Gen Re

April 2013

Cyber Liability – virtuell oder real?

von Björn Seitz und
Dr. Sven-Markus Thiel

Sonderdruck aus PHi 2/2013, S. 42 - 50

PHi | Haftpflicht international – Recht & Versicherung

Ein Unternehmen der Berkshire Hathaway Gruppe

Cyber Liability – virtuell oder real?

von Björn Seitz und Dr. Sven-Markus Thiel, Köln

Die Autoren sind Rechtsanwälte der auf Haftungs- und Versicherungsrecht spezialisierten Kanzlei BLD Bach Langheid Dallmayr Rechtsanwälte Partnerschaftsgesellschaft.
seitz@bld.de
thiel@bld.de

Schlagzeilen über Datendiebstahl, Datenverlust und Hacker-Angriffe auf die Datenbestände großer Unternehmen sind in der heutigen Zeitungswelt keine Ausnahme mehr. Als Alltagsphänomen wird man dieses Problemfeld sicherlich noch nicht bezeichnen müssen, wobei natürlich fraglich ist, ob überhaupt alle Fälle an die Öffentlichkeit dringen.[1] Aufsehen erregende Fälle der nahen Vergangenheit waren die Angriffe auf Sony mit ihrem Playstation-Network, Yahoo, LinkedIn, Nvidia, Adobe, Twitter und Evernote.[2] Nun haben diese Angriffe für die betroffenen Unternehmen nicht nur Reputationsschäden oder unzufriedene Kunden, sondern auch handfeste juristische Auseinandersetzungen zur Folge. Denn zumindest im Fall Sony sieht sich das Unternehmen diversen (Sammel-)Klagen von Nutzern des Playstation-Networks, aber auch von Kreditkartenunternehmen ausgesetzt. Allein in den USA geht man von mindestens 25 Klageverfahren vor US Federal Courts aus.[3] All diese Klagen richten sich auf Schadensersatz, es geht also um die Frage der Haftung von Sony für den Datenverlust – oder „Neudeutsch“ um cyber liability. Schon der Umstand, dass diese Klagen erhoben werden, zeigt, dass ein reales Risiko besteht, sich entsprechenden Ansprüchen ausgesetzt zu sehen. Es bleibt allerdings die Frage, ob die Ansprüche auch begründet sein können.

1 Einleitung

Die nachfolgende Darstellung beschäftigt sich daher mit der Frage, welche (begründeten) Haftungsszenarien für all die Unternehmen möglich sind, die elektronische Einrichtungen zum Speichern von Daten und/oder Internet-Technologien nutzen und dabei (zumindest fahrlässig) Schäden bei ihren (potenziellen) Geschäftspartnern oder bei Dritten anrichten. Die Haftung von IT-Dienstleistern, die sich bspw. auch nach den kauf- bzw. werkvertraglichen Gewährleistungsregeln (§§ 437 Nr. 3, 634 Nr. 4 BGB) richtet, soll dagegen außer Betracht bleiben. Gleiches gilt für die Haftung wegen vorsätzlicher Delikte gem. §§ 823, 826, 280 Abs. 1, 241 Abs. 2 BGB. Hier sind als Schutzgesetze, die i. V. m. § 823 Abs. 2 BGB zur zivilrechtlichen Haftung führen können, insbesondere die §§ 202 a), 202 b), 303 a), 303 b) StGB zu nennen.[4] Die genannten Vorschriften sind allerdings ausschließlich Vorsatztaten (§ 15 StGB), weshalb die fahrlässige Verwirklichung ihres objektiven Tatbestands keine unmittelbare deliktische Haftung gem. § 823 Abs. 2 BGB zu begründen vermag. Gleichwohl kann, wie sich zeigen wird, die fahrlässige Begehung oder Ermöglichung dieser Delikte haftungsbegründend wirken.

2 Fallkonstellationen

Die Möglichkeiten, den (potenziellen) Geschäftspartner oder einen Dritten bei der Nutzung des Internets zu schädigen, sind vielfältiger Natur. So nennt Spindler in seiner grundlegenden Studie[5] Viren,[6] Würmer,[7] Trojaner,[8] Spyware,[9] unsichere Konfiguration, webbasierte Dienste, Bot-Netze,[10] Ausnutzung von Sicherheitslücken, Input-Validierung und die gezielte Überlastung von Diensten (Denial-of-Service-Angriffe)[11].

Ein Beispiel bildet insoweit die Übermittlung virenbehafteter E-Mails durch den Nutzer der Internet-Technologien.[12] Soweit diese beim Empfänger zu einer Datenvernichtung, -unterdrückung, -unbrauchbarmachung oder -veränderung führt, sind zugleich die objektiven Voraussetzungen des § 303 a) Abs. 1 StGB erfüllt.

Ein weiteres plastisches Beispiel bildet die Ermöglichung des Zugriffs auf Kundendaten etwa im Fall des bereits erwähnten Datenlecks bei der Firma

Sony im April/Juni 2011.[13] In solchen Fällen kann nicht ausgeschlossen werden, dass die Hacker auch an sensible Daten, wie Kreditkarteninformationen, gelangen. Eine Sicherheitslücke beim Internetkonzern Yahoo führte jüngst dazu, dass Hacker über 450.000 Benutzernamen und Kennwörter entwenden und ins Internet stellen konnten.[14] Der „Diebstahl" (Ausspähen von Daten, § 202 a StGB) und ggf. anschließende Verkauf von Daten stellt eine Fallgruppe dar, die im Folgenden zu behandeln sein wird. Darüber hinaus besteht die Möglichkeit, dass Mitarbeiter eines Unternehmens aus dem Netzwerk heraus versehentlich aufgrund einer Fehlbedienung Dritten schaden, z. B. durch die ungewollte Herausgabe von Kundendaten oder die Verbreitung von Schadsoftware. Dies kann auch vorsätzlich geschehen, bspw. mittels einer distributed denial of service attack (DDoS), durch die Internet-Verbindungen der angegriffenen Unternehmen durch gezielte Überlastung lahm gelegt werden.[15] Schließlich besteht die Möglichkeit, dass Dritte den Internetzugang eines Unternehmens für unerlaubte Handlungen oder sogar Straftaten missbrauchen, indem z. B. über ein (nicht ausreichend gesichertes) WLAN ein unerlaubter Zugriff erlangt bzw. ermöglicht wird.[16]

3 Haftungsgrundlagen

Als Haftungsgrundlagen sind § 823 Abs. 1 BGB, § 280 Abs. 1 BGB, ggf. i. V. m. § 311 Abs. 2, § 241 Abs. 2 BGB sowie § 7 BDSG in Betracht zu ziehen. Diese Grundlagen werden im Folgenden dargestellt, setzen aber eine von dem IT-nutzenden Unternehmen zu vertretende Pflichtverletzung voraus, auf deren Voraussetzungen unter 4 eingegangen wird.

