HEUSSEN
Rechtsanwaltsgesellschaft mbH
Dr. Axel Czarnetzki LL.M.

Juristische Aspekte der IT-Security

HAFTUNGSRISIKEN DURCH HACKER-ANGRIFFE FÜR UNTERNEHMEN, DEREN FÜHRUNGSORGANE SOWIE MAßGEBLICHE MITARBEITER

Angriffe auf die IT-Umgebung von Unternehmen sind heute an der Tagesordnung. Mussten früher Geheimdienste mühsam Mitarbeiter einschleusen oder bestechen, um an Firmengeheimnisse heranzukommen oder Konkurrenten konkrete Sabotage betreiben, um ein Unternehmen im Wettbewerb zu schädigen, erfolgen heute derartige Angriffe bequem vom Schreibtisch aus. Geheimdienste, Hacker und auch einfach nur „Computer-Kids“ scheinen es als teilweise sportliche Aufgabe zu empfinden, Daten auszuspähen oder Unternehmen zu sabotieren, indem Daten zerstört, verändert oder einfach nur Viren eingeschleust werden. Häufig sind sich derartige Angreifer nicht einmal bewusst, dass sie sich strafbar machen und schadenersatzpflichtig sind.

Aber auch das Unternehmen selbst kann aus vielfachen Gründen einer Haftung unterliegen. Diese kann sich auf die Führung eines Unternehmens (**Geschäftsführer, Vorstände und Aufsichtsräte**) auswirken, wenn diese keine von einem sorgfältigen Kaufmann zu erwartenden Sicherungsvorkehrungen ergriffen haben. IT-Security ist daher **Chefsache** und ein ernst zu nehmendes Thema.

Dieser Beitrag soll die Risiken und Gefahren für Unternehmen darstellen und Auswege aus der Haftung aufzeigen.

I. Einleitung

Monatlich gibt es inzwischen Meldungen über Angriffe auf Firmendaten und Firmen-IT. Selbst Rechnersysteme von Staaten werden durch gezielte Angriffe sabotiert. Innerhalb weniger Stunden gelang es z.B. einem bislang noch Unbekannten, weltweit Millionen von Rechnersystemen lahmzulegen und Schäden in Höhe von mehreren Milliarden Dollar zu verursachen. Ein einfaches e-mail-Attachment, welches als „I love you-Virus“ in die Computergeschichte eingegangen ist, drang in die e-mail-Systeme der Rechner ein und vervielfältigte sich selbst über die Adressverzeichnisse der jeweiligen e-mail-Systeme der Rechner, welche von ihm befallen wurden.

Betroffen waren nicht nur einfache, ungeschützte Systeme. Weltweit wurden Firmen bis hin zur Größenordnung von Microsoft und Behörden bis hin zu Bundesbehörden und Ministerien von dem Virus befallen. In Deutschland mussten einige Ministerien noch Tage später bestätigen, dass ihre e-mail-Systeme noch immer nicht einwandfrei funktionierten.

Bot-Netze werden eingerichtet, um Milliarden von SPAM-Mails zu versenden, Rechner von Privaten und Unternehmen werden gekapert, ohne dass diese Kenntnis davon erlangen, dass ihre Systeme dazu verwendet werden, SPAM-Mails an Dritte zu versenden. Inzwischen machen SPAM-Mails nach den Statisti-

ken der Provider nahezu 70-80 % der gesamten E-Mail-Kommunikation aus. Aktuelle Veröffentlichungen zeigen, dass sich das SPAM-Aufkommen allein zwischen 2006 und 2007 schon heute (Stand 1.6.2007) verdoppelt hat, bis zum Jahresende kann es also das Vierfache erreicht haben.

Diese unter Umständen extrem kostenaufwendigen, jedoch ungezielten Angriffe sind hinsichtlich ihrer Langzeitwirkung nahezu vernachlässigbar im Verhältnis zu gezielten Angriffen von Hackern und Industriespionen, welche es konkret auf die Firmengeheimnisse, Forschungsergebnisse, Kunden- und Lieferantendatenbanken, Konditionen und andere wichtige Informationen abgesehen haben.

