04. Oktober 2007

Haftung inklusive

von Martin Koch, Axel Czarnetzki Ariane Rüdiger

Seite 1 | 2 | 3 | 4

Gold wert sind oft die Daten, die sich – häufig schlecht gesichert – in Unternehmens-Laptops verstecken.

Der Stellenwert der IT für Unternehmen jeglicher Größe wächst stetig. Damit werden auch die möglichen Auswirkungen einer Infektion mit Schadsoftware, eines Datenverlusts oder auch nur einer längeren Betriebsstörung durch einen Hard- oder Softwareausfall immer schwerwiegender. Durch Datendiebstahl können Betriebsgeheimnisse in die Hände eines Konkurrenten geraten und dessen Marktposition so sehr stärken, dass die Existenz des eigenen Unternehmens bedroht ist. Ein durch eine Vireninfektion verursachter Server-Ausfall kann nicht nur das eigene Geschäft unterbrechen, sondern auch – wie beispielsweise im Fall eines Internet-Providers – das Geschäft von Dutzenden von Kunden lahm legen. Produktionsstörungen durch IT-Ausfälle können zu verspäteten Lieferungen an Kunden führen, deren Schadensersatzforderungen unter Umständen immens sind und den Bestand eines Unternehmens bedrohen. Nicht zuletzt verfügen Finanzdienstleister, aber auch sonstige Unternehmen über Kundendaten, deren Vertraulichkeit durch gesetzliche Bestimmungen wie das Bundesdatenschutzgesetz (BDSG) festgeschrieben ist. Gelangen diese Daten aufgrund mangelnder Sicherheitsvorkehrungen in die Hände Dritter, ist ein Straftatbestand wegen Verletzung des BDSG erfüllt. Verstöße können etwa Bußgelder bis zu 25000 Euro und Freiheitsstrafen von bis zu zwei Jahren zur Folge haben (§§43, 44 BDSG). Diese Beispiele beschreiben natürlich jeweils besonders düstere Szenarien. Doch müssen Unternehmen sich auch gegen unwahrscheinliche, aber dafür besonders schwerwiegende Schäden absichern. Es liegt daher im besten Interesse der Geschäftsleitung, Schäden im IT-Bereich zu verhindern, denn im Zweifel muss die Vorstandsetage vor Gericht für die eingetretenen Folgen gerade stehen.

Eigentlich ist der Sachverhalt ganz einfach: Nach den §§303a ff StGB wird ein Hacker mit zwei Jahren Freiheitsentzug oder einer Geldstrafe bedroht, wenn er die Daten eines Unternehmens rechtswidrig löscht, verändert oder unbrauchbar macht. §303b StGB droht sogar bis zu fünf Jahre Haft an, falls dadurch der Betrieb eines fremden Unternehmens oder einer Behörde unterbrochen wird. Und gemäß §§202a ff StGB drohen bis zu drei Jahre Freiheitsstrafe für den Diebstahl von besonders gesicherten und nicht für den Dieb bestimmten Daten. Die zivilrechtlichen Ansprüche eines Unternehmens gegen Hacker auf Ersatz des durch das Hacking entstandenen Schadens werden durch den §823 II BGB geregelt. Das schließt eventuell entstandene Vermögensschäden und die Schadensersatzansprüche Dritter mit ein. In der Praxis können jedoch kaum ausreichende Ansprüche gegen den Täter geltend gemacht werden. Erstens ist die Ermittlung in den Weiten des Internets über Landes- und Staatsgrenzen hinweg extrem schwierig bis unmöglich. Zweitens kann eine Einzelperson einen Schaden in Millionenhöhe kaum kompensieren. Im Ergebnis bleibt das Unternehmen in der Regel auf seinem Schaden beziehungsweise auf den Ersatzansprüchen von Kunden und Geschäftspartnern sitzen. Dann können Vorstände und Geschäftsführer für die Folgen verantwortlich gemacht werden, sofern sie ihre Sorgfaltspflichten gegenüber dem Unternehmen nicht ausreichend wahrgenommen haben. Handhabe dafür liefern Strafrecht und Zivilrecht.

Diverse Normen machen Vorstände und Geschäftsführer von Unternehmen persönlich haftbar, wenn sie ihre Sorgfaltspflichten hinsichtlich des Schutzes des Unternehmens vernachlässigen.