3.1 Haftung gem. § 823 Abs. 1 BGB (Leben, Körper, Gesundheit und Freiheit)

Zwar sind Softwarefehler nicht geeignet, unmittelbar Beeinträchtigungen an den personenbezogenen Rechtsgütern des § 823 Abs. 1 BGB zu bewirken. Im Schrifttum wird jedoch zu Recht darauf hingewiesen, dass mittelbare Beeinträchtigungen vorstellbar sind, wenn es z. B. aufgrund der Veränderungen von Daten zu Fehlfunktionen bei Geräten kommt, die die personenbezogenen Rechtsgüter schützen sollen.[17] Derartige mittelbare Rechtsgutverletzungen sind in der Praxis vermehrt denkbar, weil mittels Software gesteuerte Systeme immer mehr zur Anwendung gelangen, bspw. bei der Steuerung von industriellen Anlagen oder Robotern, bei der Flugsicherung oder Verkehrsleitsystemen sowie im medizinischen Bereich, wo Softwarefehler oder die Fehlbedienung von Geräten dazu führen können, dass Leben, Körper oder Gesundheit Dritter in Mitleidenschaft gezogen werden; auch die Verletzung der persönlichen Freiheit durch Ausfall mittels Software gesteuerter Fahrstühle oder Türen ist möglich.[18]

3.1.1 § 823 Abs. 1 BGB (Eigentum)

Als weitere Anspruchsgrundlage könnte § 823 Abs. 1 BGB auch insoweit Anwendung finden, als durch die Vorschrift das Rechtsgut Eigentum geschützt wird.

a) Hier ist allerdings eine Abgrenzung zu reinen Vermögensschäden vorzunehmen und es stellt sich die Frage, ob und inwieweit die Beeinträchtigung von Daten eine Eigentumsverletzung begründen kann, wenn damit keine Schädigung der Hardware einhergeht. Das Fehlen einer Substanzbeeinträchtigung spricht auf den ersten Blick gegen die Annahme einer Eigentumsverletzung. Nach der Rechtsprechung des BGH handelt es sich jedoch z. B. bei Standardsoftware um eine bewegliche Sache, denn nach dessen Ansicht ist es entscheidend, dass es sich um ein auf einem Datenträger verkörpertes Programm und damit um eine körperliche Sache i. S. des § 90 BGB handelt.[19] Dem ist im Ergebnis zuzustimmen. Selbst wenn der Datenträger in seiner körperlichen Substanz unversehrt bleibt, wenn die darauf befindlichen Daten gelöscht werden, so ist doch eine Eigentumsverletzung i. S. des § 823 Abs. 1 BGB gegeben, weil es sich bei der Löschung von Daten um eine Einwirkung auf die Sache handelt, die den Eigentümer daran hindert, mit ihr seinem Wunsch entsprechend (§ 903 BGB) zu verfahren.[20]

1 *Dies könnte sich aber bald ändern, da auf Ebene der EU an einem Gesetzentwurf für eine Meldepflicht gearbeitet wird. Danach müssen alle Datenverluste und -angriffe einer nationalen Cyber-Behörde gemeldet werden (http://www.zdnet.de/88140322/eu-gesetzentwurf-internetfirmen-mussen-datenverluste-melden/).*
2 *http://www.zdnet.de/themen/datendiebstahl/.*
3 *http://www.reuters.com/article/2011/05/12/us-sony-lawsuits-idUSTRE74B5IA20110512.*
4 *Für den Schutzgesetzcharakter dieser Vorschriften: Spindler, in: Beckmann/Matusche-Beckmann, Versicherungsrechts-Handbuch, 2. Aufl. 2009, § 40 Rn. 36.*
5 *Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, Studie im Auftrag des BSI 2007, (im Folgenden zitiert als Spindler, Studie), Rn. 58 ff., abrufbar im Internet unter https://www.bsi.bund.de/cae/servlet/contentblob/486890/publicationFile/30962/Gutachten_pdf.pdf.*
6 *http://de.wikipedia.org/wiki/Computervirus.*
7 *http://de.wikipedia.org/wiki/Computerwurm.*
8 *http://de.wikipedia.org/wiki/Trojanisches_Pferd_(Computerprogramm).*
9 *http://de.wikipedia.org/wiki/Spyware.*
10 *http://de.wikipedia.org/wiki/Bot-Netz.*
11 *http://de.wikipedia.org/wiki/Ddos.*
12 *Vgl. dazu grundlegend Koch, NJW 2004, 801 ff.*
13 *http://www.fr-online.de/digital/super-klau-bei-sony-datenleck-betrifft-millionen-deutsche,1472406,8382778.html; http://www.tagesschau.de/wirtschaft/sony124.html.*
14 *http://www.ftd.de/unternehmen/handel-dienstleister/:datendiebstahl-hacker-erbeuten-kundendaten-von-yahoo/70062813.html.*
15 *Vgl. beispielhaft den Fall LG Düsseldorf, Urt. v. 22.3.2011 – 3 KLs 1/11; zitiert nach juris.*
16 *Vgl. dazu BGH, NJW 2010, 2061 ff.*
17 *Koch, NJW 2004, 801, 802.*
18 *Spindler, Studie, Rn. 107.*
19 *BGH, NJW 1993, 2436, 2437 f.*
20 *OLG Karlsruhe, NJW 1996, 200, 201; vgl. auch OLG Oldenburg, Verfügung v. 3.11.2011 – 2 U 98/11; zitiert nach juris: Verkörperung des Datenbestands im Material; Wagner, in: Münchener Kommentar zum BGB, 5. Aufl. 2009, § 823 Rn. 103.*

Das dagegen vorgebrachte Argument, durch Stromausfall gelöschte Daten stellten kein Eigentum i. S. von § 823 Abs. 1 BGB dar, weil elektronische Daten sich lediglich im Arbeitsspeicher befinden oder auf einem Datenträger wie Diskette oder Festplatte gespeichert sind, aus elektrischen Spannungen bestehen und daher nicht dem sachenrechtlichen Sachenbegriff unterfallen,[21] ist nicht stichhaltig. Dabei wird nämlich verkannt, dass § 823 Abs. 1 BGB bereits die Funktionalität und innere Ordnung des Eigentums schützt,[22] weshalb bspw. eine Eigentumsstörung vorliegt, wenn Sachgesamtheiten, z. B. ein Archiv, in Mitleidenschaft gezogen werden, bei denen die Funktionsfähigkeit und damit der bestimmungsgemäße Gebrauchswert wesentlich auf der Vollständigkeit und systematischen Erfassung beruht.[23]

