Seminar:
Deutsches und Internationales Wirtschaftsrecht

Seminarthema:

Die Zivilrechtliche Verantwortlichkeit für Schadprogramme (Malware)

bei
Professor Dr. Georg Borges

vorgelegt von:

Stud. iur. Martin Hossenfelder
Stiepeler Straße 71a
44799 Bochum
martinhossenfelder@web.de

6. Fachsemester
Matrikelnummer: 108002231701

Bochum, den 14. August 2006

Inhaltsverzeichnis

Literaturverzeichnis

Bar, Christian von — Verkehrspflichten – richterliche Gefahrsteuerungsgebote im Deliktsrecht, Carl Heymanns Verlag, Köln u. a. 1980 (zitiert: *Bar*).

Bestmann, Sylle — „Und wer muss zahlen? – Datenschutzrecht im Internet – die Bußgeldvorschriften“, K&R 2003, S. 496-502.

Büchner, Wolfgang **/** ***Ehmer***, Jörg **/** ***Geppert***, Martin u. a (Hrsg.) . — Beck´scher TKG-Kommentar, 2. Auflage, C.H. Beck Verlag, München 2002 (zitiert: *Verfasser*, in: Büchner).

Bundesbeauftragter für den Datenschutz (Hrsg.) — Datenschutzgerechtes eGovernment, http://www.datenschutz.de (zuletzt abgerufen: 12.08.2006) (zitiert: *BfD*, Datenschutzgerechtes eGovernment).

Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.) — „Antispam-Strategien“, http://www.bsi.bund.de/literat/studien/antispam/antispam.pdf, S. 13 (zuletzt abgerufen: 12.08.2006) (zitiert: *BSI,* Antispam-Strategien).

Bundesamt* für die *Sicherheit in der Informationstechnik (Hrsg.) — „Computer-Viren“, http://www.bsi.de/gshb/deutsch/g/g05023.htm (zuletzt abgerufen: 12.08.2006) (zitiert: *BSI,* Computer-Viren).

Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.) — „Denial-of-Service-Attacken“, http://www.bsi-fuer-buerger.de/abzocker/05_04.htm (zuletzt abgerufen: 12.08.2006) (zitiert: *BSI,* Denial-of-Service-Attacken).

Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.) — „Die Lage der IT-Sicherheit in Deutschland“, http://www.bsi.de/literat/lagebericht/lagebericht2005.pdf (zuletzt abgerufen: 12.08.2006) (zitiert: *BSI,* Die Lage der IT-Sicherheit in Deutschland).

Bundesamt für die Sicherheit in der Informationssicherheit (Hrsg.) Grundschutzhandbuch, http://www.bsi.de/gshb (zuletzt abgerufen: 12.08.2006) (zitiert: *BSI*, GrundschutzHB).

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) „Viren“, http://www.bsi-fuer-buerger.de/viren/04_02.htm (zuletzt abgerufen: 12.08.2006) (zitiert: *BSI,* Viren).

Cohen, Frederick „Computer Viruses – Theory and Experiments“, Computer & Security 6/1987, S. 22-35.

Deckert, Martina „Die Verkehrspflichten“, Jura 1996, S. 348-354.

Eichhorn, Bert Internet-Recht – Ein Lehrbuch für das Recht im World Wide Web, 3. Auflage, Fortis Verlag, Troisdorf 2003 (zitiert: *Eichhorn*).

Eichelberger, Jan „Sasser, Blaster, Phatbot & Co. – alles halb so schlimm? - Ein Überblick über die strafrechtliche Bewertung von Computerschädlingen“, MMR 2004, S. 594-597.

Erben, Meinhard **/** ***Zahrnt***, Christoph „Die Rechtssprechung zur Datensicherung“, CR 2000, S. 88-91.

Ernst, Stefan „Hacker und Computerviren im Strafrecht“, NJW 2003, S. 3233-3239.

Ernst, Stefan (Hrsg.) Hacker, Cracker & Computerviren, Dr. Otto Schmidt Verlag, Köln 2004 (zitiert: *Verfasser*, in: Ernst).

Edenfeld, Stefan „Grenzen der Verkehrspflicht“, VersR 2002, S. 272-278.

Faustmann, Jörg „Der Deliktische Datenschutz“, VuR 2006, S. 260-263.

Formen, Björn Anforderungen des Rechts an die IT-Sicherheit im Unternehmen, http://www.genua.de/news/rechtliches/publications/Anforderungen_des_Rechts_an_IT-Sicherheit.pdf (zuletzt abgerufen: 12.08.2006) (zitiert: *Formen*).

Gerstenberg, Ekkehard — „Löschen von Tonbändern als neuer strafrechtlicher Tatbestand“, NJW 1956, S. 540.

Gliss, Hans — „Outsourcing der Datenverarbeitung“, DSB 6/2001, S. 6.

Gola, Peter / ***Schomerus***, Rudolf — Kommentar zum Bundesdatenschutzgesetz, 8. Auflage, C. H. Beck, München 2005 (zitiert: *Gola/Schomerus*).

Gravenreuth, Günter Freiherr von — „Juristisch relevante Fragen zur Beurteilung von Computer-Programmen“, GRUR 1986, S. 720-727.

Gravenreuth, Günter Freiherr von — Computerviren, 2. Auflage, Carl Heymanns Verlag, Köln u. a. 1998 (zitiert: *von Gravenreuth*).

Harley, David / ***Slade***, Robert / ***Gattiker***, Urs — Das Anti-Viren-Buch, mitp-Verlag, Bonn 2002 (zitiert: *Harley/Slade/Gattiker*).

Heckmann, Dirk — „Rechtspflichten zur Gewährleistung von IT-Sicherheit im Unternehmen – Maßstäbe für ein IT-Sicherheitsrecht“, MMR 2006, S. 280-285.

Heidrich, Joerg — „Unwissenheit schützt vor Strafe nicht – Wer für die Verbreitung von Viren haftet“, c´t 19/2004, S. 168-169.

Hein, Frank Martin — „E-Mail, Portale und Intranet weit verbreitet, traditionell genutzt“, DSWR 2006, S. 189-192.

Hüffer, Uwe — Kommentar zum Aktiengesetz, 7. Auflage, C. H. Beck, München 2006 (zitiert: *Hüffer*, AktG).

Institut der Wirtschaftsprüfer in Deutschland (Hrsg.) — Checkliste zur Abschlussprüfung bei Einsatz von Informationstechnologie, IDW Verlag, Düsseldorf 2002 (zitiert: *IDW*, Checkliste).

Institut für Telematik (Hrsg.) „Security Auditing - Erkennung von IT-Sicherheitsrisiken“, http://www.telematik-institut.org/ profil_ und_ kontakt/info-material/Security_ Auditing_ger.pdf (zuletzt abgerufen: 12.08.2006) (zitiert: *Institut für Telematik*).

IT-Systemtechnik & Fachinformatik (Hrsg.) „Arbeitsspeicher - Hauptspeicher - RAM“, http://www.its05.de/html/arbeitsspeicher.html (zuletzt abgerufen: 12.08.2006) (zitiert *IT-Systemtechnik*).

Janssen, Wilhem „RAM, Internet und e-commerce“, Online-Lexikon, http://www.at-mix.de/ram.htm (zuletzt abgerufen: 12.08.2006) (zitiert: *Janssen*)

Klaeren, Herbert Viren, Würmer und Trojaner – Streifzüge durch die Computerwelt, Klöpfer & Meyer Verlag, Tübingen 2006 (zitiert: *Klaeren*).

Klußmann, Niels Lexikon der Kommunikations- und Informationstechnik, 3. Auflage, Hüthig Verlag, Heidelberg 2001 (zitiert: *Klußmann*).

Koch, Robert „Haftung für die Weiterverbreitung von Viren durch E-Mails“, NJW 2004, S. 801-807.

Kötz, Hein / ***Wagner***, Gerhard Deliktsrecht, 10. Auflage, Luchterhand Verlag, München 2006 (zitiert: *Kötz/Wagner*).

Kropff, Bruno / ***Semler***, Johannes (Hrsg.) Münchener Kommentar zum Aktiengesetz, Band 3, §§ 76-117, 2. Auflage, C. H. Beck, München 2004 (zitiert: *Verfasser*, in: MüKo/AktG).

Krüger, Alfred Angriffe aus dem Netz – Die neue Szene des digitalen Verbrechens, Heise Zeitschriften Verlag, Hannover 2006 (zitiert: *Krüger*).

Landesman, Mary — Free Antivirus Software, http://antivirus.about.com/od/antivirussoft warereviews/a/freeav_2.htm (zuletzt abgerufen: 12.08.2006) (zitiert: *Landesman*).

Lang, Markus — „PC, aber sicher! – Sicherheit beim Einsatz von Personalcomputern“, JurPC Web-Dok. 205/2001, http://www.jurpc.de/aufsatz/20010205.htm (zuletzt abgerufen: 12.08.2006).

Larenz, Karl (Begr.) — Lehrbuch des Schuldrechts, Band 2, Halbband 2, 13. Auflage, C. H. Beck Verlag, München 1994 (zitiert: *Larenz*/Verfasser).

Leible, Stefan / ***Wildemann***, Andree — Kommentar zu BGH, Urteil v. 4.3.2004 – Az: III ZR 96/03, K&R 2004, S. 288-290.

Lemhöfer, Bernt — „Die überholende Kausalität und das Gesetz“, JuS 1966, S. 337-344.

Libertus, Michael — „Zivilrechtliche Haftung und strafrechtliche Verantwortlichkeit bei unbeabsichtigter Verbreitung von Computerviren“, MMR 2005, S. 507-512.

Mankowski, Peter — Anmerkung. zu BHG, Urteil v. 4.3.2004 – Az: III ZR 96/03, MMR 2004, S. 312-315.

Meier, Klaus / ***Wehlau***, Andreas — „Die Zivilrechtliche Haftung für Datenlöschung, Datenverlust und Datenzerstörung“, NJW 1998, S. 1585-1591.

Mühle, Kerstin — Hacker und Computerviren im Internet – eine strafrechtliche Beurteilung, Diss. iur. Passau 1998. (zitiert: *Mühle*).

Palandt, Otto (Begr.) — Bürgerliches Gesetzbuch, Kommentar, 65. Auflage, C.H. Beck Verlag, München 2006 (zitiert: *Verfasser*, in: Palandt).

Raab, Thomas — „Die Bedeutung der Verkehrspflichten und ihre systematische Stellung im Deliktsrecht“, JuS 2002, S. 1041-1048.

Rebmann, Kurt /
Rixecker, Roland /
Säcker, Franz Jürgen (Hrsg.)
Münchener Kommentar zum Bürgerlichen Gesetzbuch,
Band 1, §§ 1 – 240, 4. Auflage 2001,
Band 2a, §§ 241 – 432, 4. Auflage 2003,
Band 5, §§ 705 – 853, 4. Auflage 2004,
C.H. Beck Verlag, München
(zitiert: *Verfasser*, in: MüKo/BGB).

Rechenberg, Peter /
Pomberger, Gustav
Informatik-Handbuch,
3. Auflage,
Hanser Verlag, München 2002
(zitiert: *Verfasser*, in: Rechenberg/Pomberger).

Rössel, Markus
„Haftung für Computerviren - Die Aktuelle Rechtslage zur Haftung im Überblick“,
ITRB 2002, S. 214-216.

Schlosser, Hans
„Deliktischer Schadensersatzanspruch aus § 823 Abs. 2 BGB und eigenständiger Interessenschutz des Verkehrsopfers – Entscheidungsrezension zu BGH, NJW 1980, S. 1792“,
JuS 82, S. 657-661.

Schmidtbauer, Franz
„Schadensersatz wegen Viren“,
http://www.internet4jurists.at/news/aktuell36a.htm (zuletzt abgerufen: 12.08.2006) (zitiert: *Schmidtbauer*).

Schneider, Jochen /
Günther, Andreas
„Haftung für Computerviren“,
CR 1997, S. 389-396.

Simitis, Spiros (Hrsg.)
Kommentar zum Bundesdatenschutzgesetz,
6. Auflage,
Nomos Verlag, Baden-Baden 2006
(zitiert: *Verfasser*, in: Simitis).

Soergel, Hans (Begr.)
Kommentar zum Bürgerlichen Gesetzbuch,
Band 12, §§ 823 – 853,
13. Auflage,
Kohlhammer Verlag, Stuttgart 2006
(zitiert: *Verfasser*, in: Soergel).

Spindler, Gerald
„Haftung und Verantwortlichkeit im IT-Recht",
CR 2005, S. 741-747.

Spindler, Gerald
Anm. zu BHG, Urteil v. 4.3.2004 – Az: III ZR 96/03, JZ 2004, S. 1128-1132.

Spindler, Gerald / ***Schmitz***, Peter /
Geis, Ivo
Kommentar zum Teledienstgesetz,
C. H. Beck Verlag, München 2004
(zitiert: *Verfasser*, in: Spindler).

Staudinger, Julius von (Begr.) — Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetzen und Nebengesetzen, Zweites Buch, Recht der Schuldverhältnisse, §§ 249 – 254, 14. Bearbeitung. 2005, §§ 823 – 825, 13. Bearbeitung 1999, de Gruyter Verlag, Berlin (zitiert: *Verfasser*, in: Staudinger).

Steffen, Erich — „Verkehrspflichten im Spannungsfeld von Bestandsschutz und Handlungsfreiheit“, VersR 1980, S. 409-412.

Taeger, Jürgen — Außervertragliche Haftung für fehlerhafte Computerprogramme, J. C. B. Mohr Verlag, Tübingen 1995 (zitiert: *Taeger*).

The Honeynet Project & Research Alliance (Hrsg.) — „Know your Enemy: Tracking Botnets”, http://www.honeynet.org/papers/bots/ (zuletzt abgerufen: 12.08.2006) (zitiert: *The Honeynet Project & Research Alliance).*

Thorbrügge, Marco — „Botnetze –ferngesteuerte Rechner im Dienste von Kriminellen“, DFN-Mitteilungen 2005, Ausgabe 68, S. 21.

