Rechtliche Rahmenbedingungen für die IT-Sicherheit

Die Informations- und Kommunikationstechnologie entwickelt sich mit hoher Geschwindigkeit, damit auch die Risiken und Anforderungen an die Sicherheit. Der Gesetzgeber reagiert mit entsprechenden Vorschriften und die Rechtsprechung passt ihre Anforderungen den aktuellen Möglichkeiten an. Doch aktuelle Tagesnachrichten zeigen immer wieder die Spitze des Eisbergs hinsichtlich Datenpannen und Verstöße gegen geltendes Rechts.

Welche Konsequenzen drohen dem Unternehmen und den verantwortlichen Personen?

Während der vergangenen Jahre wurden mehrere Rechtsvorschriften erlassen, aus denen sich zu Fragen der IT-Sicherheit unmittelbare Handlungs- und Haftungsverpflichtungen der Geschäftsführung bzw. des Vorstands eines Unternehmens ableiten lassen.

Diese Regelungen gelten sowohl für Aktiengesellschaften als auch für GmbHs.

Die Konsequenz

- **Vorstände** und **Geschäftsführer** haften persönlich, wenn zukünftige Risiken für das Unternehmen nicht durch ein **Risikomanagement** überwacht und durch geeignete Maßnahmen vorgebeugt werden (AktG, GmbHG, HGB, KonTraG)
- **Abschlussprüfer** sind verpflichtet zu prüfen ob die Risiken der künftigen Entwicklung zutreffend dargestellt sind (HGB)
- Verwendung von **Informationstechnik** (Internet, Telekommunikationsdienste) werden tlw. sehr genau geregelt (Gesetz zur Nutzung von Telediensten, Telekommunikationsgesetz, Mediendienste-Staatsvertrag, Urheberrecht, Richtlinien auf EU-Ebene)
- Der Umgang mit **personenbezogenen Daten** wird in den Datenschutzgesetzen (Bund und Länder), dem Telekommunikationsrecht und weiteren Gesetzen geregelt. (GG, BDSG, TKG, TMG, SGB, StGB ..)
- Banken sind verpflichtet, bei der Kreditvergabe **IT-Risiken** des Kreditnehmers zu berücksichtigen, mit Auswirkung auf die angebotenen Konditionen **(Basel II)**.
- Berufsgruppen mit **Berufsgeheimnis** unterliegen zusätzlichen Sonderregelungen im Strafgesetzbuch (auch Freiheitsstrafe)
- **IT-Sicherheitsvorfälle** können massive wirtschaftliche Schäden verursachen und ggf. den Bestand eines Unternehmens gefährden.
- Ein **fahrlässiger Umgang** mit **Informationstechnik** kann o.g. Sachverhalte bereits erfüllen.
- Konkrete Verpflichtungen eines angemessenen **IT-Sicherheitsniveaus** im Unternehmen lassen sich ableiten

Rechtliche Rahmenbedingungen

Die Aufgaben

- Sicherstellung einer bedarfs- und rechtskonformen IT-Nutzung
- Bestellung eines betrieblichen Datenschutzbeauftragten
- Einführung eines Sicherheitskonzepts (inkl. Katastrophen- und Zugriffsschutz)
- Einführung eines Datenschutzkonzeptes
- Ständige Aktualisierung des Sicherheits-/Datenschutzkonzeptes
- Sicherung von Vertraulichkeit und Geheimhaltung
- Ordnungsgemäße Abbildung der wirtschaftlichen Verhältnisse in der Buchführung
- Datenschutzrechtliche Konformität sicherstellen
- Regelung für die Nutzung von E-Mail und Internet am Arbeitsplatz
- Verhinderung von Schädigung Dritter durch firmeneigene IT
- Verwendung lizenzierter Software
- Einhaltung der Urheberrechte

Ihr Vorteil

- Erstellung eines angemessenen **IT-Sicherheitsniveaus** in Ihrem Unternehmen
- **IT-Risikomanagement** aufbauen und durch Maßnahmen zukünftigen **IT-Risiken** begegnen
- **Rechtskonforme IT-Nutzung** gewährleisten
- Schutz von **Unternehmenswissen**, **Wettbewerbs**- und **Geschäftsgeheimnissen** und der **personenbezogenen Daten**
- Verminderung von **Haftungsrisiken**, **Schadensersatzforderungen**, **Bußgeld** und **finanziellen Folgen** von Systemausfall und Datenverlust