Dem lässt sich auch nicht entgegenhalten, dass nach § 453 Abs. 1 BGB die Vorschriften über den Kauf von Sachen auf den Kauf von Rechten und sonstigen Gegenständen entsprechende Anwendung finden und unter die sonstigen Gegenstände i. S. dieser Vorschrift auch die Computersoftware fällt.[24] Der Gesetzgeber verfolgte mit der Schaffung des § 453 Abs. 1 BGB die Absicht, hinsichtlich sonstiger Gegenstände der Rechtsprechung, die die Vorschriften des Kaufvertragsrechts anwandte, soweit sie passten, zu folgen, wobei er auch die Software im Blick hatte.[25] Dem kann jedoch gerade nicht entnommen werden, dass die Frage, ob das Eigentumsrecht i. S. des § 823 Abs. 1 BGB verletzt wurde, anders als zuvor zu beurteilen wäre.[26]

Dagegen wird man in Fällen, in denen der Ausfall des EDV-Systems zu Betriebsstörungen und Produktionsausfällen führt, nur ausnahmsweise, wenn das System z. B. langfristig nicht genutzt werden kann, von einer Eigentumsverletzung ausgehen können.[27]

b) Wendet man diese Grundsätze auf die eingangs gegebenen Fallbeispiele an, so folgt daraus Folgendes:

Die Übermittlung virenbehafteter E-Mails stellt, auch wenn sie sich nur dergestalt auswirkt, dass es zu einem Datenverlust beim Empfänger kommt, eine gem. § 823 Abs. 1 BGB relevante Eigentumsverletzung dar. Wird dagegen einem Angreifer der Zugriff auf Kundendaten ermöglicht, ohne dass diese gelöscht oder nicht mehr nutzbar gemacht werden, so liegt eine Beeinträchtigung der auf dem Datenträger verkörperten Daten nicht vor, so dass eine Haftung nach § 823 Abs. 1 BGB wegen Eingriffs in das Eigentum ausscheidet. Auch bei der versehentlichen Fehlbedienung durch eigene Mitarbeiter kommt es daher auf die Frage an, ob es durch die jeweilige Handlung tatsächlich zu einem Datenverlust (z. B. Versendung von Malware) oder nur zu einer ungewollten Weitergabe von Daten kommt (beim Dateninhaber bleiben die Daten weiterhin vorhanden), da je nachdem eine Eigentumsverletzung i. S. von § 823 Abs. 1 BGB angenommen werden kann oder nicht. Sofern Mitarbeiter aus dem Netzwerk heraus die DDoS-Angriffe starten, hängt es davon ab, mit welcher Intensität, insbesondere in welchem zeitlichen Umfang, der Adressat solcher Angriffe auf ein funktionsfähiges Computersystem verzichten muss. In den Fällen des Datendiebstahls und -verkaufs kommt es darauf an, ob die Daten lediglich kopiert worden sind (dann liegt keine Haftung aus § 823 Abs. 1 BGB wegen Eigentumsstörung vor) oder ob die Daten zugleich von der Festplatte des berechtigten Dateninhabers entfernt worden sind (dann ist eine solche Haftung nach § 823 Abs. 1 BGB in Betracht zu ziehen). Sofern der WLAN-Zugang durch Unbefugte missbraucht wird, wird man in der Regel keine Eigentumsverletzung annehmen können, da die verkörperten Daten davon unberührt bleiben.

3.1.2 § 823 Abs. 1 BGB (Gewerbebetrieb)

Für den Fall, dass die Sachqualität der verkörperten Daten und damit ein Eingriff in das Eigentum gem. § 823 Abs. 1 BGB verneint wird, wird im Schrifttum vertreten, dass eine Verletzung des Auffangrechts am eingerichteten und ausgeübten Gewerbetrieb anzunehmen ist.[28] Das Recht am eingerichteten und ausgeübten Gewerbebetrieb umfasst insbesondere auch die betriebsbezogenen gespeicherten Daten.[29]

21 LG Konstanz, NJW 1996, 2662.
22 Spindler, Studie, Rn. 110.
23 BGH, NJW 1980, 1518, 1519.
24 So Faust, in: Bamberger/Roth, BeckOK BGB, Stand 1.3.2011, § 453 Rn. 23; vgl. auch Palandt/Weidenkaff, BGB, 72. Aufl. 2013, § 453 Rn. 8, wonach Software zumindest ein sonstiger Gegenstand ist.
25 DTDrs. 14/6040, S. 242.
26 So auch Koch, NJW 2004, 801, 802 f.
27 Spindler, Studie, Rn. 113.
28 Koch, NJW 2004, 801, 803.
29 Palandt/Sprau, BGB, 72. Aufl. 2013, § 823 Rn. 127.

Demgegenüber wird freilich auch vertreten, dass es regelmäßig am erforderlichen betriebsbezogenen, finalen Eingriff fehlen wird.[30] Die Betriebsbezogenheit ist zu bejahen, wenn sich der Eingriff gegen den Betrieb als solchen richtet und nicht lediglich vom Gewerbebetrieb ablösbare Rechtspositionen beeinträchtigt; ist das Unternehmen bloß mittelbar betroffen, ist die Betriebsbezogenheit zu verneinen.[31] So hat das Landgericht Konstanz in dem durch einen Stromausfall aufgrund der Leitungsbeschädigung bei Baggerarbeiten ausgelösten Datenverlust zutreffend lediglich einen mittelbaren Schaden gesehen, der von § 823 Abs. 1 BGB nicht mehr umfasst ist.[32]

Im Übrigen wird man hier nach den Fallgruppen differenzieren müssen. So ist bei der Übermittlung virenbehafteter E-Mails davon auszugehen, dass das Merkmal der Betriebsbezogenheit gegeben ist, weil der Virenschreiber in der Regel vorsätzlich handelt.[33] Sofern ein Unternehmen es Dritten ermöglicht, Zugriff auf die Kundendaten zu nehmen, wird man dagegen eher nicht von einem betriebsbezogenen Eingriff ausgehen können, da es sich lediglich um eine mittelbare Rechtsgutverletzung handelt. Beruht die Schädigung Dritter auf dem Versehen eines Mitarbeiters, wird man die Betriebsbezogenheit eher verneinen können. Dagegen ist die Schädigung eines anderen Unternehmens durch Mitarbeiter, die DDoS-Attacken starten, genauso zu beurteilen wie die Versendung (bewusst) virenbehafteter E-Mails. In den Fällen von Datendiebstahl und -verkauf wird man einen zielgerichteten unmittelbaren Eingriff bejahen können. Denn in diesen Fällen richtet sich die Aktion desjenigen, der den Gewerbebetrieb beeinträchtigt, unmittelbar und zielgerichtet auf den geschädigten Betrieb. Gleiches gilt für den Missbrauch von Internetzugängen, etwa in den Fällen des WLAN-Missbrauchs, weil dadurch gezielt Schäden bei Drittunternehmen hervorgerufen werden.

