von Rechtsanwalt **Max-Lion Keller**, LL.M. (IT-Recht)

Rechtsrahmen der IT-Sicherheit

Ein Gesetz, welches sämtliche Regelungen mit Bezug zur IT-Sicherheit zusammenfassen würde, gibt es nicht. Vielmehr hat man sich die entsprechenden gesetzlichen Regelungen mühsam aus verschiedenen gesetzlichen Bestimmungen zusammenzusuchen. Dies wird wohl auch ein Grund mit dafür sein, dass sich viele Unternehmen bzw. deren Geschäftsführung noch immer nicht darüber im Klaren sind, dass der Gesetzgeber sie konkret zur Errichtung einer effizienten und vor allem sicheren IT-Infrastruktur verpflichtet hat. Nur wer einen Überblick über die relevanten Gesetze und Verordnungen hat und ein geeignetes Sicherheitskonzept verfolgt, kann sich hier vor rechtlichen Konsequenzen schützen. Rechtsanwalt Max-Lion Keller fasst für GULP Leser zusammen, welche Gesetze, Verordnungen und Richtlinien in Sachen "IT-Sicherheit" zu beachten bzw. befolgen sind.

IT-Sicherheit bedeutet nichts anderes, als dass die

- ständige Verfügbarkeit,
- die Vertraulichkeit und
- die Unversehrtheit von Daten bzw. der Informationstechnik

zur Aufrechterhaltung der Geschäftsprozesse und der Abwehr von Schäden gewährleistet werden muss. Diesbezüglich nimmt der Gesetzgeber Unternehmen und ihre (IT-)Verantwortlichen mit diversen Gesetzen, Verordnungen und Richtlinien in die Pflicht. Einerseits dient das dem Schutz der eigenen Unternehmensdaten, andererseits müssen überlassene Daten vor unberechtigtem Zugriff geschützt werden - insbesondere personenbezogene Datenbestände. Aus den folgenden gesetzlichen und vertraglichen Regelungen zu Fragen der IT-Sicherheit lassen sich unmittelbare Handlungs- wie auch Haftungsverpflichtungen der Geschäftsführung bzw. des Vorstands sowie den IT-Verantwortlichen eines Unternehmens ableiten.

Risikofrüherkennung gem. KonTraG

Hierbei muss in aller Kürze auf das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) hingewiesen werden. Dieses Gesetz wurde bereits im Mai 1998 verabschiedet. Der Gesetzgeber bezweckte damit die Verbesserung der Kontrolle und der Transparenz in Aktiengesellschaften und auch in größeren GmbHs. Dies wurde regelungstechnisch dadurch erreicht, dass durch das KonTraG das damals bereits vorhandene Aktiengesetz (AktG) sowie das GmbH-Gesetz entsprechend ergänzt (§ 91 II AktG, § 116 AktG) bzw. entsprechend angewendet wurden (§ 43 GmbHG). Neu bei Inkrafttreten des KonTraG war nun insbesondere, dass der Vorstand einer AG und insbesondere auch die Geschäftsführung einer GmbH verpflichtet wurde, geeignete Maßnahmen zur frühzeitigen Erkennung von Entwicklungen zu treffen, die den Fortbestand der Gesellschaft konkret gefährden (vgl. § 91 II AktG). Um dies zu gewährleisten bedarf es eines Überwachungssystems, welches in der Lage ist, bei kritischen Situationen auch tatsächlich frühzeitig Alarm zu schlagen. Damit aber nicht genug.

Einrichtung eines Risikomanagements

Zugleich wird der Geschäftsführung durch Gesetz auferlegt, ein unternehmensweites Risikomanagement zu installieren, welches alle Bedrohungen erfasst, die durch IT-Systeme und deren Einsatz entstehen können. Demnach sind also die Vorstände nicht nur unmittelbar gesetzlich aufgefordert, angemessene Überwachungsmechanismen einzurichten. Sie haben vielmehr auch präventiv durch entsprechende Informations- und Vorsorgemaßnahmen die Sicherheit der in ihrem Unternehmen verwendeten IT-Systeme zu gewährleisten. Ein solches unternehmerisches Risikomanagement hat man sich wie folgt vorzustellen:

1. Schritt: Zunächst müssen im Rahmen einer Risikoanalyse alle Risiken im Zusammenhang mit dem Einsatz von unternehmenseigenen IT-Systemen ermittelt und analysiert werden, um dadurch in die Lage versetzt zu werden, das Gesamtrisiko für das Unternehmen einschätzen zu können.