Trepte, Andreas — „Arbeitsspeicher mit Langzeitgedächtnis“, http://www.innovations-report.de/html /berichte /informationstechnologie/bericht-10599.html (zuletzt abgerufen: 12.08.2006) (zitiert: Trepte).

Wehlau, Andreas — „Haftung für Datenverlust – der Datenbestand als sonstiges Recht i. S. d. § 823 Abs. 1 BGB“, OLGR 2004, K, S. 27-31.

Erman, Walter (Begr.) — Handkommentar zum Bürgerlichen Gesetzbuch, 11. Auflage, Band I, §§ 1 – 811, Band II, §§ 812 – 2385, Dr. Otto Schmidt Verlag 2004 (zitiert: *Verfasser*, in: Erman).

Winterer. Andreas — Viren, Würmer und Trojanische Pferde, Data Becker Verlag, Düsseldorf 2002 (zitiert: *Winterer*).

Wuermeling, Ulrich — „Einsatz von Programmsperren“, CR 1994, S. 585-595.

Es wurden die üblichen Abkürzungen benutzt.
Vgl.:

Butz, Cornelie / ***Kirchner***, Hildebert,	Abkürzungen der Rechtssprache, 5. Auflage, de Gruyter Verlag, Berlin 2003.

A. Einführung

Kein Medium hat in den letzten Jahren die Kommunikationsgewohnheiten der Menschen so verändert, wie das Internet. Die Verbreitung von E-Mail, Instant Messaging und Internettelefonie ermöglicht Unternehmen wie Privatleuten, schnelle, einfache und kostengünstige Kommunikation.[1] Allerdings werden die Vorteile dieser neuen Plattformen durch die zunehmende Verbreitung von Schadprogrammen bzw. Malware begleitet. Die Anzahl an weltweit existierenden Schadprogrammen wird auf über 150.000 geschätzt, wobei jeden Monat Hunderte neu entstehen.[2] Schäden, die sich allein auf Computerviren zurückführen lassen, liegen in Deutschland im dreistelligen Millionenbereich.[3] Diese können in Form von Hardwarefehlfunktionen oder –zerstörungen, und als Datenvernichtung bzw. -veränderung auftreten. Die weltweite Vernetzung hat somit zu einer parallel anwachsenden Verbreitung von Malware geführt, die ein sich vergrößerndes Gefahrenpotenzial erzeugt hat.[4] Der Programmierer der Malware wird zumeist nicht identifiziert.[5] Es stellt sich daher die Frage, wer für den durch die Malware verursachten Schaden haftet.

I. Ziel der Arbeit

Ziel der nachfolgenden Untersuchung ist es, die Verantwortlichkeit des Internet-Nutzers für Schäden zu erläutern, die sich durch Malware ergibt, welche über seine Einrichtungen verbreitet wird. Ein Großteil der Malware wird heute durch selbst verbreitende Schadprogramme, insbesondere durch Massenmailwürmer verursacht.[6] Ein aktives Tun des Computernutzers wird somit oft nicht vorausgesetzt. Als Schwer-

---

[1] *Hein*, DSWR 2006, S. 191.
[2] *BSI*, Viren (zuletzt abgerufen: 12.08.2006); *Krüger*, S. 33.
[3] *BSI*, Informationen zu Computerviren (zuletzt abgerufen: 12. August 2006).
[4] *Klaeren*, S. 100; *Krüger*, S. 45; *Harley/Slade/Gattiker*, S. 631, *Mühle*, S. 1.
[5] *von Gravenreuth*, S. 28.
[6] *BSI*, Die Lage der IT-Sicherheit in Deutschland 2005, S. 19 (zuletzt abgerufen: 12.08.2006).

punkt der Arbeit soll daher die deliktsrechtliche Verantwortlichkeit für die unbeabsichtigte Verbreitung von Malware erarbeitet werden. Zudem wird untersucht, ob sich Unterschiede in der haftungsrechtlichen Beurteilung von sich selbst verbreitender Malware und durch den Nutzer verbreiteten Schadprogrammen ergeben. Darüber hinaus soll ermittelt werden, ob unterschiedliche Haftungsrisiken bzw. Sorgfaltsmaßstäbe für Unternehmen und Private bestehen.

II. Gang der Darstellung

Um die Verantwortlichkeit des Internetnutzers für Schadprogramme beurteilen zu können, wird in einem ersten Schritt der Begriff und die Art der Verbreitung von Malware erklärt (B). In einem zweiten Schritt soll im Rahmen des Deliktsrechts geprüft werden, welche Haftungsansprüche sich aus der unbeabsichtigten Weiterverbreitung von Malware ergeben (C). Im Zuge der Darstellung wird im Besonderen herauszuarbeiten sein, welche Sorgfaltsanforderungen zur Vermeidung der Verbreitung zu erwarten sind, und ob diese für Unternehmer und Private variieren. Darauf folgend soll kurz auf die (vor-)vertragliche Haftung eingegangen werden (D). Um die Verantwortlichkeit beurteilen zu können, werden abschließend Malware-spezifische Umstände, die die Haftung einschränken können, aufgezeigt (E).

B. Malware

Malware steht für „malicious software“[7] und bezeichnet Programme, die Schäden verursachen.[8] Um verstehen zu können, welche Schäden Malware verursacht und wie man präventiv bzw. repressiv dagegen vorgehen kann, müssen zuerst die Besonderheiten der einzelnen Schadprogramme analysiert werden. Dabei wird in der rechtswissenschaftlichen Literatur oftmals nur der Begriff Virus benutzt.[9] So wird z. B. jede Art von Schadprogramm als Virus im weiten Sinne qualifi-

[7] Bösartige Software.
[8] *Harley/Slade/Gattiker*, S. 89.
[9] So *Koch*, NJW 2004, S. 801 (803); *Ernst*, NJW 2003, S. 3233 (3234 f.); *Schneider/Günther*, CR 1997, S. 389, Fn. 1.

ziert.[10] Die verschiedenen Schadprogramme haben unterschiedliche Eigenschaften, so dass auch die Rechtsfolgen variieren können. Im Folgenden sollen die charakteristischen Eigenschaften der verschiedenen Programme herausgearbeitet werden.

I.Viren

Ein Computervirus ist ein Programmcode, der sich selbst vervielfältigt und der eine oder mehrere weitere Funktionen enthält.[11] Voraussetzung eines Virus ist ein Wirtsprogramm, an das er sich anhängen kann, um bei Aktivierung des Programms weitere Programme zu infizieren.[12] Dies geschieht dadurch, dass er diese insoweit verändert, dass das Programm eine Kopie des Virus aufnimmt.[13] Die infizierten Dateien sind somit gestört und können oftmals ihre normale Funktion nicht mehr ausführen.[14] Zumindest führen sie (auch) etwas anderes aus als vom Anwender gewünscht. Die neu infizierten Programme suchen daraufhin nach Programmen, die sie anstecken können. Dadurch entsteht eine Kettenreaktion, die durch Netzwerke verstärkt wird. Darüber hinaus hat der Virus, neben seiner Fähigkeit zu Reproduktion, eine weitere Funktion.[15] Diese ist regelmäßig eine Schadensfunktion.[16] Die Schäden, die Art des Zugangs des Virus in das System und die Beseitigungsmöglichkeiten unterscheiden sich nach der Art des Virus.

1. Bootviren

Bootviren infizieren die Systemsoftware eines Datenträgers, in der Startphase des Computers, während des Bootvorgangs.[17] Sie platzieren sich auf einer Diskette oder einer Festplatte und gelangen während

---

[10] *Rössel*, ITRB 2002, S. 214.
[11] Grundlegend *Cohen*, Computers & Security 6/1987, S. 22 ff.; *Piepenbrock*, in: Geppert, Teil C, C.; *Pierrot*, in Ernst, Rn. 81; *von Gravenreuth*, GRUR 1986, S. 720; *Mühle*, S. 25.
[12] *Mühle*, S. 29.
[13] *Lang*, JurPC Web-Dok. 205/2001, Abs. 49 (zuletzt abgerufen: 12.08.2006).
[14] *Winterer*, S.72.
[15] *von Gravenreuth*, S. 1.
[16] *Pierrot*, in: Ernst, Rn. 83; *Mühle*, S. 24.
[17] *Pierrot*, in: Ernst, Rn. 115.

des Bootvorgangs und vor dem Laden des Betriebssystems in den Arbeitsspeicher.[18] Die Bootsektoren nicht schreibgeschützter Disketten werden infiziert.[19] Verbreitet werden sie grds. durch das Booten infizierter Disketten auf anderen Computern. Bootviren haben heute nur noch einen geringen Stellenwert, da Disketten kaum noch genutzt werden.[20]

2. Dateiviren

Dateiviren infizieren ausführbare Dateien (z. B. COM und EXE Dateien), indem sie sich anhängen[21] oder diese überschreiben.[22] Wird die Programmdatei überschrieben ist sie nicht mehr ausführbar.[23] Der Virus wird durch die Ausführung des infizierten Programms aktiviert.[24] Der Dateivirus wird speicherresident und infiziert die nach ihm ausgeführten Programme.[25]

3. Makroviren

Anwendungsprogramme, wie Tabellenkalkulations- und Textverarbeitungsprogramme verfügen oft über eine eigene Makrosprache. Damit kann man kleine Programme schreiben, um häufig wiederkehrende Aktionen zu automatisieren. Makros laufen nur in Verbindung mit dem jeweiligen Anwendungsprogramm (z. B. Microsoft Word). Diese Makrosprachen lassen sich aber auch nutzen um schädigende Wirkungen zu erzeugen, indem ein Makro mit einer Schadensroutine versehen wird. Makroviren infizieren nicht die Anwendungsprogramme, sondern die erzeugten Dokumentdateien.[26] Word-Makroviren sind die

---

[18] *Harley/Slade/Gattiker*, S. 147 ff. *BSI*, Computer-Viren (zuletzt abgerufen: 12.08.2006); *Lang*, JurPC Web-Dok. 205/2001, Abs. 56 (zuletzt abgerufen: 12.08.2006).
[19] *BSI*, Computer-Viren (zuletzt abgerufen: 12.08.2006).
[20] *Pierrot*, in: Ernst, Rn. 118.
[21] *BSI*, Computer-Viren (zuletzt abgerufen: 12.08.2006).
[22] *Lang*, JurPC Web-Dok. 205/2001, Abs. 60 (zuletzt abgerufen: 12.08.2006).
[23] *BSI*, Computer-Viren (zuletzt abgerufen: 12.08.2006).
[24] *Pierrot*, in: Ernst, Rn. 113.
[25] *Pierrot*, in: Ernst, Rn. 113.
[26] *Lang*, JurPC Web-Dok. 205/2001, Abs. 61 (zuletzt abgerufen: 12.08.2006).

Viren, die mittlerweile die meisten Systeme infizieren.[27] Die Gefahr liegt darin, dass Makroviren nicht betriebssystemabhängig sind, und sich überall dort verbreiten können, wo das entsprechende Anwendungsprogramm installiert ist.

4. Polymorphe Viren

Polymorphe Viren haben die Fähigkeit sich nach der Infizierung zu verändern, indem sie sich neu verschlüsseln oder den Programmcode ändern.[28] Dadurch wird ein Aufspüren anhand der Byte-Folge bzw. Signatur durch Antiviren-Software unmöglich.[29] Die neue Generation von Antiviren-Software kann diesen Typus mittels algorithmischer Suche oder heuristischer Analyse teilweise erkennen.

5. Hybride Viren

Hybride Viren kombinieren Verbreitungsmöglichkeiten um das System zu infizieren.[30] Zumeist treten sie als Kombination von Datei- und Bootsektorviren auf. Das Problem besteht darin, dass bei Bereinigung des Bootsektors dieser wieder durch den Dateivirus infiziert wird und umgekehrt.

II. Würmer

Würmer sind Programme, die sich selbst innerhalb eines Netzwerkes replizieren, aber im Gegensatz zu einem Virus keine Wirtsdatei benötigen.[31] Es handelt sich um ein eigenständiges Programm. Des Weiteren warten Würmer nicht, wie Viren, darauf aktiviert zu werden, um andere Programme zu infizieren. Sie verbreiten sich selbstständig über Netzwerke (LAN[32], Internet) oder E-Mail,[33] z. B. indem sie sich an

---

[27] *BSI*, Grundschutz-HB, G 5.43 (zuletzt abgerufen: 12.08.2006).
[28] *Pierrot*, in: Ernst, Rn. 127; *Lang*, JurPC Web-Dok. 205/2001, Abs. 68 (zuletzt abgerufen: 12.08.2006).
[29] *Lang*, JurPC Web-Dok. 205/2001, Abs. 68 (zuletzt abgerufen: 12.08.2006).
[30] *Pierrot*, in: Ernst, Rn. 126.
[31] *Pierrot*, in: Ernst, Rn. 109:
[32] Local Area Network
[33] *Pierrot*, in Ernst, Rn. 109; *von Gravenreuth*, S. 15.

die ersten fünfzig Einträge des Adressbuches verschicken. Ferner haben Würmer zumeist keine Schadensroutine.[34] Die Gefahr ergibt sich aus der Überlastung der Netzwerksysteme bzw. eines Servers und verstopften Leitungen.[35] Dies kann das Abschalten ganzer Systeme notwendig machen,[36] da teilweise bereinigte Netzwerkbereiche durch die nicht bereinigten erneut infiziert werden können. Darüber hinaus können Würmer Viren und Trojanische Pferde transportieren und sind daher Schadensmultiplikatoren.[37]

III. Trojanische Pferde

Trojanische Pferde sind Programme, die sich als nützliche Anwendungen tarnen und im Hintergrund versteckte Programme installieren, die eine schädliche Wirkung entfalten.[38] Im Gegensatz zu Viren und Würmern können sie sich nicht selbst replizieren. Die nicht sichtbaren Programme werden z. B. zum Fernsteuern des Systems oder zum Ausspähen von Passwörtern und Benutzerdaten verwendet.[39] Sie können aber auch als Dropper[40] für andere Schadprogramme dienen. Ferner können Trojanische Pferde zum Löschen von Dateien, zur Modifizierung von Zugriffsrechten und zur Installierung von Backdoors benutzt werden.[41]