3.1.3 § 823 Abs. 1 BGB (Allgemeines Persönlichkeitsrecht)

In Erwägung zu ziehen ist ferner, dass der Nutzer der Internettechnologie wegen der Beeinträchtigung des allgemeinen Persönlichkeitsrechts des Gegners haftet, § 823 Abs.1 BGB.[34] Man wird hier zu unterscheiden haben zwischen persönlichen Daten von Kunden, die das IT-nutzende Unternehmen gespeichert hat und Betriebsgeheimnissen anderer Unternehmen, deren Schutz durch das Recht auf den eingerichteten ausgeübten Gewerbebetrieb gewährleistet werden sollte.

3.1.4 § 823 Abs. 1 BGB (Recht auf die eigenen Daten)

Streitig ist, ob auch ein Recht am eigenen Datenbestand als sonstiges Recht i. S. des § 823 Abs. 1 BGB anzuerkennen ist.[35] Dafür spricht, dass es nicht gerechtfertigt ist, den deliktischen Schutz des Geschädigten davon abhängig zu machen, dass die beschädigten oder zerstörten Daten zufälligerweise verkörpert sind oder nicht.[36] Allerdings wird dadurch die Grenze zur Erfassung deliktisch nicht geschützter Vermögensschäden verschoben.[37]

3.2 § 280 Abs. 1 BGB (Schutzpflichten)

§ 280 Abs. 1 BGB sanktioniert auch die Verletzung von Schutzpflichten, die vertragliche (oder vorvertragliche – § 311 Abs. 2 i. V. m. § 241 Abs. 2 BGB) Nebenpflichten sind. Es ist anerkannt, dass der Schuldner die Pflicht hat, sich bei der Abwicklung des Schuldverhältnisses so zu verhalten, dass Körper, Leben, Eigentum und sonstige Rechtsgüter des anderen Teils nicht verletzt werden.[38] Im Rahmen der (vor-)vertraglichen Beziehung kommen insoweit die Rechtsgüter in Betracht, die zuvor im Rahmen des § 823 Abs. 1 BGB erörtert worden sind. Die Verletzung von Schutzpflichten gem. § 280 Abs. 1 BGB ist daher auch als Haftungsgrundlage in Betracht zu ziehen. Zu den Schutzpflichten i. S. des § 280 Abs. 1 BGB gehören auch die Verkehrssicherungspflichten, die insoweit als vertragliche Pflichten zu qualifizieren sind.[39]

Für den Geschäftspartner des Unternehmens bzw. den im vorvertraglichen Bereich angesprochenen Haftungsgegner ist die Verletzung der Schutzpflicht gem. § 280 Abs. 1 BGB insofern vorteilhaft, als auch das Vermögen des

30 *Spindler, Studie, Rn. 108.*
31 *Wagner, a. a. O. (Fn. 20), § 823 Rn. 194.*
32 *LG Konstanz, NJW 1996, 2662; a. A. Geuer/Seidl, jurisPR-ITR 8/2012 Anm. 6, bezogen auf die Eigentumsverletzung.*
33 *Koch, NJW 2004, 801, 803.*
34 *Ebenda.*
35 *Dafür Meier/Wehlau, NJW 1998, 1585, 1588 f.; Spindler, in: Bamberger/Roth, BeckOK BGB, Stand 1.2.2013, § 823 Rn. 93.*
36 *Spindler, ebenda, § 823 Rn. 93.*
37 *Krit. auch Wagner, a. a. O. (Fn. 20), § 823 Rn. 103: Ein „Recht am eigenen Datenbestand" ließe sich kaum inhaltlich fixieren und in seinem Schutzbereich definieren.*
38 *Palandt/Grüneberg, BGB, 72. Auflage 2013, § 280 Rn. 28.*
39 *Vgl. Palandt/Grüneberg, ebenda.*

Geschädigten durch § 280 Abs. 1 BGB geschützt wird.[40] Sofern man also eine Schutz-/Verkehrssicherungspflicht zu bejahen hat, kommt die Haftung des IT-Nutzers in sämtlichen unter Punkt 3 dargestellten Fallgruppen grundsätzlich in Betracht.

3.3 § 7 BDSG

Als weitere Anspruchsgrundlage ist § 7 BDSG in Betracht zu ziehen. Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger nach dieser Gesetzesvorschrift dem Betroffenen zum Schadensersatz verpflichtet, wobei die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falls gebotene Sorgfalt beachtet hat.

In dieser Vorschrift ist eine verschuldensabhängige Haftungsgrundlage zu sehen, wobei § 7 Satz 2 BDSG bezüglich des Verschuldens eine Umkehr der Beweislast anordnet, wenn mit den Daten rechtswidrig umgegangen wurde.[41] Die Verarbeitung von Daten umfasst auch das Speichern personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung (§ 3 Abs. 4 Satz 2 Nr. 1 BDSG). Zu beachten ist, dass nur der Betroffene, nicht aber eine juristische Person anspruchsberechtigt ist.[42]

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben gem. § 9 BDSG 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, wobei nur Maßnahmen erforderlich sind, wenn ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht. In der Anlage zu § 9 Satz BDSG sind die organisatorischen Anforderungen niedergelegt, wobei aus Nr. 3 und 4 die Pflicht abgeleitet werden kann, ein Antivirenprogramm einzurichten.[43]

Die Verletzung der Pflicht muss zu einem Schaden führen. Ersatzfähig sind Vermögensschäden, wobei öffentliche und nicht öffentliche Stellen bei schwerwiegenden Verletzungen des Persönlichkeitsrechts auch ein Schmerzensgeld schulden können. Dies folgt für die öffentlichen Stellen unmittelbar aus § 8 Abs. 2 BDSG und für die nicht öffentlichen Stellen aus einer analogen Anwendung des § 847 BGB bzw. aus § 823 Abs. 1 BGB i. V. m. Art. 1 und 2 Abs. 1 GG.[44]

