung auch Mitarbeiter für die Erfüllung von Pflichten bzw. bestimmte Regelungen verantwortlich, z.B. **IT- Leiter oder der betriebliche Datenschutzbeauftragte**.

Des Weiteren kann auch der **einzelne Mitarbeiter** davon betroffen sein, z. B. im Falle der Verwendung nicht ausreichend lizenzierter Software.

Die jeweiligen Haftungsrisiken sind unterschiedlich. Bei Schäden durch die Pflichtverletzung oder durch die Nichtregelung haftet das Unternehmen und in besonderen Fällen auch der Vorstand.

Der Mitarbeiter haftet gegenüber dem Unternehmen (und Dritten) im Rahmen seiner Rolle als Arbeitnehmer.

## Eingeschränkter Versicherungsschutz – weitere Risiken

Zwar können sich Manager auch in Deutschland versichern lassen, allerdings erlischt der Versicherungsschutz bei Vorsatz oder einer „wissentlichen Pflichtverletzung“ – wenn ein Manager beispielsweise in einem Expertengutachten explizit auf die mangelhafte IT- Sicherheit in seinem Unternehmen hingewiesen wurde und untätig bleibt.

Auch wenn die Versicherung den Schaden der persönlich Verantwortlichen bis zu einer gewissen Höhe trägt sind weitere Nachteile, insbesondere für das Unternehmen, zu befürchten wie z.B.:

- Unternehmensverluste / Insolvenz durch Ausfall der Systeme bei sehr hohen Schäden
- Ggf. Verlust von Versicherungsschutz des Unternehmens
- Verteuerung der Unternehmenskredite (Basel II)
- Imageschaden nach Verlust von personenbezogenen Daten aufgrund von Sicherheitslücken

## Erläuterungen zur Arbeitnehmerhaftung

### Haftung im Innenverhältnis ( gegenüber Arbeitgeber)

Grundlage für eine mögliche Arbeitnehmerhaftung ist zunächst eine schuldhaft begangene Pflichtverletzung (Schlechterfüllung, unerlaubte Handlung) im Rahmen eines bestehenden Arbeitsverhältnisses.

Ist der Schaden auf leichteste und leichte Fahrlässigkeit zurückzuführen, haftet der Arbeitnehmer nicht.

Bei normaler („mittlerer“) Fahrlässigkeit ist der Schaden in aller Regel zwischen Arbeitgeber und Arbeitnehmer quotal zu verteilen, zumeist aber mit Begrenzung auf zwei Monatsgehälter.

Bei grober Fahrlässigkeit des Arbeitnehmers hat dieser in aller Regel den gesamten Schaden zu tragen, in Abwägung des Einzelfalles sind Haftungserleichterungen möglich.

Vorsätzlich verursachte Schäden hat der Arbeitnehmer grundsätzlich in vollem Umfang zu tragen.

### Haftung im Aussenverhältnis ( Vertragspartner, sonstiger Dritter)

Schädigt der Arbeitnehmer im Rahmen seiner betrieblichen Tätigkeit einen Vertragspartner oder einen sonstigen außen stehenden Dritten, dann haften Arbeitgeber und Arbeitnehmer als sog. Gesamtschuldner. In diesen Fällen kann der Dritte seinen Schaden sowohl gegenüber dem Arbeitgeber als auch gegenüber dem Arbeitnehmer geltend machen.

Den vollständigen Text des Leifadens finden Sie unter der Homepage von BITKOM unter: [www.bitkom.org/de/publikationen/1357\\_31034.aspx](http://www.bitkom.org/de/publikationen/1357_31034.aspx)

**Georg Osner**  
**Datenschutzberater**