IV. Backdoors

Backdoors (Hintertüren) sind Systemkomponenten, die es dem Benutzer ermöglichen über Programmteile, die für den normalen Betrieb nicht benötigt werden, Zugang zum System zu bekommen, indem die normale Zugriffssicherung umgangen wird.[42] Diese Zugriffsmöglichkeit wird oft von Programmautoren in die Anwendung eingefügt, da-

---

[34] *Pierrot*, in Ernst, Rn. 109.
[35] *von Gravenreuth*, S. 15; *Mühle*, S. 27;
[36] Beispiele bei *von Gravenreuth*, S. 15.
[37] *Pierrot*, in: Ernst, Rd. 110.
[38] *von Gravenreuth*, S. 11; *Mühle*, S. 27; *BSI*, Grundschutz-HB, M 2.224, (zuletzt abgerufen: 12.08.2006).
[39] *Krüger*, S. 51 ff.
[40] Programm das ein anderes Schadprogramm „abwirft"..
[41] *Lang*, JurPC Web-Dok. 205/2001, Abs. 44 (zuletzt abgerufen: 12.08.2006).
[42] *von Gravenreuth*, S. 14; *Mühle*, S 29 f.

mit Wartungstechniker, Systemprogrammierer etc. aus der Entfernung schnellen und umkomplizierten Zugang zu den einzelnen Systemen bekommen können.[43] Eine solche Umgehung kann auch durch Programme nachträglich im Zuge eines Hackerangriffs bzw. durch ein Trojanisches Pferd auf dem System installiert werden.[44] Durch eine Backdoor wird ein ungehinderter Zugang zum System ermöglicht.[45]

V. Spyware

Als Spyware werden Programme bezeichnet, die ohne den Nutzer zu informieren, persönliche Daten sammeln und bei Einwahl ins Internet zu einem Dritten verschicken.[46] Spyware wird häufig durch „Aktive Inhalte“[47] (Java-Applets, ActiveX-Anwendungen etc.) von Internetseiten auf das System installiert. Sie kann auch über Trojanische Pferde oder Würmer übertragen werden.

VI. Malware-ähnliche Programme

Als Malware-ähnliche Programme kann man Spam und Dialer einordnen. Spam-Nachrichten sind unerwünscht übertragene E-Mails, die massenhaft versendet werden und zumeist einen werbenden Charakter haben.[48] Nach Schätzungen sind heute 60 bis 90 % aller E-Mails als Spam zu qualifizieren.[49] Dialer sind Einwahlprogramme, durch die über das Telefon- oder ISDN-Netz eine Internetverbindung hergestellt werden kann. Diese Technik kann missbraucht werden, wenn ein Dialer durch Trojanische Pferde oder Würmer auf dem System installiert wird, um eine teurere Verbindung aufzubauen, wodurch höhere Entgeltabrechungen entstehen.

---

[43] *von Gravenreuth*, S. 14.
[44] *Institut für Telematik* (zuletzt abgerufen: 12.08.2006).
[45] *Institut für Telematik* (zuletzt abgerufen: 12.08.2006).
[46] *Klaeren*, S. 107 f.; *Krüger*, S.83 ff.
[47] Aktive Inhalte bezeichnen nicht sichtbare Funktionen von Webseiten, die durch den Browser ausgeführt werden.
[48] *Klaeren*, S. 109; *BSI*; Antispam-Strategien, S.13 (zuletzt abgerufen: 12.08.2006).
[49] *BSI*, Antispam-Strategien, S.10 (zuletzt abgerufen: 12.08.2006).

VII. Weitere Möglichkeiten des Einsatzes von Malware

Malware kann eingesetzt werden um Netze zur massenhaften Verbreitung von Spam zu erstellen oder um Netzwerke, Server und Webseiten so zu belasten, dass sie nicht mehr funktionieren.

1. Botnetze

Ein Bot ist ein Programm, das, sobald es auf einem Computersystem installiert ist, das System fernsteuern kann.[50] Nach der Installation verbindet es sich mit einem Server, zumeist mit einem voreingestellten Internet Relay Chat (IRC)-Server. IRC ist ein textbasiertes Chat-Protokoll.[51] Nach der Verbindung mit dem Server wählt der Bot sich unter einem Passwort in einen speziellen Kanal ein. Über IRC-Befehle steuert das nun die Kontrolle besitzende System (Botmaster) die mit Bots infizierten Systeme (Bothosts) und verbindet sich zu einem Botnetz.[52] Verbreitet werden Bots meistens durch Würmer oder Trojanische Pferde. Botnetze können z. B. zur massenhaften Verbreitung von Spam, Viren, Trojanischen Pferden etc. oder zur Durchführung einer Distributed Denial of Service (DDoS)-Attacke genutzt werden.[53]

2. Denial of Service-Attacken

Eine Denial of Service (DoS)-Attacke ist ein Angriff auf zumeist einen Server mit dem Ziel, diesen so zu überlasten, dass das System anstehende Aufgaben nicht mehr bewältigen kann oder zusammenbricht.[54] Ein Mittel zur Überlastung kann z. B. die massenhafte Zusendung von E-Mails an einen Server sein.

---

[50] *Klaeren*, S. 108; *Thorbrügge*, DFN Mitteilungen 68/2005, S. 21.
[51] Protokolle sind Ablaufregeln, die das Format, den Inhalt, die Reihenfolge und die Bedeutung gesendeter Nachrichten zwischen den einzelnen Instanzen bestimmen. HTTP (Hyper Text Transfer Protocol) und FTP (File Transfer Protocol) sind weitere Protokolle.
[52] *Thorbrügge*, DFN Mitteilungen 68/2005, S. 21; *The Honeynet Project & Research Alliance* (zuletzt abgerufen: 12.08.2006).
[53] Vgl. *Krüger*, S. 191.
[54] *Pierrot*, in: Ernst, Rn. 128; *BSI*, Denial-of-Service-Attacken (zuletzt abgerufen: 12.08.2006).

3. Distributed Denial of Service-Attacken

Als Distributed Denial of Service (DDoS)-Attacke bezeichnet man einen koordinierten DoS-Angriff mittels einer großen Anzahl anderer Systeme.[55] Entweder mehrere Angreifer greifen zur gleichen Zeit an oder ein Botnetz wird genutzt, um eine große Anzahl an Systemen fernzusteuern.[56] Durch die Bündelung der Systeme kann der angegriffene Server effizienter und schneller überlastet werden.

VIII. Schutz vor Malware

Antiviren-Software und Firewalls können das Eindringen von Malware z. T. verhindern. Antiviren-Software kann zumeist nicht alle Arten von Schadprogrammen erkennen. Spezielle Software zur Erkennung von Spyware, Backdoors bzw. Dialern ist für einen umfassenden Schutz unabdingbar. Da sich täglich neue Viren, Würmer und Trojanische Pferde verbreiten, bedarf es ständiger Software-Updates,[57] auch wenn Malware aufgrund ihrer Neuheit nicht immer von der Software erkannt werden kann.[58] Ein umfassender Schutz ist nicht möglich.[59] Neben dem Einsatz von Schutzprogrammen ist der vorsichtige Umgang mit Internet und E-Mail Grundvoraussetzung um Gefährdungen abzuwehren.

---

[55] *Klaeren*, S. 109.
[56] Ausführlich *Pierrot*, in: Ernst, Rn. 132; *Harley/Slade/Gattiker*, S. 117.
[57] *Mankowski*, in: Ernst, Rn. 492.
[58] *Klaeren*, S. 121.
[59] *Klaeren*, S. 121.

C. Deliktsrechtliche Haftung für unbeabsichtigte Verbreitung von Malware

Ist Malware in ein Computersystem eingedrungen, besteht die Gefahr der Weiterverbreitung auf andere Systeme, auf denen es Schäden verursachen kann. Wird Malware vorsätzlich weitergeleitet, haftet der Schädiger aus § 826 BGB wegen vorsätzlicher sittenwidriger Schädigung.[60] Daneben können Ansprüche aus den §§ 823 Abs. 1, Abs. 2 BGB i. V. m. Schutzgesetzen in Betracht kommen.[61] Durch E-Mails, Instant Messenger-Nachrichten usw. kann der Internet-Nutzer Malware unbeabsichtigt an Dritte weiterleiten. Darüber hinaus können sich Würmer eigenständig z. B. als E-Mail-Anhang an alle Kontakte des Adressbuchs verschicken[62] oder der Computer wird als Teil eines Botnetzes missbraucht um Malware zu verbreiten,[63] wobei kein aktives Tun des Internet-Nutzers vorliegt. Da im Rahmen unbeabsichtigter Weiterverbreitung von Malware im Internet- und E-Mail-Verkehr zwischen Versender und Empfänger oft keine vertragliche oder vorvertragliche Beziehung besteht,[64] sind vorrangig Ansprüche aus Delikt zu prüfen.

I. Haftung nach § 823 Abs. 1 BGB

Durch die Weiterverbreitung von Malware müsste eines der von § 823 Abs. 1 BGB geschützten Rechtsgüter verletzt sein. Ob eine Verletzung vorliegt, hängt von der Schadensroutine der Malware ab. Daten können gelöscht, verändert, verschoben und ausspioniert werden.[65] Hardwareschäden können auftreten,[66] wodurch das System in seiner Substanz beschädigt wird. Durch (D)Dos-Attacken kann das System

---

[60] *Mankowski*, in: Ernst, Rn. 514; *Libertus*, MMR 2005, S. 507; *Koch*, NJW 2004, S. 801.
[61] *Mankowski*, in: Ernst, Rn. 514; *Libertus*, MMR 2005, S. 507; *Koch*, NJW 2004, S. 801.
[62] S. o. B. II.
[63] S. o. B. VII. 1.
[64] *Libertus*, MMR 2005, S. 508.
[65] S. o. B. I., IV.
[66] *Harley/Slade/Gattiker*, S. 143; *Pierrot*, in Ernst, Rn. 111.

überlastet werden. Hierbei gibt es keine Veränderung von Daten. Durch die Attacke wird kein Schadprogramm installiert. Der Schaden besteht in einer Störung der Nutzbarkeit des Gesamtsystems.[67] Die Unterschiedlichkeit an möglichen Schadensroutinen führt dazu, dass auch verschiedene Rechtsgüter verletzt sein können.

1. Rechtsgutverletzungen durch Malware

a. Leben, Körper und Gesundheit

Eine Verletzung von Leben, Körper und Gesundheit kann nicht unmittelbar durch Malware verursacht werden. Dennoch ist es vorstellbar, dass ein Schadprogramm Computersysteme so verändert bzw. beeinträchtigt, dass z. B von EDV-Anlagen gesteuerte medizinische Geräte versagen und durch eine mittelbare Verletzung ein Schaden eintritt.[68]

b. Eigentum

Der Eigentumsschutz des § 823 Abs. 1 BGB bezieht sich nur auf bewegliche und unbewegliche Sachen im Sinne des § 90 BGB.[69] Die Sache kann in der Substanz verletzt sein z. B. durch Zerstörung, Beschädigung oder Verunstaltung.[70] Ferner ist die Entziehung der Sache Verletzungshandlung im Rahmen des § 823 Abs. 1 BGB.[71] Schließlich soll auch eine nicht nur kurzfristige Gebrauchs- bzw. Nutzungsbeeinträchtigung der Sache genügen.[72]

---

[67] S. o. B., VII., 3.
[68] *Koch*, NJW 2004, S. 802; *Schneider/Günther*, CR 1997, S 389 (391); *Taeger*, S. 259 f.
[69] *Hager*, in: Staudinger, § 823, Rn. B 58.
[70] *Sprau*, in Palandt, § 823, Rn. 7.
[71] *Sprau*, in Palandt, § 823, Rn. 7.
[72] BGH, NJW 1994, S. 517 (518); *Hager*, in: Staudinger, § 823, Rn. B 97; *Schiemann*, in: Erman, § 823, Rn. 25.

aa. Eigentumsverletzung bei Hardwareschäden und Störungen des Gesamtsystems

Wird durch Malware ein Hardwareschaden verursacht, liegt eine den Anforderungen des § 823 Abs. 1 BGB genügende Eigentumsverletzung im Sinne einer Beschädigung oder Zerstörung vor.[73] Hat die Schadensroutine eines Malwareprogramms das Gesamtsystem so in seiner Ausführbarkeit beeinträchtigt, z. B. bei permanenten Systemabstürzen oder Unfähigkeit des Startens bei Infizierung eines Boot-Virus, ist zumindest eine nicht nur kurzfristige Gebrauchsbeeinträchtigung des Computers als Ganzes anzunehmen und somit eine Eigentumsverletzung gegeben. Auch die Folgen eines DDos-Angriffes führen in der Regel zu Störungen und Überlastungen von Servern und Netzwerken.

bb. Eigentumsverletzung bei Löschung und Veränderung von Daten

Wesentlich öfter als Hardwareschäden oder Störungen des Gesamtsystems löschen oder verändern Schadprogramme Daten. Sachen im Sinne des § 90 BGB sind körperliche Gegenstände. Sie müssen im Raum abgrenzbar sein.[74] Daten sind Informationen, die bearbeitet und übertragen werden.[75] Sie sind, für sich allein, nicht im Raum abgrenzbar und stellen damit keine körperlichen Gegenstände dar. Sie sind somit grds. keine Sachen im Sinne des § 90 BGB.[76] Ihrer Natur nach sind sie aber grds. in irgendeiner Form gespeichert, da man sie ansonsten auch nicht abrufen oder löschen könnte. So werden Daten im Arbeitsspeicher i. d. R. kurzfristig und auf Festplatten langfristig gespeichert. In Rechtsprechung und Literatur überwiegt die Ansicht, dass Daten immer dann eigentumsrechtlichen Schutz genießen sollen, wenn sie auf einem Datenträger verkörpert sind.[77] Es wird darauf hingewiesen, dass