4 Verkehrssicherungspflicht

4.1 Grundlagen

Eine Haftung gem. § 823 Abs. 1 BGB setzt voraus, dass sich das Unternehmen bei der Schädigung des Dritten (zumindest) fahrlässig verhalten hat. Fahrlässig handelt gem. § 276 Abs. 2 BGB, wer die im Verkehr erforderliche Sorgfalt außer Acht lässt. In der Bestimmung der erforderlichen Sorgfalt liegt die Bedeutung der Verkehrssicherungspflichten. Denn eine Verkehrssicherungspflichtverletzung ist mit der Außerachtlassung der im Verkehr erforderlichen Sorgfalt i. S. des § 276 Abs. 2 BGB gleichzusetzen.[45]

Allgemein gilt der Grundsatz, dass derjenige, der eine Gefahrenlage schafft, verpflichtet ist, die notwendigen und zumutbaren Vorkehrungen zu treffen, um eine Schädigung anderer möglichst zu verhindern; die rechtlich gebotene Verkehrssicherung umfasst danach diejenigen Maßnahmen, die ein umsichtiger und verständiger, in vernünftigen Grenzen vorsichtiger Mensch für notwendig und ausreichend hält, um andere vor Schäden zu bewahren. Voraussetzung ist daher, dass sich vorausschauend für ein sachkundiges Urteil die naheliegende Gefahr ergibt, dass Rechtsgüter anderer verletzt werden können.[46] Allerdings muss nicht für alle denkbaren Möglichkeiten eines Schadenseintritts Vorsorge getroffen werden, sondern es sind nur die Vorkehrungen zu treffen, die geeignet sind, die Schädigung anderer tunlichst abzuwenden, weshalb der im Verkehr erforderlichen Sorg-

40 *Ebenda, § 280 Rn. 28 a.*
41 *Gola/Schomerus, BDSG, 11. Aufl. 2012, § 7 Rn. 9.*
42 *Ebenda, § 7 Rn. 6.*
43 *Koch, NJW 2004, 801, 805.*
44 *Gola/Schomerus, a. a. O. (Fn. 41), § 7 Rn. 12 f., 19; BGH VersR 1996, 339.*
45 *Wagner, a. a. O. (Fn. 20), § 823 Rn. 64.*
46 *BGH, NJW 2004, 1449, 1450.*

falt gem. § 276 Abs. 2 BGB genügt ist, wenn im Ergebnis derjenige Sicherheitsgrad erreicht ist, den die im entsprechenden Bereich herrschende Verkehrsauffassung für erforderlich hält. Es reicht aus, diejenigen Sicherheitsvorkehrungen zu treffen, die ein verständiger, umsichtiger, vorsichtiger und gewissenhafter Angehöriger der betroffenen Verkehrskreise für ausreichend halten darf, um andere Personen vor Schäden zu bewahren, und die ihm den Umständen nach zuzumuten sind.[47]

4.2 Anwendung auf IT-nutzende Unternehmen

Diese Kriterien sind auch im Bereich der IT-Nutzung für die Frage maßgeblich, welche Pflichten den IT-Nutzer treffen, damit er die im Verkehr erforderliche Sorgfalt einhält.

a) Bei einem Unternehmen, das die Internettechnologien nutzt, handelt es sich um den Beherrscher einer Gefahrenquelle, so dass grundsätzlich vom Bestehen einer Verkehrssicherungspflicht auszugehen ist.[48] Gleichwohl ist fraglich, ob eine Verkehrssicherungspflicht besteht, weil nicht nur vom Versender, sondern auch vom Empfänger der E-Mail Sicherungsmaßnahmen zu treffen sind.

Allerdings sind Verletzungen einer den Geschädigten treffenden Verkehrssicherungspflicht grundsätzlich beim Mitverschulden gem. § 254 BGB zu berücksichtigen.[49] Im Bereich der IT-Nutzung ließe sich argumentieren, dass jeder Verkehrsteilnehmer selbst dafür verantwortlich ist, ein Anti-Virus-Programm und eine Firewall zu installieren und auf dem aktuellen Stand zu halten. Es wäre dann das allgemeine Lebensrisiko, wenn der Empfänger der E-Mail, die mit einem Virus behaftet ist, Schäden an seinen Rechtsgütern erleidet. Dieser Auffassung ist jedoch entgegenzuhalten, dass den Versender der E-Mail ebenfalls die Verpflichtung trifft, entsprechende Schutzmaßnahmen zu treffen. Dennoch gelangt Koch[50] zu dem Resultat, dass lediglich für Unternehmen im Verhältnis zu privaten Empfängern eine Verkehrssicherungspflicht zum Virenschutz besteht, während im Verhältnis von Unternehmern oder Privaten untereinander oder im Verhältnis vom sendenden Privaten zum empfangenden Unternehmen keine Verkehrssicherungspflicht bestehe. Dies begründet Koch damit, dass Unternehmer die Kommunikation per E-Mail weitaus intensiver als Private nutzen und durch den Einsatz des Mediums erhebliche betriebswirtschaftliche Vorteile erlangen, wobei sie bewusst das Risiko in Kauf nehmen, Opfer einer Virusattacke zu werden und zur Weiterverbreitung von Viren beizutragen. Dem ist jedoch entgegenzuhalten, dass die Schädigung eines IT-nutzenden Unternehmens durch ein anderes Unternehmen nicht das allgemeine Lebensrisiko betrifft, sondern als wesentliche Einschränkung und Verletzung der allgemeinen Rechtssphäre empfunden wird.[51] Insofern kann dahinstehen, was zu gelten hat, wenn ein Privater virenverseuchte E-Mails versendet. Jedenfalls bei Unternehmen sollte es bei der Anwendung des § 254 BGB bleiben, die zudem gerechtere Abwägungsergebnisse ermöglicht, als dies bei jeglicher Ablehnung einer Haftung des versendenden Unternehmens im Verhältnis zu dem empfangenden Unternehmen der Fall wäre.