2. Schritt: Anschließend gilt es, ein Sicherheitskonzept zu erstellen, um das ermittelte Risiko basierend auf einer wirksamen Risikoprävention zu reduzieren. Dabei wäre tatsächlich schon viel gewonnen, wenn sich das jeweilige Unternehmen zunächst einmal zum Ziel setzen würde, die bereits eingangs erwähnten Grundwerte der IT-Sicherheit (Verfügbarkeit, Unversehrtheit, Vertraulichkeit der Daten) sicher zu stellen. Dazu gehört insbesondere eine regelmäßig wie auch häufige Datensicherung, ein wirksamer Sabotage- und Ausfallschutz und natürlich auch der Schutz vor missbräuchlicher IT-Nutzung (durch Mitarbeiter oder Dritte).

3. Schritt: Dieses Sicherheitskonzept ist dann auch in die Praxis umzusetzen und vor allem penibel

einzuhalten.

Datenschutzrecht

Während die oben genannten Formulierungen für den juristischen Laien teilweise recht allgemein und eher unverbindlich klingen ("Sorgfalt eines ordentlichen Geschäftsmannes"), wird das Datenschutzrecht in dieser Hinsicht sehr viel genauer. So verpflichtet § 9 Bundesdatenschutzgesetz (BDSG) i.V.m. der Anlage zu § 9 Satz 1 BDSG alle datenverarbeitenden Stellen, durch geeignete technische wie auch organisatorische Maßnahmen die Gewährleistung der datenschutzrechtlichen Anforderungen sicherzustellen. Aus der Anlage zu § 9 Satz 1 BDSG wird deutlich, welche Maßnahmen in diesem Zusammenhang konkret gemeint sind, wobei im Folgenden insbesondere auf die drei wichtigsten Maßnahmen eingegangen werden soll:

- **Zugangskontrolle:** Das datenverarbeitende Unternehmen hat sicherzustellen, dass kein Unbefugter Zutritt zu den Computern hat, auf denen personenbezogene Daten verarbeitet werden. Es entspricht der Realität, dass sich Computer meist in normalen Büroräumen befinden, in denen es in aller Regel keine besonderen Zutrittsregelungen z. B. für Gebäude- und Raumreiniger gibt. Schon einfache organisatorische Maßnahmen können hierbei helfen, das Risiko mit einzudämmen. So gehören etwa Computer, die als Server eingesetzt werden, in einen zugangsgeschützten Extraraum.
- **Zugriffskontrolle:** Das datenverarbeitende Unternehmen hat sicherzustellen, dass die Berechtigten nur auf die Daten zugreifen können, für die sie eine Zugriffsberechtigung haben. Das IT-System muss daher in der Lage sein, differenzierte Zugriffsberechtigungen technisch umzusetzen - etwa durch eine Benutzerkontrolle, die die berechtigten Benutzer identifiziert und auch authentifiziert.
- **Weitergabekontrolle:** Gerade der so genannten Weitergabekontrolle (oder auch Datenträgerkontrolle) kommt beim Computer-Einsatz eine herausragende Bedeutung zu. So gehört es heute zur Grunderkenntnis der IT-Sicherheit, dass etwa der Umgang mit Disketten, CDs oder sonstigen Speichermedien, die in großen Mengen vorhanden sein können, trotz eines hohen organisatorischen Aufwandes kaum mit hinreichender Sicherheit organisiert werden kann. Daher müssen hier nach Möglichkeit Maßnahmen getroffen werden, die die Verwendung beweglicher Datenträger beschränkt - etwa auf bestimmte Benutzergruppen.

Bestellung eines Datenschutzbeauftragten

Angesichts des Umstands, dass heutzutage in nahezu jedem Unternehmen jedenfalls in der IT-Abteilung, im Personalwesen und der Buchhaltung, oft aber auch in den Fachabteilungen, über Netzwerke verbundene Computer vorhanden sind und mit personenbezogenen Daten gearbeitet wird, entgingen in der Vergangenheit nur wirklich kleine Unternehmen der Pflicht zur Bestellung des Beauftragten. Der Gesetzgeber plante nun auch diejenigen Unternehmen, die höchstens neun Personen beschäftigen, zu entlasten. So schuf er das "Erste Gesetz zum Abbau bürokratischer Hemmnisse insbesondere in der mittelständischen Wirtschaft". Am 26. August 2006 kam es zu einer entsprechenden Novellierung des BDSG mit folgenden Konsequenzen:

- Die Pflicht zur Bestellung von Datenschutzbeauftragten wird auf Unternehmen reduziert, die mindestens zehn (statt bisher fünf) mit Personendatenverarbeitung betrauten Personen beschäftigen. Damit entfällt für viele kleine Unternehmen die kostenintensive Bestellung eines betrieblichen Datenschutzbeauftragten. Aber Vorsicht: Auch der Bezugsgegenstand ändert sich, da nunmehr das Gesetz auf Personen abhebt. "Personen" im Gesetzessinn sind dabei zunächst einmal alle im Unternehmen tätigen Menschen, also nicht nur, wie zuvor Angestellte, sondern auch z.B. Auszubildende und Geschäftsführer. Frei stellt es das BDSG jedoch in diesem Zusammenhang auch, ob ein eigener Mitarbeiter (sog. "interne Lösung") oder eine Person, die dem Unternehmen nicht angehört, zum Datenschutzbeauftragten bestellt wird (sog. "externe Lösung"), vgl. § 4f II S. 3 BDSG.
- Die erwähnte Anhebung dieses Schwellenwerts gilt nicht nur für die Bestellung eines betrieblichen Datenschutzbeauftragten, sondern auch für die Meldepflichten des Unternehmens.
- Besteht eine Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz, ist die Verpflichtung spätestens innerhalb eines Monats nach Aufnahme der betrieblichen Tätigkeit zu erfüllen.
- Unabhängig von der Anzahl der Arbeitnehmer ist ein Datenschutzbeauftragter auch für den Fall zu bestellen, dass automatisierte Verarbeitungen vorgenommen werden, die wegen besonderer Sensitivität vor Einsatz zu prüfen sind (Vorabkontrolle) oder personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung oder der anonymisierten Übermittlung erhoben, verarbeitet oder genutzt werden.

Sonderregelungen

Zum Teil stellen branchenspezifische Regelungen auch strengere Anforderungen als die oben bereits erwähnten Regelungen an die IT-Sicherheit, etwa bei Banken oder Versicherungen. Zudem enthält das Strafgesetzbuch für bestimmte Berufsgruppen, wie Ärzte, Rechtsanwälte oder Angehörige sozialer Berufe Sonderregelungen, die Freiheitsstrafen vorsehen, wenn etwa vertrauliche Angaben von Patienten, Mandanten bzw. Klienten ohne deren ausdrückliche Einwilligung öffentlich gemacht werden (vgl. § 203 StGB). Insbesondere auch die IT-Security-Verantwortlichen in Unternehmen der privaten Kranken-, Unfall- oder Lebensversicherung oder einer sonstigen privatärztlichen Verrechnungsstelle werden hier besonders in die Pflicht genommen. Unter Umständen kann somit bereits ein fahrlässiger Umgang mit Informationstechnik den Tatbestand des § 203 StGB erfüllen.

Vertragliche Regelungen

Selbstverständlich lassen sich auch über vertragliche Regelungen Rechtspflichten im Hinblick auf die IT-Sicherheit begründen. Beispiele dafür können etwa sein:

- **Vertraulichkeitsvereinbarungen (non-disclosure agreement):** Hier geht es zumeist um eine Vereinbarung zwischen einem Unternehmer und einer für den Unternehmer tätig werdende Person (beispielsweise einem externen Mitarbeiter/IT-Dienstleister), die ihn vor der Weitergabe vertraulicher Informationen an Dritte schützen soll. Der Unterzeichner stimmt dabei zu, ihm im Rahmen seiner Tätigkeit zugänglich gemachte Daten, Informationen und Wissen (insbesondere Betriebsgeheimnisse wie technologisches oder Prozesswissen) geheim zu halten.
- **Softwarehinterlegungsvereinbarung (Escrow Agent Agreement):** Der Escrow-Agent hat den Quellcode gemäß den zwischen allen Parteien in einem Hinterlegungsvertrag niedergelegten Bestimmungen aufzubewahren. Unter anderem legt dieser Vertrag auch fest, unter welchen Umständen der Quellcode an den Anwender herausgegeben werden muss. Der Escrow-Agent hat hierbei in aller Regel die vertragliche Verpflichtung, den unberechtigten Zugriff auf die hinterlegte Software unter allen Umständen zu verhindern.
- **IT-Outsourcing:** Natürlich besteht auch für IT-Outsourcing Dienstleister die vertragliche Verpflichtung, die Absicherung der verwendeten IT-Systeme sicherzustellen. Dies gilt insbesondere für die Vertraulichkeit der Daten.

Verletzt ein Vertragspartner vertragliche Pflichten, die ihm gerade in Bezug auf die IT-Sicherheit auferlegt wurden, treffen ihn die Sanktionen, die der jeweilige Vertragstext für diesen Fall vorhält. Die hier

vorstellbaren Konsequenzen sind mannigfaltig und reichen von Vertragsstrafen, Herabstufung der Bonität (Stichwort: Basel II) über den Imageverlust des Unternehmens bis hin zur Erhöhung von Versicherungsbeiträgen.

Autor:
RA Max-Lion Keller, LL.M. (IT-Recht)
Rechtsanwalt