---

[73] *Libertus*, NJW 2005, S. 507 (508); *Schneider/Günther*, CR 1997, S. 389 (390)
[74] *Heinrichs*, in: Palandt, § 90, Rn. 1.
[75] *Klußmann*, S. 214.
[76] LG Konstanz, NJW 1996, S. 2662; *Heinrichs*, in: Palandt, § 90, Rn. 2.
[77] BGH, NJW 1993, S. 2436 (2437 f.); OLG Karlsruhe, NJW 1996, S. 200 (201); OLG Stuttgart, NJW 1989, S. 2635 (2336); a. A. LG Konstanz, NJW 1996, S. 2662;

durch die magnetische Speicherung auf der Festplatte eine Verkörperung der Daten im Material vorhanden sei.[78] Mit Hilfe einer Magnetlupe ließen sich die gespeicherten Daten auch optisch ablesen. Veränderungen durch die Speicherung von Daten seien körperlich-gegenständlich messbar. Nach der Löschung sei der Datenträger anders als vorher. Zumindest aber sei der Datenträger in seiner Nutzung beeinträchtigt.[79] Die Gegenansicht versteht Daten, ob im Arbeitspeicher oder auf einer Festplatte gespeichert, als elektrische Spannungen, die, da sie nicht in einem der drei Aggregatzustände (fest, flüssig, gasförmig) auftreten, kein Eigentum darstellen können.[80]

Die zweite Ansicht verkennt, dass Daten ihrer Natur nach nur in Speichermedien verkörperter Form auftreten können. Sind sie nicht auf einem Datenträger oder zumindest im Arbeitspeicher gespeichert, sind sie im betreffenden System nicht existent. Enthält der Datenträger keine Daten ist seine Nutzung eingeschränkt. Daten machen eine den Datenträger bestimmende Eigenschaft aus, da ohne sie eine essentielle Funktion nicht ausgeführt werden kann. Werden Daten gelöscht, liegt somit zumindest eine nicht nur kurzfristige Nutzungsbeeinträchtigung des Datenträgers vor, da die Wiederherstellung bzw. Neubeschaffung der Daten in der Regel nicht unverzüglich möglich ist. Ob die Daten sich körperlich-gegenständlich im Datenträger festsetzen ist irrelevant, da nicht auf den letzten Stand der physikalischen Wissenschaft, sondern auf die Verkehrsanschauung abzustellen ist.[81] Im Ergebnis ist der ersten Meinung zu folgen. Daten, die auf Festplatten, Disketten oder Cds gespeichert werden, sind aufgrund der notwendigen Verbindung mit Speichermedien in Datenträgern verkörperte eigentumsrechtlich zu schützende Rechtsgüter.

Hager, in: Staudinger, § 823, Rn. B 60; *Wagner*, in: MüKo/BGB, § 823, Rn. 96; *Heinrichs*, in: Palandt, § 90, Rn. 2; *Koch*, NJW 2004, S. 802 f; *Taeger*, S. 261.

[78] Ausführlich *Meier/Wehlau*, NJW 1998, S. 1588.

[79] BGH, NJW 1993, S. 2436 (2437 f.); OLG Karlsruhe, NJW 1996, S. 200 (201); OLG Stuttgart, NJW 1989, S. 2635 (2336).

[80] LG Konstanz, NJW 1996, S. 2662; *Gerstenberg*, NJW 1956, S. 540.

[81] *Heinrichs*, in: Palandt, BGB, § 90, Rn. 1.

Fraglich ist, ob die Speicherung im Arbeitsspeicher eine Verkörperung von Daten darstellt. Im Arbeitsspeicher werden Daten i. d. R. nur flüchtig gespeichert.[82] Mit der Unterbrechung der Stromzufuhr werden die Daten aus dem Arbeitspeicher gelöscht. Nun gibt es mittlerweile neben dem flüchtigen Arbeitsspeicher auch nicht flüchtige Arbeitsspeicher, z. B.NVRAM[83] oder MRAM[84], der bei Stromunterbrechungen nicht die in ihm gespeicherten Daten verliert.[85] Diese Art Arbeitsspeicher kann demnach auch Daten so speichern, dass man von einer Verkörperung ausgehen kann. Folglich müssen Daten, die in nicht flüchtigem Arbeitsspeicher gespeichert werden, genauso behandelt werden wie im Rahmen der Festplattenspeicherung. Die Speicherung im flüchtigen Arbeitsspeicher genügt diesen Anforderungen nicht,[86] da Daten dort regelmäßig nur zwischengespeichert werden und eine auf Dauer angelegte Verkörperung ausscheidet. Diese Wertung ergibt sich auch aus einer das Urheberrecht betrachtenden und vergleichenden Sichtweise. Dort werden Speicherungen im Arbeitsspeicher nicht als zu sanktionierendeVervielfältigungen qualifiziert, da es an dauerhafter körperlicher Festlegung mangelt (vgl. §§ 44a UrhG).[87] Eine Eigentumsverletzung scheidet in diesem Fall zumindest aus, wenn mit der h. M. die Verkörperung auf einem Datenträger vorausgesetzt wird.[88]

c. Sonstige Rechte

aa. Recht am eingerichteten und ausgeübten Gewerbebetrieb

Die Weiterverbreitung von Malware könnte einen Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb darstellen. Dies kommt nur in Frage, wenn man mit der Mindermeinung[89] Datenveränderung

---

[82] *Klußmann*, S. 54.
[83] Non Volatile Random Access Memory.
[84] Magnetic Random Access Memory.
[85] *Hellwagner*, in: Rechenberg/Pomberger, S. 332 f.; *IT-Systemtechnik* (zuletzt abgerufen: 12.08.2006); *Janssen* (zuletzt abgerufen: 12.08.2006); *Trepte* (zuletzt abgerufen: 12.08.2006).
[86] *Meier/Wehlau*, NJW 1998, S. 1588; LG Konstanz, NJW 1996, S. 2662.
[87] OLG München, MMR 2006, S. 162 (163).
[88] *Wagner*, in: MüKo/BGB, § 823, Rn. 96.
[89] LG Konstanz, NJW 1996, S. 2662; *Gerstenberg*, NJW 1956, S. 540 – 540.

bzw. –löschung nicht schon als Eigentumsverletzung qualifiziert, da dieses Recht als Auffangtatbestand nur subsidiär Anwendung findet.[90] Betriebsbezogene gespeicherte Daten gehören zum Gegenstand des Gewerbebetriebs,[91] wobei sowohl die Daten selbst und ihre Verfügbarkeit, als auch Vertraulichkeitsverletzungen der Daten einen Eingriff darstellen.[92] Die Rechtsprechung fordert zudem, dass der Eingriff betriebsbezogener Natur ist.[93] Nach einer Ansicht fehle es bei fahrlässiger Datenlöschung an der Betriebsbezogenheit, da der Eingriff willentlich auf eine Betriebslaufstörung gerichtet sein müsste.[94] Bei unbeabsichtigter Weiterverbreitung von Malware käme nur Fahrlässigkeit in Betracht, so dass keine Betriebsbezogenheit vorliegen würde und folglich eine Verletzung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb ausschiede. Betriebsbezogenheit ist nicht in dem Sinne zu verstehen, dass Vorsatz oder Finalität erforderlich wäre.[95] Die Handlung muss sich in seiner objektiven Stoßrichtung gegen den Gewerbebetrieb richten.[96] Daher kann die unbeabsichtigte Weiterverbreitung von Malware einen betriebsbezogenen Eingriff darstellen. Darunter fällt Spam schon bei der ersten unverlangten Zusendung.[97] Insbesondere durch (D)Dos-Angriffe verursachte Systemüberlastungen sind im Rahmen des Rechts am eingerichteten und ausgeübten Gewerbebetrieb als Eingriffe anzusehen, wenn mangels Eigentumsverletzung ein Rückgriff auf das Recht am Unternehmen zulässig ist. Eine Eigentumsverletzung wird bei (D)Dos-Angriffen doch zumeist in einer Störung des Gesamtsystems bzw. am Server zu sehen sein,[98] so dass dafür hier kein Raum bleibt.

---

[90] *Beater*, in: Soergel, § 823, Anh V, Rn. 1; *Hager*, in: Staudinger, § 823, Rn. D 20; *Schiemann*, in Erman, § 823, Rn. 61.
[91] *Sprau*, in: Palandt, § 823, Rn. 127.
[92] *Koch*, NJW 2004, S. 803.
[93] Seit BGHZ 29, S. 65 (74) ständige Rspr.
[94] BGH, NJW 1981, S. 2416; *Wehlau*, OLGR 2004, K 27 (29); *Meier/Wehlau*, NJW 1998, S. 1585 (1589).
[95] *Schiemann*, in: Erman, § 823, Rn. 63.
[96] *Hager*, in Staudinger, § 823, Rn. D 11.
[97] OLG Düsseldorf, MMR 2004, S. 820 f.
[98] S. o. C., I., 1., b., aa.

bb. Allgemeines Persönlichkeitsrecht

Durch Trojanische Pferde und Spyware können vertrauliche Daten an Dritte weitergeleitet und ausspioniert werden. Dies könnte eine Verletzung des Allgemeinen Persönlichkeitsrechts als sonstiges Recht im Sinne des § 823 Abs. 1 BGB darstellen. Dieses Recht schützt unter anderem die Privatsphäre[99] und das Recht auf Selbstbestimmung.[100] Es schützt davor, dass sich Dritte unbefugt die Kenntnis von Informationen verschaffen können.[101] Das intellektuelle Selbstbestimmungsrecht schützt im Rahmen von § 823 Abs.1 BGB nur vertrauliche Daten i. S. d. des Rechts auf informationelle Selbstbestimmung.[102] Werden nicht persönliche Daten gelöscht, verändert oder versteckt, ist der Schutzbereich verlassen.[103]

cc. Recht am eigenen Datenbestand

Um den Schutz von Daten den heutigen Entwicklungen der Informationsgesellschaft anzupassen, wird in der Literatur teilweise die Anerkennung des Rechts am eigenen Datenbestand als sonstiges Recht im Sinne des § 823 Abs. 1 BGB gefordert.[104] Der Schutz von Daten über den Eigentumsbegriff sei nicht ausreichend, wenn der Nutzer der Daten und der Eigentümer des Speichermediums auseinander fallen.[105] Wird ein Speichermedium gemietet oder geleast, werden Datenbestände ausgelagert bzw. webbasiert bei anderen Unternehmen gespeichert, käme ein direkter Anspruch des Nutzers bei Datenverlust oder -beschädigung aus § 823 Abs. 1 BGB nicht in Betracht.[106] Kommt es in dieser Konstellation zu einem Schaden, so hat der Nutzer der Daten den Schaden, aber keinen Anspruch. Andererseits hat der Eigentümer des Speichermediums einen Anspruch, aber keinen Schaden. Es käme folglich ein Schadensersatzanspruch des Nutzers nur im Wege der

---

[99] *Beater*, in: Soergel, § 823, Anh IV, Rn. 42 ff.; *Kötz/Wagner*, Rn. 394.
[100] *Beater*, in: Soergel, § 823, Anh IV, Rn. 71 ff.
[101] *Beater*, in: Soergel, § 823, Anh IV, Rn. 92.
[102] BVerfG, NJW 2006, S. 976 (978).
[103] *Faustmann*, VuR 2006, S. 260 (262).
[104] *Wehlau*, OLGR 2004, K 27 ff.; *Faustmann*, VuR 2006, S. 260 (262 f.); *Meier/Wehlau*, NJW 1998, S. 1585 (1588); *Wuermeling*, CR 1994, S. 585 (590).
[105] *Wehlau*, OLGR 2004, K 27 (29); *Faustmann*, VuR 2006, S. 260 (262 f.).
[106] *Wehlau*, OLGR 2004, K 27 (29).

Drittschadensliquidation in Betracht. Dieser sei aber zum einen vom Eigentümer des Speichermediums abhängig und zum anderen können der Standort des Nutzers und der Standort des Speichermediums im Rahmen der globalen Vernetzung weit auseinander fallen, so dass sich Durchsetzungsprobleme ergeben würden.[107] Die h. M. vertritt die Auffassung, dass sich das Recht am eigenen Datenbestand inhaltlich nicht in seinem Schutzbereich definieren ließe,[108] und dass der Eigentumsschutz für den Datenträger ausreiche.[109] Des Weiteren könne sich der Geschädigte durch regelmäßige Datensicherung vor Datenverlusten schützen.[110].

d. Stellungnahme

Durch die Entwicklungen der Informationstechnologie werden Daten immer mehr zu einem wirtschaftlichen Gut. Die ansteigende Anzahl an Viren, Trojanischen Pferden und insbesondere Würmern haben ein gesamtwirtschaftliches Gefahrenpotenzial erzeugt durch das Dateninteggrität, Datenverfügbarkeit und Datensicherheit einer wesentlich größeren Bedrohung unterliegen als noch vor einigen Jahren. Durch Outsourcing[111] werden Nutzerdaten oftmals auf webbasierten Speichermedien gesichert.[112] Das Speichermedium ist dann nicht Eigentum des Datennutzers. Tritt ein Schaden am Datenbestand ein, würde dem Datennutzer kein Schadensersatzanspruch aufgrund einer Eigentumsverletzung zustehen. Dies wäre die Folge, wenn man mit der h. M. in Rechtsprechung und Literatur nur auf die Funktionsfähigkeit des Datenträgers abstellt und ein Recht am eigenen Datenbestand ablehnt. Die Argumente der h. M. sind nicht überzeugend. Das Argument, dass der Schutz des Datenträgers ausreiche, wird durch die Fälle der Trennung von Datenträgereigentum und Datennutzung widerlegt.[113] Durch Datensicherung werden Datenverluste verhindert. Weshalb ein Recht

---

[107] *Wehlau*, OLGR 2004, K 27 (29).
[108] *Wagner*, in: MüKo/BGB, § 823, Rd. 96.
[109] *Hager*, in: Staudinger, § 823, Rn. B 192.
[110] *Wagner*, in: MüKo/BGB, § 823, Rn. 96.
[111] Ausführlich zum Outsourcing von Daten siehe *Gliss*, DSB 6/2001, S. 6.
[112] Ausführlich *Wehlau*, OLGR 2004, K. 27 (29).
[113] *Wehlau*, OLGR 2004, K 27 (30).