Allerdings ist nicht unumstritten, ob den Empfänger von virenverseuchten E-Mails eine Pflicht zum Einsatz eines Virenschutzes trifft. Der BGH hat in einem Fall, in dem der Internetbenutzer keine Vorkehrungen gegen einen heimlich installierten Dialer getroffen hat, der ohne weiteres Zutun kostenpflichtige Verbindungen aufbaute, dem Telekommunikationsunternehmen das Risiko zugewiesen, dass unbemerkt Verbindungen durch heimliche Manipulationen Dritter an den Daten des Endgeräts entstehen.[52] Daraus wird in der Literatur der Schluss gezogen, der BGH wende sich generell gegen eine Obliegenheit, Schutzprogramme zu verwenden.[53] Dem ist jedoch entgegenzuhalten, dass der BGH das Risiko dem Anschlusskunden nur dann nicht auferlegt, soweit der Kunde die unbemerkte Herstellung von Verbindungen nicht zu vertreten hat. Das eröffnet die Möglichkeit, Versäumnisse des Empfängers von virenbehafteten E-Mails im Rahmen des Mitverschuldens zu berücksichtigen. Das Landgericht Stralsund hat die

47 BGH, NJW 2006, 2326, wo zwischen einem Unglück und dem Unrecht unterschieden wird.
48 So auch Mantz, K&R 2007, 567; vgl. auch Koch, NJW 2004, 801, 803, der danach differenziert, ob es sich um „Massenmail"-Würmer handelt (dann Beherrschung einer Gefahrenquelle) oder um die vom Versender veranlasste Übertragung der E-Mail (dann Schaffung einer besonderen Gefahrenlage aus vorrangegangenem Tun).
49 Unberath, in: Bamberger/Roth, BeckOK BGB, Stand 1.3.2011, § 254 Rn. 23.
50 NJW 2004, 801, 804 - 806.
51 Näher Mantz, K&R 2007, 566, 570 f.
52 BGH, NJW 2004, 1590, 1591.
53 Borges, MMR 2008, 262, 264.

Rechtsprechung des BGH zwar auf den Fall der Existenz eines sog. back-door-Trojaners auf der Festplatte des für Internetzwecke genutzten Rechners übertragen.[54] Danach oblag es dem dortigen Beklagten nicht, seinen Rechner gegen den Sperrvirus zu schützen. Diese im Bereich der Risikozuweisung bei Telekommunikationsdienstleistungen ergangene Rechtsprechung lässt sich aber nicht auf den hier zu erörternden Fall der Versendung und des Empfangs virenbefallener E-Mails übertragen. Es besteht außerdem keine Veranlassung, denjenigen Empfänger, der mögliche und zumutbare Sicherheitsvorkehrungen unterlassen hat, haftungsrechtlich zu begünstigen.

b) Entscheidend ist nach allem, dass der Versender virusbehafteter E-Mails im Stande ist, erforderliche und zumutbare Sicherheitsvorkehrungen gegen den Befall von Rechnern durch Schadprogramme zu treffen.[55]

Die Frage, wann eine Pflicht zur Ergreifung von Sicherungsmaßnahmen besteht, ist im Einzelnen danach zu beantworten, dass entsprechende Sicherungsmaßnahmen zur Verfügung stehen und auch bekannt sind. Es ist eine Zumutbarkeitsprüfung anzustellen, in die folgende Parameter eingehen:[56] Zunächst einmal muss das Sicherheitsproblem bekannt sein, d. h., es kommt darauf an, ob ein verständiger objektiver Nutzer von einer entsprechenden Gefahr wusste oder zumindest damit rechnen musste. Des Weiteren ist zu berücksichtigen, dass auch die Sicherungs- bzw. Gegenmaßnahmen aus Sicht eines objektiven verständigen Nutzers bekannt waren oder hätten bekannt sein müssen. Darüber hinaus müssen die zu ergreifenden Maßnahmen für das Unternehmen auch wirtschaftlich zumutbar sein, was der Fall ist, wenn sie nicht außerhalb eines angemessenen Verhältnisses stehen, wobei auch das Eigeninteresse des Unternehmens zu berücksichtigen ist.[57]

Dabei ist der Einsatz der folgenden Sicherungsmaßnahmen zu diskutieren:[58] Danach besteht eine Pflicht zum Einsatz von Virenscannern und Firewalls. Das Einspielen von System- und Programmupdates ist differenzierter zu betrachten. Die Nutzung von Nutzerkonten mit eingeschränkten Rechten und die Erstellung eines Administratorkontos sind sinnvoll, sofern nicht in sehr kleinen Unternehmen die Nutzer auch die Pflege der IT-Infrastruktur übernehmen. Die Verwendung von Intrusion detection-Systemen wird man nur großen Unternehmen abverlangen können. Der regelmäßige Einsatz von Malware-Entfernungsprogrammen alle zwei bis vier Wochen kann den Unternehmen zugemutet werden, zumal diese Programme häufig kostenlos verfügbar sind.

Demzufolge lässt sich als Teil der Verkehrssicherungspflicht der Anwender eine Verpflichtung zur Virenvorsorge bejahen.[59] Insofern genügt es nicht, ein Anti-Viren-Programm und eine Firewall zu installieren, sondern einmal installierte Virenscanner sind regelmäßig auf neue Viren einzustellen und Sicherheitslücken mit Updates von Software zu schließen.[60] Streitig ist, wie häufig ein Update durchzuführen ist. Hier reicht die Bandbreite der Meinungen von monatlichen Updates bis hin sogar zu stündlichen Aktualisierungen.[61] Richtig dürfte es sein, den Unternehmen abzuverlangen, dass sie ihren Virenschutz täglich aktualisieren. Dies ist auch technisch machbar und gehört zum Standardumfang professioneller Virenschutzprogramme.

Den Beherrscher einer Gefahrenquelle treffen die Verkehrssicherungspflichten grundsätzlich auch dann, wenn erfahrungsgemäß mit einem Fehlverhalten Dritter zu rechnen ist.[62] Die vorgenannten Überlegungen gelten daher auch für die Ermöglichung des Zugriffs auf Kundendaten, für die Ermöglichung von Datendiebstahl und -verkauf. Hier besteht wertungsmäßig kein Unterschied zur Übermittlung virenbehafteter E-Mails. Die erkennbaren, erforderlichen und zumutbaren Sicherheitsvorkehrungen müssen getroffen werden. Diese bestehen im ersten Schritt natürlich darin, dass schon der Zugriff von Dritten auf die gespeicherten Kundendaten durch Firewall und weitere Zugriffsbeschränkungen vermieden wird. Darüber hinaus kann es aber auch erforderlich sein, dass man die Kundendaten für den Fall eines unerlaubten Zugriffs auch noch dadurch