In einer Zeit, in der die e-mail als Kommunikationsmittel immer stärker verbreitet wird und selbst die juristischen Grundlagen für wirksame Vertragsschlüsse durch e-mail geschaffen werden, in der fast jeder Rechner Zugang zum Internet bietet und damit umgekehrt ein Einfallstor für externe Angriffe darstellt, kann ein Angriff nicht nur unmittelbare Schäden, sondern auch mittelbare Schäden dadurch auslösen, dass nicht nur Daten verloren gehen, sondern an Dritte übertragen werden, welche diese Daten nicht zur Kenntnis erhalten sollten.

Ebenso wie es bei einem „I love you-Virus“ nur eine Weiteleitung der jeweils selben mail war, hätte es auch ein Ausspähen von Daten des Unternehmens sein können, welche anschließend an eine bestimmte oder an beliebige Internet-Adressen weitergeleitet hätten werden können. Pishing und Trojaner bis hin zum Bundestrojaner sind inzwischen Begriffe, die jeder Computernutzer nicht nur kennt sondern fürchtet, vor wenigen Jahren hätte niemand diese Begriffe auch nur erläutern können.

Mit diesem Beitrag wollen wir Sie darüber informieren, welche zivil- und strafrechtlichen Risiken auf das Unternehmen selbst zukommen, wenn es sich nicht ausreichend vor Angriffen auf seine Daten und Informationen schützt. Hierbei spielt es keine Rolle, ob es sich um einen externen oder internen Angriff handelt. Auch soll dargestellt werden, welche Möglichkeiten das Unternehmen selbst hat, nach einem Angriff gegen den Angreifer vorzugehen.

II. Haftung des Angreifers für von ihm verursachte Schäden

Sofern der Angreifer identifiziert werden kann, sind die zivil- und strafrechtlichen Grundlagen für eine Haftung eindeutig definiert. Die §§ 303 a ff. StGB regeln die strafrechtliche Verantwortung eines Angreifers. Gemäß § 303 a StGB wird mit Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe bestraft, wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert. Gemäß § 303 b StGB wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft, wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, dass er entweder eine Straftat nach § 303 a StGB begeht oder eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert. In beiden Fällen ist bereits der Versuch der Straftat strafbar.

Soweit der Angriff darauf gerichtet ist, Daten eines Unternehmens zu beschaffen, finden die §§ 202 a ff. StGB Anwendung. Danach wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft, wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft. § 203 StGB hat den Schutz von Betriebs- oder Geschäftsgeheimnissen zum Inhalt. Die zivilrechtliche Haftungsnorm des Täters gegenüber dem Unternehmen ist § 823 II BGB i.V.m. den eben genannten Strafrahmen. § 823 BGB regelt die Schadenersatzpflicht eines deliktisch Handelnden. Wer vorsätzlich oder fahrlässig das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich ersetzt, ist diesem gegenüber zum Ersatz des daraus entstehenden Schadens verpflichtet. Während § 823 I BGB Vermögensschäden nicht erfasst, werden diese durch § 823 II BGB abgedeckt. Voraussetzung hierfür ist jedoch, dass ein besonderes sogenanntes Schutzgesetz verletzt wurde. Zu diesen zählen sämtliche strafrechtlich relevanten Normen.

Während in zivil- und strafrechtlicher Hinsicht die Haftung des Täters vergleichsweise einfach herzuleiten ist, ist in praktischer Hinsicht die Geltendmachung des Schadens häufig schwierig. Zunächst muss der Täter ermittelt werden, was im weltweiten Datennetz häufig auf erhebliche Probleme stößt. Sofern sich der

Täter im Ausland befindet, muss im Wege der internationalen Rechtshilfe versucht werden, den Täter in strafrechtlicher Hinsicht zur Verantwortung zu ziehen. Die unterschiedliche Rechtslage in verschiedenen Staaten erschwert den Zugriff auf den Täter hierbei erheblich. Selbst wenn es in zivil- und strafrechtlicher Hinsicht gelingt, den Täter zur Verantwortung zu ziehen, ist damit noch nicht sichergestellt, dass die von ihm verursachten Schäden von ihm ersetzt werden können. Auch können Langzeitschäden für ein Unternehmen so massiv sein, wenn z.B. Betriebsgeheimnisse an die Konkurrenz geraten und damit mühsam erkämpfte Wettbewerbspositionen verloren gehen, dass der Bestand des Unternehmens gefährdet ist, unabhängig davon, ob finanzieller Schadenersatz in angemessener Höhe erlangt werden kann.