Strafrechtlich sind Verantwortliche haftbar, wenn durch eine Handlung innerhalb des Unternehmens aufgrund von Entscheidungen der Unternehmensleitung ein Straftatbestand erfüllt wurde und offensichtlich erforderliche Schutzmaßnahmen durch das Management unterlassen wurden. §14 StGB behandelt den Vertreter eines Unternehmens wie einen Straftäter, wenn ein Straftatbestand durch das Unternehmen begangen wurde. Zivilrechtlich haften Geschäftsführer (§43 GmbHG) beziehungsweise Vorstände (§93 II AktG) gegenüber dem Unternehmen, wenn sie sich nach §266 StGB einer Verletzung der Vermögensbetreuungspflicht schuldig gemacht haben. Sie verlangt, dass Geschäftsführer, Vorstände und Aufsichtsräte sämtliche erkennbar notwendigen Maßnahmen ergreifen, um Schäden vom Unternehmen abzuwenden. Hinsichtlich der IT müssen sie also alle erforderlichen Maßnahmen treffen, um Schaden durch Hackerangriffe, Vireninfektionen oder auch längere Betriebsunterbrechungen durch einen Serverausfall abzuwenden. Diese Rechtsauffassung hat der Bundesgerichtshof (BGH) durch das ARAG-Garmenbeck-Urteil (BGHZ 135, 244) aus dem Jahr 1997 festgeschrieben. Da Vorstände und Geschäftsführer selbst kaum die Zeit und das Fachwissen haben, um selbst für eine Absicherung der IT zu sorgen, müssen sie zumindest die notwendigen organisatorischen Maßnahmen treffen. Sofern nicht im eigenen Haus eine mit ausreichenden Ressourcen und Kompetenzen ausgestattete IT-Abteilung existiert, kann man auf Beratungsunternehmen wie etwa Symantec Consulting Services zurückgreifen. Der IT-Berater führt Sicherungsmaßnahmen und Mitarbeiterschulungen durch und hilft so, die IT-Sicherheit stets auf aktuellem Stand zu halten. Die Arbeit eines solchen Beratungsunternehmens muss in das Berichtssystem des eigenen Unternehmens eingebettet sein. Um der Sorgfaltspflicht der Unternehmensleitung zu genügen, muss sie darauf achten, dass der gewählte IT-Dienstleister das erforderliche Wissen hat und seriös ist. Seine Mitarbeiter müssen sich kontinuierlich fortbilden. Nicht zuletzt muss die Beratungsfirma selbst ausreichend abgesichert sein, um bei einem Schaden die (vertraglich festzulegende) zivilrechtliche Haftung leisten zu können. Durch die Auswahl einer derartigen Beraterfirma kann die Geschäftsführung Schaden vom Unternehmen abwenden und sich selbst von eventuellen Haftungsansprüchen befreien. Sollte es dann immer noch zu einem Schaden kommen, können anfallende – eigene oder fremde – Schadensersatzansprüche an die Beraterfirma weitergereicht werden. Um Haftungsrisiken dauerhaft zu vermeiden, ist darüber hinaus die regelmäßige Analyse der Bedrohungssituation und der eigenen Absicherung notwendig. Verändert sich die Gefährdungslage, müssen auch die eigenen Sicherungsmaßnahmen angepasst werden.

Vorstände und Geschäftsführer müssen die IT-Sicherheit ihres Unternehmens als Chefsache verstehen. Sie sollten Prozesse, Abläufe und ein Berichtswesen implementieren, das eine ununterbrochene Beobachtung aller IT-Risiken gewährleistet. Es muss sicherstellen, dass eine sich ändernde Bedrohungssituation auch zu geänderten Sicherheitsmaßnahmen führt. Bei der Implementierung solcher Abläufe auch unter Berücksichtigung des Transparenz-Gesetzes und von Corporate Governance empfiehlt sich die Einschaltung einer spezialisierten Rechtsanwaltsgesellschaft. Sie gewährleistet eine angemessene Absicherung der Risiken des Unternehmens und seiner Leitungsorgane. Der erste Schritt zu einer umfassenden Sicherung des Unternehmens gegen IT-lastige Angriffe besteht aber darin, sich des bestehenden Risikos bewusst zu werden. Die Geschäftsführung muss erkennen, dass es nicht mit der Installation von Firewall und Virenscannern getan ist. Sicherheit erfordert vielmehr kontinuierliche Aufmerksamkeit.

Martin Koch ist freier Journalist. Dr. Axel Czarnetzki ist Rechtsanwalt und Partner der Heussen Rechtsanwaltsgesellschaft mbH in München.

Seite 1 | 2 | 3 | 4

Seite 1: Haftung inklusive
Seite 2: Rechtlich eindeutig und doch häufig hilflos
Seite 3: Straf- und zivilrechtliche Haftung

Artikel verschicken | Artikel drucken | E-Mail an Verfasser

News | Services & Lösungen | Trends & Technologien | Unternehmen & Märkte | Recht & Management | Marktforschung | SOA | Whitepaper
Events | Impressum | Kontakt | Mediadaten | Site Map | Mitarbeiter