54 *LG Stralsund, MMR 2006, 487, 488 f.; aufgehoben durch BGH, NJW-RR 2007, 357.*
55 *Vgl. Koch, CR 2009, 485, 487.*
56 *Vgl. zum Folgenden eingehend Mantz, K&R 2007, 566, 568 - 570.*
57 *Während also bei Unternehmen die wirtschaftliche Zumutbarkeit zur technischen Behebung des Problems maßgeblich ist, soll es bei privaten IT-Nutzern darauf ankommen, ob sie eine technisch zumutbare Lösung ergreifen können.*
58 *Vgl. Spindler, Studie, Rn. 384 ff.*
59 *Koch, CR 2009, 485, 488.*
60 *Mantz, K&R 2007, 566, 570; Koch, CR 2009, 485, 488.*
61 *Koch, ebenda, 489 f.*
62 *Spindler, Studie, Rn. 119.*

schützt, dass diese lediglich in verschlüsselter Form beim Unternehmen gespeichert werden. Dies ist zumindest für die gespeicherten Passwörter der Kundenaccounts als durchaus üblich anzusehen.

Deshalb müssen Unternehmen den Missbrauch von Internetzugängen oder unterhaltenen WLAN-Netzen bei den Sicherungsmaßnahmen mit einkalkulieren. Die Maßstäbe, die daran angelegt werden müssen, sind sicherlich strenger als bei Privatpersonen.[63] Dem Unternehmen ist es zuzumuten, nicht nur die beim Erwerb der entsprechenden Hardware (z. B. WLAN-Router) verfügbaren Sicherheitsmechanismen zu installieren, sondern auch diese regelmäßig zu aktualisieren. Andernfalls haftet es ggf. gem. § 823 Abs. 1 BGB.

Das Fehlverhalten seiner Mitarbeiter muss sich das Unternehmen im Verhältnis zu Dritten zurechnen lassen. Dieser Bereich ist sehr schwierig zu kontrollieren, sinnvoll ist es insoweit, bei der Auswahl der Mitarbeiter viel Wert auf deren Integrität zu legen und unternehmensinterne Richtlinien aufzustellen, wobei auch solche Maßnahmen versehentliche Falschbedienungen nicht vollkommen ausschließen können.

Darüber hinaus wird im Schrifttum vertreten, dass der Anwender, der feststellt, dass er trotz aktueller Anti-Viren-Software von Schadprogrammen überflutet wird und die Weiterverbreitung an Dritte über das Internet nicht ausschließen kann, im Einzelfall zum zumindest temporären Dekonnektieren des Rechners oder zum Blockieren der Rechnerausgänge, über die Schadprogramme an Dritte übertragen werden können, verpflichtet ist.[64]

4.3 Schutzpflichten gem. § 280 Abs. 1 BGB

Wie bereits erwähnt, impliziert die Verletzung einer Verkehrssicherungspflicht im (vor-)vertraglichen Bereich zugleich die Verletzung der Schutzpflicht gem. § 280 Abs. 1 BGB. Als ein Beispiel für einen „ähnlichen geschäftlichen Kontakt“ i. S. des § 311 Abs. 2 Nr. 3 BGB kann insoweit der Versand von Werbe-E-Mails angesehen werden.[65]

5 Sonstige tatbestandliche Voraussetzungen und Einwendungen

Mit dem Verstoß gegen die Verkehrssicherungspflicht bzw. Schutzpflicht ist die Pflichtwidrigkeit festgestellt. Hinzutreten müssen das Verschulden, die Kausalität und der Schaden.

a) Dabei ist zu beachten, dass das Verschulden gem. § 280 Abs. 1 Satz 2 BGB, § 7 Satz 2 BDSG vermutet wird. Das Unternehmen, das sich der IT bedient, muss also den Entlastungsbeweis führen. Doch auch hinsichtlich Verletzung einer Verkehrssicherungspflicht im Rahmen des § 823 Abs. 1 BGB gilt im Ergebnis nichts anderes. Der objektive Pflichtverstoß indiziert nämlich die Verletzung der inneren Sorgfaltspflicht oder führt zu einem Anscheinsbeweis, den der Schädiger entkräften muss.[66]

Das Landgericht Köln hat in einem Fall, in dem eine virenbehaftete fremde Diskette verwendet wurde, die Haftung aus § 823 BGB mit der Begründung verneint, dass seitens des Klägers nicht dargelegt worden ist, dass bei der Installation einer Firewall als Virenschutz der fragliche Virus überhaupt entdeckt worden wäre und die Nicht-Installation eine Firewall insoweit nicht als ursächlich für den eingetretenen Schaden angesehen.[67] Teilweise wird die Verteidigung mit dem Argument, ein Virus habe wegen seiner Neuartigkeit auch bei entsprechendem Antiviren-Programm oder Update nicht erkannt werden können, als Einwand des rechtmäßigen Alternativverhaltens qualifiziert.[68] Dem ist zuzustimmen, weil es darum geht, dass auch der Einsatz eines aktuellen Virusprogramms den Schaden nicht verhindert hätte. Dagegen ist bereits das Vertretenmüssen zu verneinen, wenn ein Programm installiert und aktualisiert ist, die Schutzlücken aber unvermeidbar sind.[69]

b) Bei der Bemessung von Schäden kann es zu praktischen Schwierigkeiten kommen. So wird zu Recht darauf hingewiesen, dass finanzielle Verluste durch den „Diebstahl“ von Kundendaten oftmals schwer zu beziffern sein werden.[70] Dem Geschädigten kommt hier die Vorschrift des § 287 ZPO zugute, die für das Beweismaß und

63 Dagegen scheidet ein Schadensersatzanspruch gegen den privaten Inhaber eines WLAN-Anschlusses, der nicht ausreichend gesichert ist, aus, weil die WLAN-Nutzung im Privatbereich auch mit unangemessenen Haftungsrisiken belastet würde, wenn der Anschlussinhaber bei Annahme einer täterschaftlichen Verantwortung unbegrenzt auf Schadensersatz haften würde, wenn außenstehende Dritte seinen Anschluss in für ihn nicht vorhersehbarer Weise für Rechtsverletzungen im Internet nutzen. Gleichwohl hat der BGH einen Unterlassungsanspruch des Geschädigten bejaht, weil der Inhaber des WLAN-Anschlusses im Kaufzeitpunkt des Routers die für den privaten Bereich marktüblichen Sicherungen ihrem Zweck entsprechend wirksam einzusetzen hatte (BGH, NJW 2010, 2061, 2062).
64 Koch, CR 2009, 485, 490.
65 Koch, NJW 2004, 801, 806.
66 Palandt/Sprau, a. a. O. (Fn. 29), § 823 Rn. 54.
67 LG Köln, NJW 1999, 3206.
68 Koch, NJW 2004, 801, 806.
69 Koch, ebenda, 807; Koch, CR 2009, 485, 490.
70 Spindler, in: Beckmann/Matusche-Beckmann, Versicherungsrechts-Handbuch, 2. Aufl. 2009, § 40 Rn. 19.