Das Beispiel des „I love you-Virus“ zeigt, dass die Hoffnung auf den Ersatz des tatsächlich entstandenen Schadens häufig illusorisch ist. Kein Täter der Welt wäre in der Lage, die prognostizierten US$ 10 – 20 Milliarden, welche an Schäden entstanden sein sollen, zu ersetzen. In tatsächlicher Hinsicht verbleiben daher die Schäden meist beim Unternehmen. Schon aus diesem Grund ist ein effizienter Schutz vor Angriffen auf die eigenen Unternehmensdaten sowohl in technischer als auch organisatorischer Hinsicht zwingend erforderlich, um Schäden vom Unternehmen abzuwenden.

Neben den eigenen Schäden, welche dem Unternehmen direkt durch den Datenangriff entstehen können, verbleiben erhebliche weitere Risiken, welche gegenüber Kunden des Unternehmens und dessen Mitarbeitern bestehen. Nicht zuletzt verbleiben die Risiken der maßgeblichen verantwortlichen Mitarbeiter wie auch der Geschäftsführer, des Vorstandes und der Aufsichtsräte.

III. Haftung des Unternehmens gegenüber Dritten für etwaige Datenschäden

Die in einem Unternehmen vorhandenen Daten können aus verschiedenen Gründen heraus schutzbedürftig sein. Das eigene Interesse eines Unternehmens, dass seine Daten nicht Dritten zur Verfügung gestellt werden, kann wirtschaftliche oder gesetzliche Gründe haben. Wichtige Unternehmensdaten können Betriebsgeheimnisse sein. Diese vor Wettbewerbern oder sonstigen Dritten zu schützen, kann für ein Unternehmen von existentieller Bedeutung sein.

Daneben können jedoch auch zwingende gesetzliche Vorschriften, wie z. B. das Bundesdatenschutzgesetz, von einem Unternehmen verlangen, dass fremde Dritte keinen Zugriff auf die im Unternehmen vorhandenen schutzbedürftigen Daten erhalten. Verstöße gegen das Bundesdatenschutzgesetz können nicht nur die Verhängung von Bußgeldern bis zu € 250.000,--, sondern auch Freiheitsstrafen von bis zu zwei Jahren oder Geldstrafen zur Folge haben (§§ 43, 44 BDSG).

Hinzu kommt die Verantwortung und Haftung für Daten oder Anwendungen von Dritten, für die das Unternehmen die Verantwortung oder Betreuung übernommen hat. Insbesondere bei Internet-Providern, Application-Service-Providern oder anderen Unternehmen, welche fremde Daten verwalten, bestehen in aller Regel vertragliche Vereinbarungen gegenüber den Kunden, welche zu einer Haftung führen können, wenn die Daten der Kunden nicht ausreichend vor Zugriffen Dritter oder sonstiger Beeinflussung geschützt werden. Eine Haftung eines Application-Service-Providers kann bereits dann entstehen, wenn ein Zugriff auf die Daten des Kunden nicht erfolgt, sondern der Provider selbst seine Dienste nicht mehr erbringen kann, weil er z. B. durch einen Virenangriff seine Server nicht mehr betreiben kann und seine Kunden deren Geschäft im Internet nicht mehr betreiben können. Kann das Unternehmen seine vertraglich geschuldeten Leistungen nicht mehr erbringen, können Schadenersatzansprüche des Kunden entstehen. Inwieweit diese gegen das Unternehmen durchgreifen, hängt unter anderem von der vertraglichen Gestaltung des Vertrages mit dem Endkunden ab und kann daher in diesem Beitrag nicht abschließend erörtert werden. Zumindest in rechtlicher Hinsicht können jedoch unabsehbare Risiken entstehen, wenn das Unternehmen sich nicht ausreichend gegen externe Angriffe absichert.