am eigenen Datenbestand daher nicht nötig sei, ist nicht einleuchtend. Würde man dem folgen, dürften auch Daten nicht auf Datenträgern im Sinne des Eigentums geschützt werden, da auch in diesem Falle stets die Möglichkeit der Datensicherung besteht. Folge wäre, dass Daten überhaupt keinem deliktsrechtlichen Schutz unterliegen würden. Schließlich ist auch nicht die Gefahr einer ausufernden Schutzbereichsbestimmung gegeben. So könnte man den Schutzbereich des Rechts am eigenen Datenbestand wie folgt definieren: „Das Recht am eigenen Datenbestand umfasst die unkörperlichen elektronisch gespeicherten Daten und Informationen in ihrem Bestand als für den Verfügungsberechtigten jederzeit zugängliche und zur Weiterverarbeitung geeignete Information".[114] Es wäre zudem widersprüchlich die Schutzbedürftigkeit von Daten hier zu verneinen, während der Gesetzgeber den Schutz im Strafrecht durch Hinzufügen neuer Straftatbestände in den §§ 202a, 303a und 303B StGB als angemessen angesehen hat.[115] Zusammenfassend betrachtet wird man der heutigen Bedeutung von Daten nur gerecht, wenn sich der deliktsrechtliche Schutz dem Gefahrenpotenzial durch Malware und der sich fortentwickelnden Informationsgesellschaft anpasst. Der Schutz des Rechts am eingerichteten und ausgeübten Gewerbebetrieb reicht für die heutigen Anforderungen an effektiven Rechtsschutz vor Datenbeeinträchtigungen nicht aus. Es ist nicht einzusehen, dass die Haftung bezüglich Datenverlusten gegenüber Unternehmen anders zu beurteilen ist als bei privaten Nutzern.[116] Das Allgemeine Persönlichkeitsrecht ist in seinem Schutzbereich zu beschränkt um Malwareschäden umfassend abzudecken. Die Anerkennung des Rechts am eigenen Datenbestand stellt eine logische Konsequenz der Entwicklung der globalen Vernetzung dar.

---

[114] *Wehlau*, OLGR 2004, K 27 (31).
[115] Ähnlich *Faustmann*, VuR 2006, S. 260 (263).
[116] Vgl. *Wuermeling*, CR 1994, S. 585 (590).

2. Das Korrektiv der Verkehrspflichten zur Bestimmung der Zurechenbarkeit

Bei Unterlassungen und mittelbaren Verletzungen bedarf es über die Feststellung der Rechtsgutverletzung hinaus zusätzlich eines Verstoßes gegen Verkehrspflichten.[117] Bei der unbeabsichtigten Weiterverbreitung von Malware kann die Verletzung deliktsrechtlich geschützter Rechtsgüter auf unterschiedliche Weise geschehen. Zunächst kann der Internet-Nutzer unbeabsichtigt Viren, Trojanische Pferde etc. via E-Mail verschicken. Wird das System des Empfängers infiziert, kann das Verhalten des Versenders als aktives Tun qualifiziert werden, da er die E-Mail versandt hat. Auch ein Unterlassen kann angenommen werden, wenn auf den nicht erfolgten Virenschutz abgestellt wird.[118] Bewertet man das Verschicken der E-Mail als aktives Tun, so wird in der Verletzung des Rechtsguts nur eine mittelbare Verletzung zu sehen sein. Das Versenden führt grds. nicht unmittelbar zu einem Verletzungserfolg. Erst durch das Hinzukommen weiterer Ursachenbeiträge, z. B. durch die Schutzmaßnahmen und die Anfälligkeit des Empfängersystems gegenüber Malware, das Betriebssystem an sich und das Verhalten des Empfängers bei eingehenden E-Mails, wird die Verletzung konkretisiert. Die Verletzung durch Zusendung einer infizierten Mail durch den unwissenden Versender ist demnach entweder als Unterlassung des Virenschutzes oder als mittelbare Verletzungshandlung zu bewerten. In dieser Konstellation kann nicht nur auf das Unterlassen des Virenschutzes abgestellt werden, so wie teilweise in der Literatur behauptet.[119] Da es sich im Rahmen einer Unterlassung bzw. einer mittelbaren Verletzung um die gleiche Zurechnungsfrage handelt, ist eine Abgrenzung aber grds. nur von theoretischer Bedeutung.[120] Darüber hinaus kann der Verletzungserfolg durch sich selbst

---

[117] *Hager*, in: Staudinger, § 823, Rn. E 3; *Schiemann*, in: Erman, § 823, Rn. 77 f.; *Sprau*, in: Palandt, § 823, Rn. 45; Bar, S. 154 ff.; *Raab*, JuS 2002, S. 1041 (1042); *Deckert*, Jura 1996, S. 348 (349).
[118] So *Koch*, NJW 2004, S. 801 (802).
[119] So z. B. *Koch*, NJW 2004, S. 801 (802); Wohl auch *Schmidtbauer* (zuletzt abgerufen: 12.08.2006).
[120] *Hager*, in: Staudinger, § 823, Rn. E 3; *Schiemann*, in: Erman, § 823, Rn. 78; Raab, JuS 2002, S. 1041 (1042).

verschickende Würmer oder durch die Zugehörigkeit zu einem Botnetz bzw. als Teil einer Denial of Service-Attacke entstehen. Ein aktives Tun liegt dabei nicht vor. Die Verletzung des Empfängers ist dem (vermeintlichen) Versender lediglich aufgrund der Unterlassung des Betreibens effektiver Virenschutzmaßnahmen zurechenbar. Bei der unbeabsichtigten Weiterverbreitung von Malware ist daher neben der Rechtsgutverletzung zu prüfen, ob der Schädigende Verkehrspflichten verletzt hat.

a. Die Begründung von Verkehrspflichten

Es besteht grds. keine allgemeine Rechtspflicht, einen Dritten vor Schäden an einem der geschützten Rechtsgüter des § 823 Abs. 1 BGB zu bewahren.[121] Daher kann der in einem seiner Rechtsgüter Verletzte den Anderen bei Unterlassung oder mittelbarer Verletzung nur in Anspruch nehmen, wenn dieser die Schädigung durch eine übermäßige Gefährdung als Folge der Vernachlässigung einer Verkehrspflicht konkretisiert hat.[122] Verkehrspflichten werden durch die Schaffung einer Gefahrenlage, die Beherrschung einer Gefahrenquelle und die Übernahme einer rechtsgüterschützenden Aufgabe begründet.[123]

aa. Schaffung einer Gefahrenlage

Die Haftung für die Schaffung einer Gefahrenlage trifft den Verursacher der Gefahr, der die Lage herbeigeführt hat und in seinem Einflussbereich andauern lässt.[124] Auch die Vergrößerung einer Gefahr soll ausreichen.[125] Grds. hat der Programmierer der Malware die Gefahr geschaffen, dass Dritten Schäden entstehen. Der Internet-Nutzer, der unwissentlich Malware auf seinem System belässt, diese via E-

---

[121] RGZ 97, S. 11 (12); BGHZ 9, S. 301 (307); BGH, NJW 1991, S. 418 (419); *Wagner*, in Müko/BGB, § 823, Rn. 227; *Sprau*, in: Palandt, § 823, Rn. 46.
[122] *Sprau*, in: Palandt, § 823, Rn. 46.
[123] *Hager*, in: Staudinger, § 823, Rn. E 12 ff.; *Wagner*, in: MüKo/BGB, § 823, Rn. 223; *Schiemann*, in: Erman, § 823, Rn. 79; *Raab*, JuS 2002, S. 1041 (1044); *Larenz*/Canaris, § 76 III 3.
[124] BGHZ 5, S. 378 (380 f.); BGH, NJW 1990, S. 1236 (1237); *Hager*, in: Staudinger, § 823, Rn. E 13.
[125] *Hager*, in: Staudinger, § 823, Rn. E 13.

Mail etc. weiterverbreitet, ist dennoch zumindest für die Vergrößerung der Gefahr verantwortlich. Denn jede Weiterverbreitung erhöht die bestehende Gefährdungslage.[126] Er schafft konkrete Gefahren für Dritte. Im Falle sich selbst verbreitender Malware ist keine aktive Herbeiführung der Gefährdungslage durch den Inter-Nutzer gegeben. Sie kann aber durch die Aufnahme von Kontaktadressen ins Adressbuch des E-Mail-Accounts geschaffen werden,[127] infolgedessen sich z. B Würmer bei Systemstart selbst verschicken können.

bb. Beherrschung einer Gefahrenquelle

Eine Verkehrspflicht kann zudem durch die Verantwortung für den Zustand des eigenen Bereichs und den daraus resultierenden beherrschbaren Gefahren begründet werden.[128] Dabei ist nicht zu berücksichtigen, durch wen die Gefahr geschaffen wurde.[129] Wird die Gefahr durch einen Dritten begründet, haftet im Rahmen der Beherrschung einer Gefahrenquelle auch der für den Bereich zuständige,[130] da es gerade nicht um die Schaffung einer Gefahr, sondern um deren Beherrschung geht. Vermeintliche von der Gefahrenquelle ausgehende Gefahren müssen kontrolliert werden, um Schäden fremder Rechtsgüter zu verhindern.[131] Ein mit Malware infiziertes Computersystem ist aufgrund der heute durch das Internet gegebenen Verbreitungswege als Gefahrenquelle einzustufen. Aufgrund der exponentiellen Verbreitung[132] von Malware in den letzten Jahren ist bereits jedes mit dem Internet verbundene und ungeschützte System als Gefahrenquelle anzusehen. Ob Malware sich selbst verbreitet oder durch den Nutzer aktiv versendet wird, spielt im Rahmen der Qualifizierung als Gefahrenquelle keine Rolle.[133]

---

[126] So auch *Koch*, NJW 2004, S. 801 (803)
[127] Vgl. *Schmidtbauer* (zuletzt abgerufen: 12.08.2006).
[128] BGH, NJW 1994, S. 3348; BGH, NJW-RR 1990, S. 409 (410); *Hager*, in: Staudinger, § 823, Rn. E 16; *Raab*, JuS 2002, S. 1044.
[129] *Hager*, in Staudinger, § 823, Rn. E 17.
[130] *Hager*, in Staudinger, § 823, Rn. E 17.
[131] *Koch*, NJW 2004, S. 801 (803).
[132] *BSI*, Die Lage der IT-Sicherheit in Deutschland 2005, S. 19 ff. (zuletzt abgerufen: 12.08.2006).
[133] A. A. *Koch*, NJW 2004, S. 801 (803).

cc. Zwischenergebnis

Im Rahmen der Nutzung von E-Mail- und Internetdiensten sind im Umgang mit Schadprogrammen Verkehrspflichten zu beachten, da die Gefahr der Verbreitung besteht. Verkehrspflichten entstehen hier aufgrund der Zuordnungskriterien der Schaffung einer Gefahrenlage und der Beherrschung einer Gefahrenquelle. Bei sich selbst verbreitender Malware kann die Gefahrenlage schon in einem früheren Stadium eintreten. Verkehrspflichten, die durch die Übernahme einer rechtsgüterschützenden Aufgabe begründet werden, sind hier nicht ersichtlich. Im Folgenden soll der Inhalt und Umfang der Verkehrspflichten erarbeitet werden, der im Umgang mit Malware zu erwarten ist.

b. Inhalt und Umfang der Verkehrspflichten

Inhalt und Umfang von Verkehrspflichten werden durch die legitimen Erwartungen des Verkehrs bestimmt.[134] Der Verkehrssicherungspflichtige muss die Maßnahmen ergreifen, „die ein verständiger und umsichtiger, in vernünftigen Grenzen vorsichtiger Mensch für notwendig und ausreichend hält, um andere vor Schaden zu bewahren“.[135] Infolgedessen ist das Verhalten des Verkehrspflichtigen in Konkordanz mit dem Ausmaß drohender Schäden und der Wahrscheinlichkeit des Schadenseintritts zu bringen.[136] Darüber hinaus ist die Möglich- und Zumutbarkeit der Vermeidung durch den Verkehrspflichtigen, die Selbstschutzmöglichkeiten des Geschädigten und der Gedanke des Vertrauensschutzes im Rahmen einer wertenden Interessenabwägung in die Bewertung mit einzubeziehen.[137]

---

[134] BGH, NJW 2002, S. 1263 (1264); 1994, S. 3348 (3349); 1985, S. 1076; *Hager*, in: Staudinger, § 823, Rn. E 27; *Koch*, NJW 2004, S. 801 (804).
[135] BGH, NJW 1990, S. 1236 (1237).
[136] BGH, VersR 1960, S. 609 (611); *Wagner*, in: MüKo/BGB; § 823, Rn. 249; *Larenz*/Canaris, § 76 III 4 b.
[137] *Wagner*, in: MüKo, § 823, Rn. 248 ff.; *Koch*, NJW 2004, S. 801 (804 f.).

aa. Das Ausmaß des drohenden Schadens und die Wahrscheinlichkeit des Schadenseintritts

Das Ausmaß des Schadens kann bei Malwarebefall variieren. Löscht ein Virus Datenbestände kann es zu größeren finanziellen Schäden kommen als bei Hardwareschäden. Werden Daten gelöscht, beschädigt, versteckt oder ausspioniert, kommt es auf die Art der Daten an. Es macht einen Unterschied, ob die letzten Urlaubsfotos gelöscht oder ob wichtige Geschäftsunterlagen, Kontozugangsinformationen, Passwörter oder ähnliches nicht mehr verfügbar sind bzw. ausspioniert wurden. Die Wahrscheinlichkeit Opfer von Schadprogrammen zu werden ist kontinuierlich gestiegen.[138] Ohne die Nutzung von Anti-Maleware-Programmen ist die Wahrscheinlichkeit, dass ein System infiziert wird, als sehr hoch einzuschätzen.