das Beweisverfahren Erleichterungen schafft. Eine Schätzung nach § 287 ZPO darf allerdings nur vorgenommen werden, wenn und soweit die festgestellten Umstände hierfür eine genügende Grundlage abgeben; sie hat zu unterbleiben, wenn greifbare Anhaltspunkte fehlen.[71] Solche konkreten Anhaltspunkte wären z. B. dann gegeben, wenn aufgrund des Datendiebstahls eine signifikante Anzahl von Kunden das betroffene Unternehmen verlässt.

c) Es wurde bereits dargelegt, dass die Geschädigten ggf. ein Mitverschulden gem. § 254 BGB trifft, sofern sie ihrerseits die ihnen zumutbaren Sicherheitsvorkehrungen nicht getroffen haben. Hier ist die Darlegungs- und Beweislast verteilt. Die Darlegungs- und Beweislast für die zur Anwendung des § 254 BGB führenden Umstände trägt grundsätzlich der Schädiger, weil er damit seine Ersatzpflicht mindern oder beseitigen will. Dabei darf dem Schädiger allerdings nichts Unmögliches angesonnen werden, sondern er kann beanspruchen, dass der Geschädigte an der Beweisführung mitwirkt, soweit es sich um Umstände aus seiner Sphäre handelt.[72] Deshalb muss der Geschädigte darlegen und beweisen, dass er die einem Anwender zumutbaren Sicherungsmaßnahmen zur Schadensminderungspflicht getroffen hat, wobei ein diesbezügliches Versäumnis einen Anscheinsbeweis zugunsten des Schädigers begründen kann.[73]

d) Fraglich ist dann, mit welcher Intensität der Schädiger und der Geschädigte den Nachweis zumutbarer Sicherheitsvorkehrungen führen müssen. Problematisch ist dies insbesondere in Bezug auf Updates. Hier sind sowohl der Schädiger als auch der Geschädigte gehalten, das regelmäßige Abrufen und Installieren aller Updates darzulegen und zu beweisen, was insbesondere bei automatisch heruntergeladenen und installierten Updates sowie sog. Silent Updates, von denen der Nutzer nichts mitbekommt, schwer fällt.[74]

Der Nachweis kann hier ggf. mit sog. Logs geführt werden, aus denen sich etwa die Bezeichnung der Release- oder Versionsnummer der Updates ergibt und die dann folgerichtig entgegen wohl bisheriger Praxis für die Dauer der möglichen Haftung aufbewahrt werden müssen.[75]

Ein großes Risiko liegt für die Streitparteien also in der Dokumentation der zumutbaren Sicherungsmaßnahmen.

6 Fazit

Die Gefahr, im Wege der sog. Cyber Liability in Anspruch genommen zu werden, ist für Unternehmen, die die Internet-Technologie nutzen, durchaus real, was sich schon anhand der diversen Klageverfahren zeigt. Der Umstand, dass die meisten dieser Verfahren nicht in Deutschland, sondern mit Vorliebe in den USA geführt werden, sollte nicht darüber hinwegtäuschen, dass entsprechende Haftungsansprüche auch in Deutschland über § 823 Abs. 1 BGB, § 280 Abs. 1 BGB, ggf. i. V. m. § 311 Abs. 2, § 241 Abs. 2 BGB oder § 7 BDSG denkbar sind.

Für Unternehmen, die die Internettechnologie für die Kommunikation, den Datenaustausch und die Informationsbeschaffung nutzen oder die personenbezogene Kundendaten speichern und verarbeiten, ist es daher wichtig, dass ausreichende Sicherungsmaßnahmen gegen Angriffe von außen, aber auch gegen die Gefährdung Dritter aus dem Unternehmen selbst getroffen werden. Aufgrund der Beweislastverteilungen ist es neben den Sicherungsmaßnahmen selbst mindestens genauso wichtig, dass die Sicherungsmaßnahmen und insbesondere deren Aktualisierung, Pflege und Kontrolle ständig dokumentiert werden, um im Streitfall den erforderlichen Nachweis hierüber führen zu können.

Im Rahmen des Risikocontrolling sollte auch überprüft werden, ob man dieses Haftungsrisiko in Form der Cyber Liability über eine Versicherung abdecken sollte. Dann ist in jedem Fall darauf zu achten, dass dieses Haftungsrisiko in den meisten Betriebshaftpflichtversicherungen ausgeschlossen ist, sodass ein Zusatzbaustein oder eine Spezialversicherung für diese Art von Risiken erworben werden müsste. Solche Versicherungen werden von namhaften Versicherern bereits angeboten.[76]

71 BGH, NJW-RR 2004, 1023.
72 BGH, VersR 2006, 286.
73 Koch, CR 2009, 485, 490.
74 Koch, ebenda, 491, der hier das Substanziierungsrisiko demjenigen auferlegt, der bspw. die Silent Updates nutzt.
75 Ebenda, 490 f.
76 Vgl. auch die Zusatzbedingungen zur Betriebshaftpflichtversicherung für die Nutzer von Internet-Technologien – Musterbedingungen des GDV, Stand: April 2007; abrufbar unter http://www.gdv.de/downloads/versicherungsbedingungen/schaden-und-unfallversicherung/zusatzbedingungen-zur-betriebshaftpflichtversicherung-fur-die-nutzer-von-internet-technologien/.

Impressum

Herausgeber:
General Reinsurance AG
Theodor-Heuss-Ring 11, 50668 Köln
www.genre.de/phi

Redaktion: *Nina Dahm-Loraing (verantwortlich), Dr. Axel Horster, Dr. Mathias Schubert, Ursula Smoll*

Anschrift der Redaktion:
Theodor-Heuss-Ring 11, 50668 Köln
Telefon (0221) 9738 650
Fax (0221) 9738 453
E-Mail rlorain@genre.com, smoll@genre.com

Zitiervorschlag: PHi, Jahr, Seitenzahl.

© General Reinsurance AG 2013

Die veröffentlichten Beiträge genießen urheberrechtlichen Schutz, solche mit Angabe des Verfassers stellen nicht unbedingt die Meinung des Herausgebers oder der Redaktion dar.