Haftungsrisiken - IT-Sicherheit - Pflichten und Risiken

Die schnelle Entwicklung der Informationstechnologie verändert auch die rechtlichen Rahmenbedingungen – neue Gesetze und Verordnungen verpflichten zum sorgsamen Umgang mit den Daten, Systemen und Risikomanagement. Die Rechtsprechung stellt angemessene Sorgfalt immer wieder neu auf den Prüfstand.

Schon etwas in die Jahre gekommen vermittelt die „Matrix der Haftungsrisiken“ der BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.) eine anschauliche Aufstellung der Pflichten und Risiken in der IT-Sicherheit (BITKOM_Leitfaden_Matrix_der_Haftungsrisiken-V1.1f.pdf).

Die Konsequenz

- Unternehmen sind zum sorgfältigen Umgang mit der IT verpflichtet
- Verfügbarkeit, Vertraulichkeit, Unversehrtheit der IT-Systeme sind zu gewährleisten
- Für personenbezogene Daten gilt die Verpflichtung zum Verpflichtung zum Datenschutz und der angemessenen Datensicherheit
- IT-Risikomanagement muss aktiv betrieben werden
- Die rechtlichen Rahmenbedingungen sind vielfältig und kaum noch zu überschauen

Die Aufgaben	**Rechtsgrundlage**
Strategisch	
• Sicherstellung einer bedarfs- und rechtskonformen IT-Nutzung	Gesellschaftsrecht
• Bestellung eines betrieblichen Datenschutzbeauftragten	Datenschutzrecht
Konzeptionell	
• Einführung eines Sicherheitskonzepts (inkl. Katastrophen- und Zugriffsschutz)	Gesellschaftsrecht
• Einführung eines Datenschutzkonzeptes	Datenschutzrecht
• Ständige Aktualisierung des Sicherheits-/Datenschutzkonzepts	Gesellschaftsrecht
• Regelungen beim Zugang von externen Dritten zu Datenverarbeitungssystemen	Datenschutzrecht
• Professionelle Beschaffung von IT-Systemen und Durchführung von IT-Projekten	Zivil- und Handelsrecht
• Sicherung von Vertraulichkeit und Geheimhaltung	Zivilrecht, Vertragl. Vertraulichkeit, ...
Operativ	
• Ordnungsgemäße Abbildung der wirtschaftlichen Verhältnisse des Unternehmens in der Buchführung	Handel-, Steuer- und Gesellschaftrecht
• Datenschutzrechtliche Konformität sicherstellen	Datenschutzrecht, UWG

• Einsatz von SPAM- und Viren-Filtern abwägen	TKG, StGB
• Regelung für die Nutzung von E-Mail und Internet am Arbeitsplatz	GG, Zivil-, Datenschutz-, Telekommunikationsrecht, BetrVG
• Virenfreier Daten-/ Datenträgeraustausch	Datenschutz- und Zivilrecht
• Verhinderung von Schädigung Dritter durch firmeneigene IT	Gesellschaftsund Zivilrecht
• Durchführung regelmäßiger Backups	Zivilrecht
• Verwendung lizenzierter Software	Urheberrecht, Gesellschaftsrecht

Ihr Vorteil

- Sicherstellung der **rechtlichen Rahmenbedingungen** für **IT-Sicherheit** und **Datenschutz**
- Erstellung eines angemessenen **IT-Sicherheitsniveaus** in Ihrem Unternehmen
- Absicherung und Aufrechterhaltung des **täglichen IT-Betriebs**
- Sicherung der Daten und Systemleistung für einen **dauerhaften Betrieb**
- Schutz von **Unternehmenswissen**, **Wettbewerbs**- und **Geschäftsgeheimnissen** und der **personenbezogenen Daten**
- Verminderung von **Haftungsrisiken**, **Schadensersatzforderungen**, **Bußgeld** und **finanziellen Folgen** von Systemausfall und Datenverlust