

Rechtliche Grundlagen zur IT-Sicherheit

Eine Vielzahl von Verordnungen und gesetzliche Vorschriften deklariert die Sicherheit in der Informationstechnik als integralen Bestandteil der Unternehmensführung. Nachfolgend eine Übersicht der wichtigsten Texte:

Handelsgesetzbuch (HGB)

Das Handelsgesetzbuch schreibt dem Kaufmann in §238 Abs. 1 vor, Bücher nach den Grundsätzen ordnungsgemäßer Buchführung (GoB) bzw. nach den Grundsätzen ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS) zu führen. Bestimmungen zur Datensicherheit findet sich unter Abschnitt 5 GoBS:

- Rd-Nr. 5.1: „Die starke Abhängigkeit der Unternehmung von ihren gespeicherten Informationen macht ein ausgeprägtes Datensicherungskonzept für das Erfüllen der GoBS unabdingbar. [...]“
- Rd-Nr. 5.3: „Die Informationen sind gegen Verlust und gegen unberechtigte Veränderung zu schützen. [...]“
- Rd-Nr. 5.5.1: „Der Schutz der Informationen gegen unberechtigte Veränderung ist durch wirksame Zugriffs- bzw. Zugangskontrollen zu gewährleisten. [...]“

Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) / Aktiengesetz (AktG)

Seit Inkrafttreten des KonTraG im Mai 1998 sind Vorstände von Aktiengesellschaften verpflichtet, ein Risikomanagementsystem zu etablieren. Die geänderten Regelungen gelten über die sogenannte „Ausstrahlwirkung“ auch für die Geschäftsführer einer GmbH.

- §91 Abs 2 AktG: „Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden. [...]“

Bundesdatenschutzgesetz (BDSG)

Datenschutzrechtliche Vorschriften finden sich im Landes- wie im Bundesrecht; sie regeln den Umgang von öffentlichen und nicht-öffentlichen Stellen (z.B. Unternehmen) mit personenbezogenen Daten.

- § 9 S. 1 BDSG: „Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. [...]“.

Die auf die im Gesetzestext verwiesene Anlage enthält Anforderungen bezüglich Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle und Verfügbarkeitskontrolle.

Staatsvertrag für Mediendienste (MDStV)

Der Staatsvertrag für Mediendienste hat das Ziel, einheitliche Rahmenbedingungen für die verschiedenen Nutzungsmöglichkeiten von Informations- und Kommunikationsdiensten, die an die Allgemeinheit gerichtet sind, zu schaffen. Der MDStV richtet sich hauptsächlich an Unternehmen, die gewerbsmäßig Mediendienste anbieten. Stellt ein Unternehmen jedoch seinen Mitarbeitern einen Internetzugang zur Nutzung bereit, so wird auch dieses Unternehmen zum Dienstleister und hat die entsprechenden Vorschriften des MDStV zu beachten.

- § 13 Abs. 2 MDStV: „Der Anbieter von Mediendiensten hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass [...] 3. der Nutzer Mediendienste gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann. [...]“

Teledienstgesetz (TDG) und Teledienstschutzgesetz (TDDSG)

Das Teledienstgesetz richtet sich an Dienstleister, die „eigene oder fremde Teledienste zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln“. In diesem Sinne ist bspw. jede Organisation, die Informationen auf einer Internet-Webseite veröffentlicht oder die Möglichkeit zur Kontaktaufnahme über E-Mail bietet, ein Dienstleister. Das Teledienstschutzgesetz gibt den datenschutzrechtlichen Rahmen vor, in dem Dienstleister die personenbezogenen Daten der Nutzer erheben, verarbeiten und nutzen dürfen.

- § 4 Abs. 4 TDDSG: „Der Dienstleister hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass, [...] der Nutzer Teledienste gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann. [...]“

Telekommunikationsgesetz (TKG)

Dieses Gesetz richtet sich an geschäftsmäßige Erbringer von Telekommunikationsdiensten. Unternehmen, deren Mitarbeiter ihren Telefonanschluß oder ihren Internetanschluß am Arbeitsplatz auch zu privaten Zwecken nutzen, zählen als Erbringer von Telekommunikationsdiensten und fallen somit in den Anwendungsbereich.