IV. Interne Haftung innerhalb des Unternehmens für eingetretene Schäden

Nach außen gegenüber Dritten, wie z. B. dem Endkunden, haftet in aller Regel das Unternehmen, da gem. § 278 BGB das Unternehmen für fremdes Verschulden (seiner Mitarbei-

ter) ohne Rücksicht auf sein eigenes Verhalten haftet, sofern ein Vertragsverhältnis zwischen dem Unternehmen und dem Dritten besteht. Außerhalb eines solchen Vertragsverhältnisses findet § 831 BGB Anwendung, wonach ein Unternehmen auch für sogenannte Verrichtungsgehilfen haftet, wenn nicht nachgewiesen werden kann, dass das Unternehmen bei der Auswahl der Personen und, sofern es Vorrichtungen oder Gerätschaften zu beschaffen hatte, bei deren Beschaffung die im Verkehr erforderliche Sorgfalt beachtet hat. Dieser Entlastungsbeweis wird insbesondere dann schwierig sein, wenn ein Unternehmen keinen ausreichenden, dem Stand der Technik angemessenen Schutz vor fremden Zugriffen auf die eigenen Daten nachweisen kann.

Auch hier ist zu unterscheiden zwischen der zivil- und strafrechtlichen Haftung.

In strafrechtlicher Hinsicht wird z. B. der Geschäftsführer eines Unternehmens gem. § 14 I StGB grundsätzlich für Straftaten, die aufgrund von Entscheidungen der Unternehmensleitung begangen wurden, zur Verantwortung gezogen, sofern er eine konkrete Möglichkeit hatte, das Geschehen zu steuern. Dies gilt auch in solchen Fällen, wo eine Straftat durch Unterlassen begangen werden kann. In Betracht kommt daher auch eine strafrechtliche Zurechenbarkeit, wenn offensichtlich erforderliche Schutzmaßnahmen unterlassen wurden. § 14 StGB behandelt den Vertreter eines Unternehmens wie einen Straftäter, wenn ein Straftatbestand durch das Unternehmen begangen wurde.

In zivilrechtlicher Hinsicht haften Geschäftsführer gem. § 43 GmbHG und Vorstände gem. § 93 II AktG dem Unternehmen gegenüber, nicht jedoch gegenüber dem Kunden oder sonstigen Dritten. Sie haben dem Unternehmen gegenüber eine Vermögensbetreuungspflicht, bei deren Verletzung sie sich gem. §266 StGB strafbar machen. Diese Vermögensbetreuungspflicht verlangt, dass Geschäftsführer, Vorstände und Aufsichtsräte sämtliche erkennbar notwendigen Maßnahmen ergreifen, um Schäden vom Unternehmen abzuwenden.

IT-Security-Risiken sind **vorhersehbare Risiken**. Die Geschäftsleitung ist daher dafür verantwortlich, dass alles Notwendige und Angemessene getan wird, um Haftungsrisiken des Unternehmens abzuwenden. IT-Security ist daher nicht nur eine Aufgabe der Fachabteilungen, sondern **Chefsache**. Die Geschäftsleitung hat alle notwendigen Verhütungsmaßnahmen zu ergreifen und ein Berichtssystem aufzubauen, um im Ernstfall unverzüglich informiert zu werden sowie eine Notfallplanung aufzustellen, wie in diesem Fall zu reagieren ist.

Es ist daher letztlich im eigenen Interesse der Geschäftsleitung eines Unternehmens, IT-Security-Risiken zu minimieren und zu einem Thema der ständigen Überprüfung und Überwachung zu machen, um nicht nur Schäden vom Unternehmen, sondern auch eigene zivil- und strafrechtliche Risiken zu vermeiden.

V. Verlagerung von Risiken

In vielen Fällen werden ein Unternehmen und dessen Geschäftsleitung in fachlicher Hinsicht nicht in der Lage sein, die potentiellen Risiken zu beurteilen und die erforderlichen Maßnahmen zu deren Abwendung zu ergreifen. Diese Unternehmen laufen permanent Gefahr, zivil- und strafrechtlicher Haftung zu unterliegen.

