MARIO
LAURISCHK
RECHTSANWALT

Kurzrefererat „Datenschutzrechtliche Haftungsrisiken"

RA M. Laurischk im Rahmen der IT-Fachmesse „IT-Profits", 15.04.2005, Berlin

1. Risiken bei mangelhaftem Datenschutz:

a) Entstehung eigener Schäden.

b) Entstehung von Fremdschäden, für die gehaftet wird.

c) Begehung von Ordnungswidrigkeiten / Straftaten.

Zu a):
Bei dem Stichwort „Datenschutz" denken die meisten zunächst an den Schutz der eigenen Daten und die Risiken für das eigene Unternehmen:

- Durch Datenverlust bedingte Betriebsausfälle infolge von Viren- oder Hackerangriffen.

Hierzu kann es kommen, wenn eigene Mitarbeiter in der Lage sind, unkontrolliert Programme zu installieren oder aus dem Internet zu laden und diese Viren oder Trojaner enthalten.

- Ausspionieren von Betriebsgeheimnissen durch Außenstehende oder eigene Mitarbeiter, die unbefugten Zugriff auf interne Daten erlangen konnten.
Dies kann u. a. geschehen durch fehlende Absicherung von Daten im betriebsinternen Netzwerk oder mangelhaften bzw. keinen Schutz von Computern, die mit dem Internet verbunden sind (fehlende oder falsch konfigurierte Firewall). Eine große Gefahr stellt auch der sorglose Umgang der eigenen Mitarbeiter mit Betriebsdaten dar, die ungeschützt und unkontrolliert per e-Mail verbreitet oder auf Diskette, CD oder Memory-Stick mit nach Hause oder zum neuen Arbeitgeber genommen werden.
Bei derartigen Schäden besteht stets die Gefahr, dass den Verantwortlichen (Inhaber, Geschäftsführer, IT-Beauftragter) grobe Fahrlässigkeit nachgewiesen werden kann und eine evtl. bestehende Betriebsversicherung daher für die entstandenen Schäden nicht eintrittspflichtig ist. Daher sollte im eigenen Interesse vorgesorgt werden.

Zu b):
Alle vorgenannten Szenarien können aber weiterhin auch Ansprüche Dritter entweder gegen das eigene Unternehmen oder gegen die für den Schaden unmittelbar Verantwortlichen begründen. Dies wäre beispielsweise der Fall, wenn wichtige Daten eines Dritten, die im eigenen Unternehmen gespeichert sind, von Mitarbeitern oder Viren bzw. Trojanern verändert, gelöscht oder an Außenstehende verbreitet werden.

- Vertragliche Ansprüche:
Besteht zu dem Geschädigten eine Vertragsbeziehung, und führt ein Datenverlust dazu, dass die ihm geschuldete Leistung fehlerhaft, verspätet oder überhaupt nicht erbracht wird, so kann dieser:

- vom Vertrag zurücktreten und sich von seiner Leistungsverpflichtung befreien.

- Schadenersatz oder eine vorher vereinbarte Vertragsstrafe verlangen. Der Schadenersatz kann entweder beinhalten, dass dem Vertragspartner alle nutzlosen Aufwendungen zu erstatten sind, er also so gestellt wird, als ob der Vertrag nie zustande gekommen wäre, oder dass ihm das positive Interesse aus dem Vertrag, üblicherweise in Form des entgangenen Gewinns, ersetzt wird. Beides kann vor allem bei geplatzten Großaufträgen schnell existenzbedrohende Ausmaße annehmen. Aber auch Schäden aufgrund der Verletzung von Nebenpflichten sind zu ersetzen, etwa wenn der Vertragspartner durch unberechtigte Weitergabe sensibler Vertragsdaten oder durch Überlassung eines mit Viren befallenen Datenträgers geschädigt wird. Allerdings sollte jeder für den Fall, dass er selbst von Viren betroffen sein könnte, Vorsorge treffen, da anderenfalls bei auftretenden Schäden regelmäßig ein zur anteiligen Kostentragung verpflichtendes Mitverschulden anzunehmen sein wird.

- Deliktische Ansprüche:

Diese greifen ein, wenn zu einem Geschädigten keine vertragliche Beziehung besteht, aber trotzdem, z.B. durch Computerviren oder mangelhafte Datensicherheit, ein Schaden verursacht wurde:

- Gemäß § 823 BGB haftet zunächst die den Schaden unmittelbar verursachende Person selbst.

- Gemäß § 831 BGB haftet zusätzlich auch das Unternehmen, sofern nicht nachgewiesen werden kann, dass bei der Auswahl der entsprechenden Person für die gefahrverursachende Tätigkeit die im Verkehr erforderliche Sorgfalt beachtet wurde.

Zu beachten ist ferner, dass - entgegen der landläufigen Meinung - in diesen Fällen auch eine persönliche Haftung der Verantwortlichen möglich ist.

Der Einzelkaufmann haftet ohnehin umfassend mit seinem Vermögen für sämtliche Verbindlichkeiten. Aber auch der GmbH-Geschäftsführer kann sich nicht ohne weiteres auf die alleinige Haftung der GmbH berufen. Zwar haftet die Gesellschaft nach außen zunächst nur mit ihrem Gesellschaftsvermögen. Allerdings hat der Geschäftsführer gemäß § 43 GmbHG in allen Angelegenheiten die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden und haftet gegenüber der Gesellschaft anderenfalls persönlich für den entstandenen Schaden. Gleiches gilt für den Vorstand einer AG gemäß § 93 AktG.