bb. Möglichkeit und Zumutbarkeit von Gefahrabwendungsmaßnahmen

Ist ein Schadprogramm aufgrund seiner Neuheit von Anti-Malware-Programmen nicht erkennbar, gibt es mangels Verhinderungsmöglichkeit keine Verkehrspflicht den Schaden abzuwenden.[139] Es ist auf einen objektiven Maßstab abzustellen.[140] Es ist nicht entscheidend, dass der Verkehrspflichtige die Gefahr erkannt hat.[141] Entscheidend ist, ob die Bedrohung mit einem gängigen Schutzprogramm hätte abgewehrt werden können. Die faktischen und rechtlichen Handlungsmöglichkeiten müssen vom Verkehrspflichtigen wahrgenommen werden.[142] Allerdings wird keine absolute Sicherheit verlangt, wonach Rechtsgutverletzungen vollends ausgeschlossen werden können.[143] Absolute Sicherheit vor Malwareschäden kann es mit Schutzprogrammen nicht geben, da die Programmierer von Schadprogrammen den Programmierern der Schutzprogramme stets einen Schritt voraus

---

[138] S. o. A., B.
[139] LG Köln, NJW 1999, S. 3206.
[140] *Hager*, in: Staudinger, § 823, Rn. E 30.
[141] *Hager*, in: Staudinger, § 823, Rn. E 30.
[142] BGH, VersR 1985, S. 641 (642); *Wagner*, in: MüKo/BGB, § 823, Rn. 248.
[143] BGH, VersR 1975, S. 812; *Wagner*, in: MüKo/BGB, § 823, Rn. 248; *Schiemann*, in: Erman, § 823, Rn. 80.

sind.[144] Maßnahmen zur Erfüllung von Verkehrspflichten müssen nicht dem empirisch-technisch möglichen Stand der Technik entsprechen.[145] Zu verlangen sind Schutzmaßnahmen, die innerhalb der Grenzen der Zumutbarkeit liegen.[146]

(1) Möglichkeit und Zumutbarkeit des Einsatzes von Schutzprogrammen

Durch die Installation von Virenschutzprogrammen, Anti-Spyware-Software, Firewalls etc. können Internet-Nutzer einen Großteil der bestehenden Malwarerisiken vermeiden. Die Zumutbarkeit von Verkehrspflichten wird grds. auch durch den wirtschaftlichen Aufwand mitbestimmt.[147] Privatpersonen können z. B. Antiviren-Software inklusive Update-Funktionen gratis oder zu geringen Preisen im Internet erwerben.[148] Im Unternehmensbereich sind die Preise je nach Unternehmensgröße bzw. Anzahl der Workstations konzipiert.[149] Die Preise sind im Vergleich mit den eventuellen Schäden als angemessen zu betrachten.[150] Dabei wird man je nach Größe des Unternehmens, dem E-Mail-Aufkommen und der Internetnutzung höhere oder niedrigere Anforderungen an die Höhe der Ausgaben für Schutzsoftware anlegen müssen. Zumindest die Anschaffung von Anti-Viren-Software ist zumutbar und kann von Internet-Nutzern grds. erwartet werden.[151]. Die Möglichkeit der Versicherbarkeit kann Einfluss auf die Maßstäbe haben, nach welchen die Zumutbarkeit bestimmt wird.[152] Es gibt vereinzelt erweiterte Softwareversicherungen, die durch Malware entstande-

---

[144] S. o. B., VIII.
[145] BGH, NJW 1989, S. 2808 f.; 1965, S. 1760 f.; *Wagner*, in: Staudinger, § 823, Rn. 248.
[146] BGH, NJW 1990, S. 1236 (1237); 1989, S. 2808 f.; *Wagner*, in: Staudinger, § 823, Rn. 248; *Schiemann*, in: Erman, § 823, Rn. 80.
[147] Vgl. *Wagner*, in: MüKo/BGB, § 823, Rn. 249; *Schiemann*, in: Erman, § 823, Rn. 81.
[148] *Landesman* (zuletzt abgerufen: 12.08.2006); Vgl. auch Avira, http://www.free-av.de/ (zuletzt abgerufen: 12.08.2006).
[149] Siehe z. B. http://www.avira.com/de/onlineshop/index.html (zuletzt abgerufen: 12.08.2006)
[150] Ca. 50 Euro kostet die Software für ein Jahr für eine Workstation, siehe z. B. Avira, http://www.avira.com/de/onlineshop/index.html (zuletzt abgerufen: 12. August 2006).
[151] So auch *Koch*, NJW 2004, S. 801 (804); *Spindler*, CR 2005, S. 741 (744).
[152] *Schiemann*, in: Erman, § 823, Rn. 81.

ne Schäden mitversichern.[153] Solch eine Versicherung kann unter Zumutbarkeitsgesichtspunkten von Privaten grds. nicht verlangt werden. Bezug nehmend auf die Verbreitungsmöglichkeiten von Malware macht es keinen Unterschied, ob Schadprogramme sich selbst verbreiten oder durch den Nutzer verbreitet werden. Entscheidend ist nur, dass die Möglichkeit besteht das Schadprogramm durch Schutzmaßnahmen zu erkennen. Ist es durch übliche Software erkennbar, ist der Schutz zumutbar und kann erwartet werden.

(2) Das Erfordernis der Aktualisierung von Schutzsoftware

Schutzsoftware ist nach einiger Zeit veraltet. Neue Malware kann ohne regelmäßige Aktualisierung nicht erkannt werden.[154] Schutzmaßnahmen gegen Malware entfalten keine Wirkung, wenn die Software nicht in regelmäßigen Abständen aktualisiert wird. Die Aktualisierung bzw. Update-Funktion von Anti-Viren-Software kann heute problemlos über das Internet vollzogen werden. Moderne Software kann durch Live-Updates aktualisiert werden, indem das Schutzprogramm selbständig Kontakt mit dem Internet aufnimmt und die neusten Updates installiert. Werden die Aktualisierungen manuell vorgenommen ist fraglich, in welchen Zyklen die Software aktualisiert werden muss. Wie bei der Bestimmung der zumutbaren Höhe der Ausgaben für Schutzsoftware,[155] ist bei Unternehmen nach der Größe, dem E-Mail-Aufkommen und der Internetnutzung, also nach dem Gefahrenpotenzial abzuwägen. Je größer das Gefahrenpotenzial, desto häufiger ist eine Aktualisierung zu verlangen. Grundsätzlich sind mindestens einmal die Woche die neusten Updates zu installieren.[156] Die regelmäßige Aktualisierung der Schutzsoftware kann mithin erwartet werden.[157]

---

[153] Für Private siehe HuK-Coburg, http://www.huk.de/produkte/recht_und_haftung/privathaftpflicht/internet_baustein.jsp (zuletzt abgerufen: 12.08.2006); Für IT-Dienstleister siehe VHV, http://www.vhv.de/web/Gewerbe/IT-Dienstleister/Elektronik /index.jsp (zuletzt abgerufen: 12.08.2006).
[154] Vgl. dazu *Mankowski*, in: Ernst, Rn. 452.
[155] S. o. C., I., 2., b, bb., 1.
[156] So auch *Libertus*, MMR 2005, S. 507 (510).
[157] Vgl. LG Hamburg, MMR 2001, S. 831.

(3) Begrenzung der Zumutbarkeit bei neuen Malwarearten

Bedenken gegenüber dieser Sorgfaltspflicht könnten sich aus der neueren Rechtsprechung in Bezug auf Dialer-Software[158] ergeben.[159] Hier wurde die Verantwortlichkeit für durch Dialer entstandene Schäden nicht von der Installierung eines Dialerschutzprogramms abhängig gemacht.[160] Dem unwissenden Nutzer von Dialer-Software könne die Benutzung eines Anti-Dialer-Programms nicht abverlangt werden.[161] Bezug nehmend auf diese Entscheidung wird die Installierung von Schutzsoftware für Backdoors ebenfalls als nicht zu erwartend angesehen.[162] Im Vergleich zu klassischen Schadprogrammen, wie Viren und Würmern, handelt es sich bei Dialern und Backdoors um vergleichsweise neuartige und in der Bevölkerung unbekannte Malware. Virenschutzprogramme gehören zum Standard jedes Computersystems und können als solche auch verlangt werden.[163] Es scheint angebracht, die Maßstäbe an die Internet-Nutzer daran zu messen, wie sich die Verbreitung des Risikobewusstseins für bestimmte Malwaretypen und dem Wissen über mögliche Gegenmaßnahmen entwickelt.[164] So wird man bei neu entwickelten Schadprogrammen, die in keine der üblichen Kategorien einzuordnen und bei einem Großteil der Internet-Nutzer unbekannt sind, grds. nicht verlangen können, dass entsprechende Schutzsoftware installiert ist. Das Bestehen der Verkehrspflicht wird somit an die Üblichkeit der Sicherheitsvorkehrungen gekoppelt.[165]

(4) Zwischenergebnis

Zusammenfassend betrachtet, ist es zumutbar und von Internet-Nutzern zu erwarten, Schutzsoftware zu installieren und regelmäßig

---

[158] S. o. B., VI.
[159] BGH, JZ 2004, S. 1124 (1127).
[160] Begrüßend *Mankowski*, MMR 2004, S. 312 f.
[161] BGH, JZ 2004, S. 1124 (1127); a. A. *Leible/Wildemann*, K&R 2004, S. 288 (289).
[162] LG Stralsund, MMR 2006, S. 487 (489).
[163] *Spindler*, JZ 2004, S. 1128 (1129).
[164] So auch *Spindler*, JZ 2004, S. 1128 (1129).
[165] BGH, VersR 1955, S. 82 (83); *Larenz*/Canaris, § 76 III 4 E.

zu aktualisieren. Dabei können von Systemen, die ein größeres Gefahrenpotenzial innehaben, höhere Anforderungen in Bezug auf die Zumutbarkeit im preislichen Bereich, als auch bei der Frage der Aktualisierungszyklen erwartet werden. Die Zumutbarkeit kann bei neuartigen Schadprogrammen reduziert sein und niedrigere Anforderungen an den Internet-Nutzer stellen. Auch hier ist das Gefahrenpotenzial des Systems mitentscheidend für die Bestimmung der zumutbaren Sicherheitsmaßnahmen.

c. Auswirkungen des Vertrauensschutzgedankens auf Verkehrspflichten

Da von jedem Internet- und E-Mail-Nutzer verlangt werden kann, dass Schutzsoftware installiert ist, trifft diese Verpflichtung nicht nur denjenigen, der Malware unbeabsichtigt weiterverbreitet, sondern auch den Geschädigten. Der Verbreitende kann sich darauf berufen, er sei davon ausgegangen, dass der Empfänger der Malware Schutzprogramme installiert habe, die einen Schaden hätten verhindern können. Man kann darauf vertrauen, dass der Andere die Gefahr erkennen und sich selbst schützen kann oder sich ihr erst gar nicht aussetzt.[166] Die Verkehrspflicht Schutzmaßnahmen zu ergreifen könnte sich daher reduzieren, wenn der Schadensgefahr durch Eigenmaßnahmen des Empfängers der Malware entgegenzuwirken wäre.[167] Die Pflicht zur Sicherung kann schon vor der Prüfung des Mitverschulden (§ 254 Abs. 1 BGB) reduziert werden. Dabei dürfe die Reduzierung der Verkehrspflichten nicht zu weit führen, da sonst für eine Verringerung der Schadensverantwortlichkeit im Wege des Mitverschuldens gemäß § 254 Abs. 1 BGB zu wenig Raum bliebe.[168] Schutzmaßnahmen sind dem Empfänger genauso zumutbar und von ihm zu verlangen wie vom Versender der Malware. Andererseits kann auch der Empfänger einwenden, er habe darauf vertraut, dass der Versender entsprechende

---

[166] BGH, LM Nr. 166 zu § 823 (Dc) unter II 1 c; *Hager*, in: Staudinger, § 823, Rn. E 32; *Wagner*, in: MüKo/BGB, § 823, Rn. 251; *Schiemann*, in: Erman, § 823, Rn. 80; *Edenfeld*, VersR 2002, S. 272 (277).
[167] *Koch*, NJW 2004, S. 801 (804).
[168] *Hager*, in: Staudinger, § 823, Rn. E 32.