Eine Haftungsverlagerung ist jedoch möglich. Die Gesetzgebung und die Gerichte erwarten nicht, dass ein Unternehmen und dessen Mitarbeiter alles Erforderliche in eigener Person leisten können. Es reicht aus, die notwendigen organisatorischen Maßnahmen zu ergreifen. Hierzu kann auch die **Verlagerung der Risiken auf einen Dritten** zählen, d. h. die Einschaltung eines geeigneten qualifizierten Unternehmens, welches die eigene IT-Security überprüft, auf dem laufenden hält und der Geschäftsführung gegenüber berichtet. Die Sorgfaltspflicht des Unternehmens richtet sich in diesem Fall darauf, ein geeignetes und seriöses Unternehmen zu finden und zu beauftragen sowie sicherzustellen, dass dessen Arbeit in das eigene Berichtssystem einbezogen wird. Hierbei können angesichts der nahezu täglich sich ändernden Risiken und Angriffspotentiale nur solche Unternehmen eingeschaltet werden, welche selbst ununterbrochen ihren Wissensstand erweitern und sich hinsichtlich der schnellen Entwicklungen im E-Business auf dem Laufenden halten.

Die Geschäftsführung eines Unternehmens hat so die Möglichkeit, sich selbst durch richtige Auswahl zu exkulpieren und ggf. Schäden vom Unternehmen abzuwenden. Zwar kann das

Unternehmen immer noch in zivil- und strafrechtlicher Hinsicht ein Fehlverhalten des hinzugezogenen Beratungsunternehmens zugerechnet werden (§§ 278, 831 BGB), zumindest jedoch hat das Unternehmen die Möglichkeit, etwaige Ansprüche auf das Beratungsunternehmen abzuwälzen. Natürlich ist in einem solchen Fall darauf zu achten, dass das Beratungsunternehmen entweder ausreichend versichert oder sonst ausreichend solvent ist, um einen etwa eintretenden Schaden auch tragen zu können.

In solchen Fällen gelten folgende Grundsätze:

- Wer einen Schaden selbst verursacht, muss für diesen Schaden auch selbst haften. Eigene Fehler oder eigenes Verschulden werden durch niemanden ersetzt.

- Berater haften für Fehler, welche im Rahmen des Beratungsverhältnisses oder Lieferantenverhältnisses gemacht werden. Eine Verlagerung der eigenen Haftung auf Berater oder Lieferanten kann daher sinnvoll sein.

- Verträge mit Lieferanten und Beratern müssen daher geeignete Haftungsvereinbarungen enthalten, wobei die Höhe von Versicherungen oder zur Verfügung stehendem Haftungsvermögen überprüft werden sollte.

VI. Zusammenfassung

Die Geltendmachung von Schadenersatzansprüchen gegen den Angreifer ist in zivil- und strafrechtlicher Hinsicht zwar vergleichsweise einfach, deren praktische Durchsetzung dürfte jedoch auf erhebliche Probleme stoßen.

Das Unternehmen selbst kann aus vielfachen Gründen einer Haftung unterliegen. Diese kann sich auf die Führung eines Unternehmens (Geschäftsführer, Vorstände und Aufsichtsräte) auswirken, wenn diese keine von einem sorgfältigen Kaufmann zu erwartenden Sicherungsvorkehrungen ergriffen haben. IT-Security ist daher Chefsache und ein ernst zu nehmendes Thema.

Die Verlagerung von Haftungsrisiken auf Dritte ist möglich, wenn sorgfältig geeignete Berater ausgewählt werden und deren fachliche Geeignetheit wie auch Bonität ausreichend überprüft werden.

Zur Vermeidung von Haftungsrisiken muss daher in jedem Unternehmen periodisch eine Risiko-Analyse vorgenommen und eine Anpassung der eigenen Absicherungsmaßnahmen gegen Angriffe Dritter an neue Bedürfnisse erfolgen. Eine Hinzuziehung fachkundiger Dritter kann in solchen Fällen Haftungs- und Risikoverlagerungseffekte mit sich bringen und ist daher zu empfehlen, sofern das Unternehmen selbst nicht über die notwendige Fachkompetenz verfügt, auftretende Risiken rechtzeitig zu erkennen und die notwendigen Sicherungsmaßnahmen umgehend zu ergreifen.

Für Rückfragen zu den in diesem Beitrag angesprochenen Themen steht Ihnen gerne zur Verfügung:

Rechtsanwalt Dr. Axel Czarnetzki LL.M.
Partner der Heussen Rechtsanwaltsgesellschaft mbH,
Brienner Straße 9 / Amiraplatz 1, 80333 München;
T: +49 89 29098-0 F: +49 89 29097200
www.heussen-law.de