Somit haftet im Außenverhältnis zwar nur das Unternehmen, indirekt aber auch der Geschäftsführer.
Sofern die Gewährleistung der Datensicherheit jedoch einem Dritten übertragen wird, sollte nicht der erstbeste Mitarbeiter „verdonnert" werden, sondern ist darauf zu achten, dass diese Person sorgfältig ausgewählt wird und tatsächlich auch die hierzu erforderlichen Kenntnisse und Fähigkeiten aufweist. Sollte nämlich ein vertraglich nicht gebundener Außenstehender einen Schaden erlitten haben, hat der Geschäftsführer bei sorgfältig erfolgter Auswahl des Datenschutz-Verantwortlichen die Möglichkeit, seine grundsätzlich bestehende Ersatzpflicht für den durch den Spezialisten verursachten Schaden gemäß § 831 BGB vollständig auf ihn abzuwälzen. Dies wäre z.B. der Fall, wenn ein Unternehmen virenbehaftete e-Mails an potentielle Kunden verschicken lässt und den Empfängern hierdurch Schäden entstehen. Sollte diese Aktion von einem kompetenten und sorgfältig ausgesuchten IT-Beauftragten veranlasst worden sein, kann sich der Geschäftsführer zu Lasten seines Beauftragten von einer Haftung freizeichnen, wenn und soweit ihn kein Auswahl- oder Organisationsverschulden trifft.
In diesem Zusammenhang kann auch die Beauftragung eines externen IT-Unternehmens günstig sein, da man dieses dann aufgrund vertraglicher Pflichtverletzung leichter in Regress nehmen kann, als einen eigenen Mitarbeiter.
Diese Überlegungen spielen jedoch im Rahmen von Schäden, die aus einer vertraglichen Beziehung mit dem Geschädigten resultieren, nur eine untergeordnete Rolle. In diesen Fällen haftet das Unternehmen gemäß § 278 BGB umfassend für das Verschulden des von ihm beauftragten IT-Spezialisten und kann sich nicht mit dem Nachweis sorgfältiger Auswahl der Haftung entziehen. Allerdings kann es auch hier wieder sinnvoll sein, einen externen Dienstleister zu beauftragen, an den eventuelle Schadenersatzforderungen weitergereicht werden können. Die Inanspruchnahme eines nicht im eigenen Unternehmen beschäftigten Datenschutzbeauftragten hat im allgemeinen auch den Vorteil, dass ein Außenstehender nicht in die betrieblichen Abläufe integriert ist und Risiken daher besser erkennen und objektiv bewerten kann.

Zu c):

Die Nichteinhaltung von Datenschutzvorschriften kann schließlich zur Verwirklichung von Ordnungswidrigkeiten- und Straftatbeständen führen:

- Ordnungswidrigkeiten:

Neben spezialgesetzlichen Regelungen finden sich die maßgeblichen Bußgeldvorschriften in § 43 BDSG. Nach dieser Vorschrift handelt u. a. ordnungswidrig, wer vorsätzlich oder fahrlässig

- einen Datenschutzbeauftragten nicht oder nicht rechtzeitig bestellt, obwohl er mehr als vier Arbeitnehmer mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt,
- personenbezogene Daten außerhalb ihrer Zweckbestimmung (gem. § 28 BDSG) übermittelt oder nutzt,
- gegen den Willen des Betroffenen personenbezogene Daten in Adress-, Rufnummern- oder Branchenverzeichnisse aufnimmt,
- unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet, sich oder einem anderen verschafft oder die Übermittlung durch unrichtige Angaben erschleicht.

Die Ordnungswidrigkeiten können mit einer Geldbuße bis zu EUR 25.000,--, in dem letztgenannten Fall sogar bis EUR 250.000,-- geahndet werden.

- Strafvorschriften:

Bei besonders schwerwiegenden Verstößen droht sogar eine Geld- oder Freiheitsstrafe:

- gem. § 44 BDSG bis zu 2 Jahren für die unbefugte Erhebung, Verarbeitung, Verschaffung oder Erschleichung der Übermittlung personenbezogener Daten, die nicht allgemein zugänglich sind, wenn hierbei gegen Entgelt oder in Bereicherungsabsicht gehandelt wird,
- gem. § 303a StGB ebenfalls bis zu 2 Jahren für die rechtswidrige Löschung, Unterdrückung, Veränderung oder das Unbrauchbarmachen fremder Daten,
- gem. § 303b StGB bis zu 5 Jahren für die Störung einer wichtigen Datenverarbeitung eines fremden Unternehmens oder einer Behörde durch die Manipulation von Daten, Datenträgern oder der Datenverarbeitungsanlage.

In diesen Fällen kann - auch wenn die Straftaten unmittelbar von Mitarbeitern begangen werden - ebenfalls eine strafrechtliche Verantwortung des Vorgesetzten oder Geschäftsführers gegeben sein. Eine Zurechnung kann hierbei als Anstiftung, Beihilfe, mittelbare Täterschaft, Mittäterschaft oder durch pflichtwidriges Unterlassen in einer Garantenstellung erfolgen, wenn der Verantwortliche Kenntnis von der Tatbegehung seiner Mitarbeiter hat oder diese sogar fördert.

MARIO
LAURISCHK
RECHTSANWALT

2. Schutzmaßnahmen:

- Bestellung eines Datenschutzbeauftragten mit umfassenden IT-Kenntnissen. Dies kann ein eigener Mitarbeiter oder externer Dienstleister sein.

- Erarbeitung von Richtlinien für eine sparsame Datenverarbeitung und kontrollierte Datenübermittlung sowie den Schutz der eigenen IT.

- Regelmäßige Schulung der Angestellten zur Sensibilisierung im Umgang mit unternehmens- und personenbezogenen Daten.