Schutzmaßnahmen ergriffen habe. Im Rahmen der Bestimmung der Verkehrserwartung muss daher der Vertrauensschutzgedanke als Grundsatz der Gewährleistung eines bestimmten Sicherheitsstandards miteinbezogen werden.[169] Haben beide Seiten darauf vertraut, dass der jeweils andere den Verkehrserwartungen genügende Schutzmaßnahmen getroffen habe, ist entscheidend, welches Vertrauen schützenswerter ist.[170]

aa. Vertrauensschutz zugunsten des Schädigenden

Der Geschädigte soll im Rahmen der Anforderungen an eigene Selbstschutzmaßnahmen grds. einen Vertrauensvorsprung haben und einen Schadensabwälzungsbonus gegenüber dem Gefahrverursacher geltend machen können.[171] Im Rahmen des Schutzes vor Malware kann erwartet werden, dass der unwissende Verbreiter und der Geschädigte aufgrund der an sie gestellten Erwartungen des Verkehrs grds. die gleichen Sicherheitsvorkehrungen erfüllen Beide unterschreiten die im Internet erforderliche Sorgfalt, wenn sie keine Schutzsoftware installiert haben. Fraglich ist, ob dem durch Malware Geschädigten grds. ein Vertrauensvorsprung zugebilligt werden kann. Dagegen spricht, dass die Rollen des Schädigenden und des Geschädigten dem Zufall überlassen bzw. austauschbar sind,[172] wie z. B. bei Kraftfahrzeugnutzern im Straßenverkehr.[173] Im Fall der unbeabsichtigten Weiterverbreitung von Malware, z. B. durch E-Mail oder Instant Messenger-Nachrichten, sind die Rollen des Schädigenden und des Beschädigten austauschbar.[174] Instant Messenger-Programmen übertragen Nachrichten in Echtzeit, so dass die Rollen der Beteiligten ständig wechseln. Darüber hinaus hat der Versender der Schadprogramme keine Kenntnis über die Art und den Wert der Dateien, die auf dem System des Empfängers geschädigt werden können. Der Geschädigte kann das Schadensrisiko besser überblicken als der Malware-Verbreitende und

---

[169] *Wagner*, in: MüKo/BGB, § 823, Rn. 251; *Bar*, S. 117 ff.
[170] *Koch*, NJW 2004, S. 801 (804)
[171] *Steffen*, VersR 1980, S. 409 (411).
[172] *Koch*, NJW 2004, S. 801 (804); *Steffen*, VersR 1980, S. 409 (411).
[173] *Steffen*, VersR 1980, S. 409 (411).
[174] *Koch*, NJW 2004, S. 801 (804).

das Schadensrisiko durch sein Verhalten in Bezug auf Schutzmaßnahmen steuern.[175] Dem Geschädigten steht nur dann ein Vertrauensvorsprung zu, wenn er die Gefahr selbst bei Beachtung der von ihm zur erwartenden Sorgfalt nicht oder nicht früh genug erkennen und vermeiden konnte.[176] Sind wichtige Daten auf dem System, kann er sie durch entsprechende Software bzw. organisatorische Maßnahmen vor der Gefahr des Datenverlustes schützen. Computernutzern ist allgemein bekannt, dass durch Datenaustausch Viren übertragen werden können.[177] Daher ist ein Vertrauensvorsprung zugunsten des Empfängers im Rahmen der unbeabsichtigten Malwareverbreitung nicht anzuerkennen.

bb. Vertrauensschutzerwägungen im Rahmen unternehmerischer Tätigkeiten

Unternehmer und Private bzw. Verbraucher unterliegen teilweise anderen gesetzlichen Regelungen. Internet- und E-Mail-Dienste werden von Unternehmen in intensiverer Weise genutzt. Es ist daher zu prüfen, ob Unternehmer weitergehende Pflichten zu erfüllen haben als Private, und ob sich diese auf den Umfang der Verkehrspflichten auswirkt.

(1) Vorteilsziehung durch Nutzung von Computertechnologie

Die Verkehrserwartungen an den Umfang der Verkehrspflichten können durch die Vorteile, die aus den gefährdenden Umständen gezogen werden, beeinflusst werden.[178] Von demjenigen, der durch etwas einen Vorteil erlangt ist zu verlangen, dass er auf den Schutz fremder Rechtsgüter besonders Rücksicht nimmt. So wird angeführt, dass Unternehmen z. B. durch den Einsatz von E-Mail-Anwendungen erhebliche wirtschaftliche Vorteile hätten, da sie dieses Medium intensiver nutzen würden und sich größere Zugangsmöglichkeiten zu Kunden

---

[175] *Koch*, NJW 2004, S. 801 (804 f.)
[176] OLG Hamm, VersR 2003, S. 605; *Sprau*, in: Palandt, § 823, Rn. 51.
[177] Vgl. LG Köln, NJW 1999, S. 3206.
[178] BGH; LM Nr. 10 zu § 823 (Db); *Larenz*/Canaris, § 76 III 3a; *Raab*, JuS 2002, S. 1041 (1044 f.).

eröffneten.[179] Zudem würden sie im Bewusstsein, Opfer von Malware und daher mögliche Verbreiter zu werden handeln und dieses Risiko bewusst hinnehmen.[180] Daher sei eine Ungleichbehandlung von Privaten und Unternehmern i. S. d. § 14 Abs. 1 BGB vertretbar.[181] Unternehmer i. S. des § 14 Abs. 1 BGB können sowohl natürliche, als auch juristische Personen, sowie rechtsfähige Personengesellschaften sein. Im Unterschied zu § 1 HGB fallen unter den Unternehmerbegriff des BGB auch freie Berufe und Kleingewerbetreibende.[182] Ferner wird verlangt, dass am Markt planmäßig und dauerhaft Leistungen gegen ein Entgelt angeboten werden.[183] Unter den Unternehmerbegriff fallen auch öffentliche und gemeinnützige Unternehmen, die etwas entgeltlich anbieten.[184]

(2) Stellungnahme

Die Ungleichbehandlung von Privaten und Unternehmern kann zu unsachgerechten Ergebnissen führen. Ein Kleingewerbetreibender im Einzelhandel, ein Arzt oder ein Rechtsanwalt ist ebenso Unternehmer i. S. von § 14 Abs. 1 BGB, wie ein multinational operierendes Unternehmen wie Ebay. Die Unternehmer der ersten Kategorie nutzen Internet und E-Mail in der Regel nicht mehr als Privatnutzer. Eine überproportionale Vorteilsziehung im Vergleich zu Privaten ist zumeist nicht gegeben. Auf der anderen Seite wird bei großen Unternehmen, wie Ebay, ein Großteil der geschäftlichen Tätigkeit durch Internet- bzw. E-Mail-Anwendungen abgewickelt. Eine Ungleichbehandlung von Privaten und Unternehmen kann sich nicht nur auf den Unternehmensbegriff des § 14 Abs. 1 BGB stützen. Es ist im Einzelfall zu prüfen, ob der Unternehmer im Vergleich mit Privaten, Internet und E-Mail als wirtschaftlichen und einen Vorteil bringenden Faktor einsetzt. Eine Vorteilsziehung kann angenommen werden, wenn der Un-

---

[179] *Koch*, NJW 2004, S. 801 (805); *Formen*, S. 6 (zuletzt abgerufen: 12.08.2006).
[180] *Koch*, NJW 2004, S. 801 (805).
[181] *Koch*, NJW 2004, S. 801 (805); *Formen*, S. 6 (zuletzt abgerufen: 12.08.2006).
[182] *Saenger*, in: Erman, § 14, Rn. 2.
[183] *Saenger*, in: Erman, § 14, Rn. 9; *Heinrichs*; in Palandt, § 14, Rn. 2.
[184] *Micklitz*, in: Müko/BGB, § 14, Rn. 19.

ternehmer eine eigene Homepage betreibt, Newsletter versendet und E-Mail-Werbung einsetzt.

(3) Der Einfluss gesetzlicher und behördlicher Vorschriften

Gesetze, behördliche Empfehlungen und Unfallverhütungsvorschriften erzeugen für Unternehmen öffentlich-rechtliche Sicherheitsstandards, die die Anforderungen an die IT-Sicherheit im Unternehmen mitbestimmen. Private könnten aufgrund dieser Normen darauf vertrauen, dass Unternehmen die geforderten Standards erfüllen.[185] Diese Sicherheitsstandards dienen zwar nicht dem unmittelbaren Schutz Dritter, sie können aber zur Entwicklung von Sorgfaltsmaßstäben und zur Konkretisierung von Verkehrspflichten herangezogen werden, soweit es um Gefahren geht, vor denen sie schützen sollen.[186] Dies bedeutet nicht, dass Verkehrspflichten exakt öffentlich-rechtlichen Standards entsprechen müssen.[187] Die Normen bilden Mindeststandards,[188] die aufgrund der „Autonomie privatrechtlicher Sorgfaltspflichten“[189] einzelfallbezogen angehoben werden können. Öffentlich-rechtliche Sicherheitsstandards ergeben sich z. B. aus dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) i. V. m. dem AktG. Der durch Art. 1 Nr. 9 c KonTraG hinzugefügte Abs. 2 des § 91 AktG bestimmt, dass Überwachungssysteme zur Abwehr gefährdender Entwicklungen geschaffen werden müssen. Es muss eine Gefahr für den Fortbestand der Gesellschaft darstellen, wobei sich die Bestandsgefährdung auf die Vermögens-, Ertrags- oder Finanzlage wesentlich auswirken muss.[190] Durch Malware ist eine den Bestand bedrohende Gefährdung denkbar, insbesondere bei Infizierungen ganzer Netzwerke und der daraus resultierender Löschung von großen Datenbeständen. Aus § 91 Abs. 2 AktG ergibt sich daher eine Pflicht Anti-Malware-Software bzw. IT-Sicherheitskonzepte zu installieren.

---

[185] *Heidrich*, c´t 19 2004, S. 168; *Koch*, NJW 2004, S. 801 (805).
[186] BGH, NJW-RR 2003, S. 1459 (1460); BGH, NJW 2001; S. 2019 (2020); BayObLG, NJW-RR 2002, S. 1249 (1250); *Hager*, in: Staudinger, § 823, Rn. E 34; *Sprau*, in: Palandt, § 823, Rn. 51; *Koch*, NJW 2004, S. 801 (805).
[187] *Wagner*, in: MüKo/BGB, § 823, Rn. 269; *Larenz*/Canaris, § 76 III 4f.
[188] *Hager*, in: Staudinger, § 823, Rn. E 34.
[189] *Wagner*, in: MüKo/BGB, § 823, Rn. 270.
[190] *Hefermehl/Spindler*, in: MüKo/AktG, § 91, Rn. 16; *Hüffer*, AktG, § 91, Rn. 6.

Diese Verpflichtung wird zudem in Regel 4.1.4 des Deutschen Corporate Governance Kodex (DCGK)[191] verdeutlicht. Zudem soll für ein angemessenes Risikomanagement und –Controlling gesorgt werden (Regel 4.1.4). Des Weiteren ergibt sich aus § 9 Bundesdatenschutzgesetz (BDSG) i. V. m. der Anlage zu § 9 BDSG, dass organisatorische Maßnahmen zur Sicherstellung datenschutzrechtlicher Pflichten gewährleistet sein müssen. Dies umfasst die Schaffung eines IT-Sicherheitskonzepts und somit u. a. auch die Installierung von Anti-Malware-Programmen.[192] Für Unternehmen, die unter das Kreditwesengesetz (KWG) fallen, bestimmen die §§ 24c Abs. 6, 25a Abs. 1 Nr. 4 BDSG, dass den Stand der Technik entsprechende Vorkehrungen zu Sicherstellung der Vertraulichkeit und des Datenschutzes vorhanden sein müssen. Weitere datenschutzrechtliche Aspekte, die den Malwareschutz mit umfassen, finden sich in § 4 Abs. 4 Nr. 2-4 des Gesetzes über den Datenschutz bei Telediensten (TDDSG) in den Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)[193] (Abschnitt V.), in der Checkliste zur Abschlussprüfung bei Einsatz von Informationstechnologie,[194] sowie in Empfehlungen des Bundesbeauftragten für den Datenschutz..[195] Da Unternehmen durch zahlreiche Gesetzte, Empfehlungen usw. zur Einhaltung eines gewissen IT-Sicherheitsstandards berufen sind, ist ein Vertrauensvorsprung zugunsten Privater gerechtfertigt ist.

d. Zwischenergebnis

Das Ausmaß von Schutzmaßnahmen richtet sich nach dem Gefahrpotenzial, das von dem Verpflichteten ausgeht. Insoweit ist es für Private zumutbar günstige oder kostenfreie Schutzprogramme zu erwerben. Unternehmer haben dagegen je nach ihrer Größe und dem Ausmaß der Nutzung des Internets verhältnismäßig größeren Aufwand zur Siche-

---

[191] DCGK in der Fassung vom 12.06.2006, Elektronischer Bundesanzeiger, https://www.ebundesanzeiger.de (zuletzt abgerufen: 12.08.2006).
[192] Vgl. hierzu *Ernestus*, in: Simitis, § 9, Rn. 63; *Koch*, NJW 2004, S. 801 (805).
[193] BStBl 1995 I, S. 738.
[194] *IDW*, Checkliste, S. 1 ff.
[195] *BfD*, Datenschutzgerechtes eGovernment, S. 35 (zuletzt abgerufen: 12.08.2006).

rung ihrer Systeme bereitzustellen Neben der Installierung der entsprechenden Software kann ein IT-Sicherheits-Management einzurichten sein. Es ist dann nicht ausreichend Schutzprogramme zu installieren. Darüber hinaus können organisatorische, personelle und bauliche Maßnahmen zur Ausgestaltung eines umfassenden IT-Sicherheits-Konzepts erforderlich werden.[196]

Im Verhältnis zwischen Privaten (C2C[197]) reduziert sich die Verkehrspflicht aufgrund des Vertrauens in Sicherheitsmaßnahmen des Geschädigten soweit, dass die Haftung entfällt. Das gleiche gilt grds. im Verhältnis zwischen Unternehmern (B2B[198]). Dort kann der Vertrauensschutzgedanke aber nicht dazu führen, dass Unternehmer jeder Art gleich behandelt werden. Private haben gegenüber Unternehmern (B2C/C2B) einen Vertrauensvorsprung, beruhend auf dem Gedanken der Vorteilsziehung und aufgrund der Vertrauensprärogative gesetzlicher, behördlicher oder fachverbandlicher Normen und Empfehlungen. Wenn kleine Unternehmer keine besonderen Vorteile aus der Nutzung von Internettechnologie ziehen und nicht von den entsprechenden Normen erfasst werden, sind sie so zu behandeln wie Private. Deshalb steht ihnen gegenüber „großen" Unternehmen ein Vertrauensvorsprung zu. Zusammenfassend entsteht eine Haftung nur, wenn Unternehmen Malware an Private oder Unternehmen, die wie Private zu behandeln sind, weiterleiten.