- § 85 Abs. 2 TKG: „Zur Wahrung des Fernmeldegeheimnisses ist verpflichtet, wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt. [...]“
- § 87 Abs. 1 TKG: „Wer Telekommunikationsanlagen betreibt, die dem geschäftsmäßigen Erbringen von Telekommunikationsdiensten dienen, hat bei den zu diesem Zwecke betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutz [...] 2. der programmgesteuerten Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe, [...] 4. von Telekommunikations- und Datenverarbeitungssystemen gegen äußere Angriffe und Einwirkungen von Katastrophen zu treffen.“

Basel II

Mit der Umsetzung der Banken- und Kapitaladäquanzrichtlinie (Basel II) in das deutsche Recht zum 01.01.2007 wird dieses für alle Branchen wichtige Regelwerk zum Gesetz. Basel II sieht vor, insbesondere bei Unternehmen vor jeder Kreditentscheidung eines Kreditgebers eine individuelle Einschätzung der Bonität vorzunehmen. Dies erfolgt auf Basis interner Rating-Systeme der kreditgewährenden Finanzinstitute oder durch externes Rating. Nach dem vom namengebenden Baseler Ausschuss für Bankenaufsicht erarbeiteten Konzept spielen bei der Vergabe sowohl Markt- und Kreditrisiken als auch operationelle Risiken des kreditnehmenden Unternehmens eine Rolle.

- Zu den operationellen Risiken eines Unternehmens zählen auch die Risiken, die sich aus dem Einsatz von Informationstechnologie in den Unternehmensprozessen ergeben. Gefordert ist ein aktives IT-Risiko-Management, das sich mit allen Aspekten der IT-Sicherheit für das jeweilige Unternehmen befasst. Wichtige IT-Systeme müssen redundant vorhanden, Verfügbarkeiten gesichert sein, Angriffe auf die IT-Systeme von innen und außen wirksam abgewehrt werden, Notfallpläne sollten erarbeitet sein und so weiter.

Als Folge der Relevanz dieser Faktoren kann ein darauf vorbereitetes Unternehmen mit gut dokumentiertem IT-Risiko-Management bei der Kreditentscheidung einer Bank durchaus für günstigere Konditionen sorgen.

Verordnung und Verlautbarungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

Die Bundesanstalt für Finanzdienstleistungsaufsicht (früher: Bundesaufsichtsamt für das Kreditwesen – BaFin) erlässt auf Basis gesetzlicher Ermächtigungen u.a. Verordnungen und veröffentlicht Verlautbarungen, die Banken und andere Finanzdienstleister betreffen, über die die BaFin die Aufsicht führt. In der „Verlautbarung über Mindestanforderungen an das Betreiben von Handelsgeschäften der Kreditinstitute“ werden u.a. die Anforderungen an das Risikomanagement und die Ausgestaltung der Internen Revision definiert:

- Rd-Nr. 3.1 Anforderungen an das System: „[...] [Das Risikomanagementsystem] soll in ein möglichst alle Geschäftsbereiche der Bank umfassendes Konzept zur Risikoüberwachung und –steuerung eingegliedert sein und dabei die Erfassung und Analyse von vergleichbaren Risiken auf Nichthandelsaktivitäten ermöglichen. [...]“
- Rd-Nr. 3.4 Betriebsrisiken: „[...] Eine schriftliche Notfallplanung hat u.a. sicherzustellen, dass beim Ausfall der für das Handelsgeschäft erforderlichen technischen Einrichtungen kurzfristig einsetzbare Ersatzlösungen zur Verfügung stehen [...] Die Verfahren, Dokumentationsanforderungen, DV-Systeme und Notfallpläne, die im Handelsgeschäft angewandt werden, sind regelmäßig zu überprüfen.“
- Rd-Nr. 5 Revisionen: „Die Einhaltung der Mindestanforderungen ist von der Innenrevision in unregelmäßigen, angemessenen Abständen zu prüfen. [...] Jeder Teilbereich der Mindestanforderungen ist zumindest in einem Turnus von drei Jahren zu prüfen [...] Als wesentliche Prüfungsfelder sind anzusehen: Veränderungen bei den EDV-Systemen [...]“.

Quellenangabe: Auszüge aus der „Studie zur Durchführung von Penetrationstests“ des Bundesamts für Sicherheit in der Informationstechnik (BSI).