II. Haftung aus § 823 Abs. 2 BGB i. V. m. Schutzgesetzen

Als Schutzgesetze i. S. v. § 823 Abs. 2 BGB kommen die §§ 202a, 303, 303a, 303b StGB,[199] 43 Abs. 2, 44 Abs. 1 BDSG, 17 Abs. 2 Nr. 1 a UWG in Frage. Bis auf § 43 Abs. 2 BDSG setzen alle Normen vorsätzliches Handeln voraus (vgl. § 15 StGB). Es bedürfte zumindest

---

[196] *Heckmann*, MMR 2006, S. 280 ff; *Heidrich*, c´t 19/2004, S. 168.
[197] Consumer to Consumer.
[198] Buisness to Buisness.
[199] Ausführlich dazu *Eichelberger*, MMR 2004, S. 594 ff.; *Ernst*, NJW 2003, S. 3233 ff.

eines billigenden Inkaufnehmens des Schadenseintritts. Bei der unbeabsichtigten Weiterverbreitung von Malware ist grds. nur ein Fahrlässigkeitsvorwurf denkbar,[200] da keine wissentlichen und voluntativen Elemente in Bezug auf die Tatbestandsverwirklichung vorliegen. Fraglich ist, ob durch die unbeabsichtigte Verbreitung von Malware gegen die Ordnungswidrigkeitsvorschrift des § 43 Abs. 2 BDSG verstoßen wird. Die Norm hat Verbotscharakter und schützt zumindest mittelbar individuelle Interessen. Die Vorschriften des BDSG sind als mögliche Schutzgesetze qualifiziert worden.[201] Geahndet wird in dieser Norm u. a. die unbefugte Verarbeitung (Nr.1). Eine Verarbeitung kann auch beim Löschen personenbezogener Daten vorliegen,[202] so dass durch Malware-bedingte Datenlöschung der objektive Tatbestand erfüllt scheint. Verbreitet sich ein Virus von einem System auf ein anderes, infiziert dort gespeicherte Daten und verändert sie, stellt sich die Frage, ob dem Schädiger dieser Geschehensablauf zugerechnet werden kann. Grundsätzlich kann jeder Täter sein, was durch das Wort „wer“ in § 43 Abs. 2 BDSG verdeutlicht wird.[203] Nach Rechtsprechung und Teilen der Literatur kann Schutz nach § 823 Abs. 2 BGB entbehrlich sein, wenn der Geschädigte anderweitig abgesichert ist und es sich lediglich um Ordnungswidrigkeiten handelt.[204] Der Geschädigte könnte gemäß § 43 Abs. 2 BDSG direkt gegen die Daten verarbeitende Stelle vorgehen. Ob die Anwendung des § 823 Abs. 2 BGB aus diesen Gründen zu versagen ist, kann offen gelassen werden, wenn schon der Schutzzweck der Norm die Anwendung ausschließt. Schutzzweck des § 43 Abs. 2 BDSG ist nicht, die Veränderung vertraulicher Daten durch unbeabsichtigte Malwareverbreiter zu sanktionieren. Vielmehr bezieht sich der Schutzzweck der Norm auf die Daten verarbeitende Stelle (vgl. auch § 1 Abs. 2 Nr. 3 BDSG) bzw. auf die automatische Datenverarbeitung.[205] Zu bedenken ist, dass mit Mal-

---

[200] Vgl. *Libertus*, MMR 2005, S. 507 (512).
[201] BGH, NJW 1981, S. 1738 (1740).
[202] *Dammann*, in: Simitis, § 43, Rn. 54.
[203] *Bestmann*, K&R 2003, S. 496 (497 f.).
[204] BGH, NJW 1980, S. 1792 (1793); *Hager*, in: Staudinger, § 823, Rn. G 6; *Schlosser*, JuS 1982, S. 659 (660).
[205] BTDrucks. 11/4306, S. 36 ff.; *Gola/Schomerus*, § 43, Rn. 3.

ware infizierte Systeme, die vertrauliche Daten speichern, gegen Malware nach § 9 BDSG gesichert sein müssen. § 43 Abs. 2 BDSG scheidet daher als Schutzgesetz im Rahmen der unbeabsichtigten Weiterverbreitung von Malware aus.

D. Malwareverbreitung bei vertraglichen und vorvertraglichen Beziehungen

Werden im Rahmen vertraglicher oder vorvertraglicher Beziehungen z. B. mit Malware infizierte E-Mails verschickt, stellt sich die Frage, inwieweit der Verbreiter haftet. Ist die Virenprüfung Teil der vertraglich vereinbarten Pflichten, stellt dies eine Hauptpflichtverletzung dar, aus der der Schädiger nach § 280 BGB ohne weiteres haftet.[206] Besteht im Rahmen eines Vertrages keine Vereinbarung in Bezug auf Malwareschutz oder handelt es sich lediglich um eine vorvertragliche Beziehung können Malware-Schutzmaßnahmen nur nebenvertragliche Schutzpflichten i. S. d. § 241 Abs. 2 BGB darstellen. Grundsätzlich hat jeder im Rahmen eines Schuldverhältnisses gemäß § 241 Abs. 2 BGB auf die Rechte, Rechtsgüter und Interessen der anderen Rücksicht zu nehmen.

I. Die Entstehung von Schutzpflichten

Um die Haftung aus einer nebenvertraglichen Schutzpflichtverletzung im Rahmen des § 280 Abs. 1 BGB begründen zu können muss, wenn kein Vertrag vorliegt, ein Schuldverhältnis i. S. d. § 311 Abs. 2 BGB entstanden sein. Dies kann durch die Aufnahme von Vertragsverhandlungen (Nr. 1), die Anbahnung eines Vertrages (Nr. 2) oder durch ähnliche geschäftliche Kontakte (Nr. 3) geschehen. Nr. 2 dient als Grundtatbestand,[207] in dessen Bereich der Begriff Vertragsanbahnungen weit auszulegen ist.[208] Werden z. B. E-Mails mit werbendem Charakter

[206] LG Hamburg, MMR 2001, S. 831; *Libertus*, MMR 2005, S. 507 (511).
[207] *Emmerich*, in: MüKo/BGB, § 311, Rn. 68; *Kindl*, in: Erman, § 311, Rn. 19.
[208] *Kindl*, in: Erman, § 311, Rn. 21

bewusst an potenzielle Kunden verschickt, ist eine einseitige und zielgerichtete Anbahnung eines Vertrages gegeben.[209] Besteht ein Vertrag zwischen Schädiger und Geschädigtem hat Erstgenannter neben den leistungsbezogenen Pflichten weitere Schutz- bzw. Verhaltenspflichten i. S. der §§ 241 Abs. 2, 242 BGB zu beachten.[210] Die Verhaltenspflicht könnte sich im Rahmen der Rücksichtnahme auf die Rechtsgüter des Vertragspartners dahingehend auswirken, dass Malwareschäden verhindert werden müssen. Es besteht mithin ein Erhaltungsinteresse, welches den anderen vor erhöhten Einwirkungsgefahren der geschäftlichen Beziehung schützen soll.[211]

II. Inhalt der Schutzpflichten

Der Inhalt der Schutzpflichten ergibt sich grds. aus dem Vertragszweck, der Verkehrssitte und den Anforderungen des redlichen Geschäftsverkehrs.[212] Der Gesetzgeber betont, dass die Schutzpflichten in Bezug auf die Rücksichtnahme auf die Rechte und Rechtsgüter des anderen Teils von den Verkehrspflichten des Deliktrechts abgegrenzt werden soll.[213] Andererseits werden Schutzpflichten durch die Verkehrssitte mit beeinflusst.[214] Diese werden wiederum auch durch den Inhalt der Verkehrspflichten konkretisiert.[215] Verkehrspflichten können daher zur Ausformung von Schutzpflichten berücksichtigt werden. Die herausgearbeiteten Grundsätze können zumindest zur „Konkretisierung des objektiven Pflichteninhalts vertraglicher Schutzpflichten herangezogen“[216] werden. Daher sind gleiche bzw. ähnliche Grundsätze[217] zu Bestimmung der Schutzpflichten bei unbeabsichtigten Malwareschäden zu berücksichtigen. Die Schutzpflichten gebieten es, Schaden vom Vertragspartner fernzuhalten und technische Sicher-

---

[209] Vgl. *Kindl*, in: Erman, § 311, Rn. 21; als ähnlichen geschäftlichen Kontakt qualifizierend *Libertus*, MMR 2005, S. 507 (511); *Koch*, NJW 2004, S. 801 (806).
[210] *Heinrichs*, in: Palandt, § 241, Rn. 6.
[211] *Roth*, in: MüKo/BGB, § 241, Rn. 39.
[212] *Heinrichs*, in: Palandt, § 241, Rn. 7.
[213] BTDrucks. 14/6040, S 125.
[214] *Roth*, in: MüKo/BGB, § 242, Rn. 173; *Heinrichs*, in: Palandt, § 241, Rn. 6.
[215] *Heinrichs*, in: Palandt, § 241, Rn. 6; *Koch*, NJW 2004, S. 801 (806).
[216] LG Hamburg, NJW 1997, S. 2606 (2607); OLG Nürnberg, NJW RR 1986, S. 1224; *Libertus*, MMR 2005, S. 507 (511); *Koch*, NJW 2004, S. 801 (806).
[217] S. o. C.

heitseinrichtungen einzusetzen.[218] Daraus ergibt sich, dass im Verhältnis zwischen Unternehmern und Privaten (B2C) den Unternehmer eine Schutzpflicht zur Sicherung seiner Systeme trifft. Zwischen Unternehmern kann sich die Schutzpflicht auswirken, wenn einer der Unternehmer wie ein Privater behandelt werden muss.[219] Zwischen Privaten (C2C) reduziert sich die Schutzpflicht aufgrund des Vertrauensschutzgedankens, so dass eine Haftung entfällt.

III. Haftungsausschluss durch Allgemeine Geschäftsbedingungen

Wird im Rahmen vertraglicher Beziehungen von den Vertragspartnern über E-Mail und sonstiges kommuniziert, kann der Schädiger die Haftung durch AGB grds. einschränken. Gemäß der §§ 276 Abs. 3, 309 Nr. 7 lit. a BGB kann die Haftung für Sachschaden nicht in Fällen des Vorsatzes oder grober Fahrlässigkeit bedingt werden. Eine Freizeichnung ist nur im Rahmen leichter Fahrlässigkeit zulässig.[220] Beruht ein Malwareschaden auf der Unterlassung des Virenschutzes, so ist zumindest bei Unternehmern ein grob fahrlässiger Verstoß gegen die im Verkehr erforderliche Sorgfalt anzunehmen. Aufgrund der gesetzlichen, behördlichen und fachverbandlichen Verhaltensnormen in Bezug auf IT-Sicherheit[221] ist die zu erwartende Sorgfalt in einem besonders schweren Maß verletzt, wenn keine Schutzmaßnahmen getroffen wurden. Für Unternehmer scheidet eine Freizeichnung daher grds. aus.

---

[218] *Rössel*, ITRB 2002, S. 214 (215).
[219] S. o. C., 2., d.
[220] Vgl. *Libertus*, MMR 2005, S. 507 (511); *Koch*, NJW 2004, S. 801 (807)
[221] S. o. C., I., 2., b., bb., (2).

E. Malware-spezifische Einschränkungen der Haftung

I. Mitverschulden im Rahmen von Malwareschäden

Lässt der Geschädigte die Sorgfalt außer Acht, die unter den gegebenen Umständen erforderlich erscheint um sich vor Schäden zu bewahren, kann der Schadensersatzanspruch gemäß § 254 Abs. 1 BGB entfallen oder gekürzt werden.[222] Das Unterlassen der Installierung von Sicherheitssoftware und fehlende Datensicherung könnten ein Mitverschulden begründen.

1. Fehlende Schutzsoftware

Das Fehlen von Schutzsoftware kann nicht nur im Rahmen der Reduzierung der Verkehrspflichten, sondern auch bei der Beurteilung des Mitverschuldensanteils eine Rolle spielen. Zumindest die Installierung von Virenschutzprogrammen ist heute von jedermann zu erwarten.[223] Der Vertrauensvorsprung Privater gegenüber Unternehmern kann nicht auf einen Ausschluss jeglicher Sicherheitsvorkehrungen hinauslaufen. Die Kenntnis über das Risiko und die finanziell verhältnismäßige Zugänglichkeit zu Schutzprogrammen erlauben es von jedem, die Installierung und Aktualisierung grundlegender Schutzvorkehrungen zu erwarten.[224] Dementsprechend ist auch bei Schädigungen durch Unternehmer bei Privaten der entstandene Ersatzanspruch zu reduzieren.

2. Fehlende Datensicherung

Die sich durch Malware ergebenden Gefahren können durch Maßnahmen zur Datensicherung vom Geschädigten begrenzt werden. Datensicherung ist eine Selbstverständlichkeit,[225] die zumindest im ge-

---

[222] BGHZ 9, S. 316 (318 f.); BGH, NJW 1997, S. 2234 (2235).
[223] S. o. C., I., 2. b., bb., (1).
[224] Ähnlich *Koch*, NJW 2004, S. 801 (807)
[225] BGH; NJW 1996, S. 2924 (2926); OLG Hamm, MMR 2004, S. 487 (488); OLG Karlsruhe, NJW-RR 1997, S. 554; OLG Hamm, NJW-RR 1992, S. 1503; *von Gravenreuth*, S. 54; *Meier/Wehlau*, NJW 1998, S. 1585 (1590).

werblichen Bereich vorausgesetzt werden darf.[226] Die mitunter großen Schäden, die durch Datenverluste entstehen können, stehen wenig beanspruchenden und günstigen Sicherungsmöglichkeiten gegenüber.[227] Im gewerblichen Bereich kann das Mitverschulden des Geschädigten die Schadensersatzpflicht entfallen lassen.[228] Datensicherung muss in regelmäßigen Abständen erfolgen, damit sie schützende Wirkung entfalten kann. Dabei wird z. T. gefordert, dass Sicherungen täglich und Vollsicherungen mindestens einmal wöchentlich erfolgen müssen.[229] Im gewerblichen Bereich ist eine tägliche Sicherung schon aus betriebswirtschaftlichen Gründen unabdingbar und wegen der Wichtigkeit der Daten auch zu erwarten. Ob fehlende Datensicherung bei Privaten zum Wegfall des Ersatzanspruches führt, ist fraglich. Grundsätzlich kann wie im Rahmen der Installation von Schutzsoftware, auch von Privaten ein Mindestmaß an Sorgfalt zur Eigensicherung erwartet werden. Ein vollständiger Wegfall des Ersatzanspruches dürfte aufgrund des Vertrauensvorsprungs Privater gegenüber Unternehmern nicht eintreten. Bezüglich der Häufigkeit der Sicherungen wird man Privaten größere zeitliche Abstände zubilligen müssen,[230] da sie EDV-Technik in unregelmäßigeren Abstände nutzen und zudem schutzwürdiger erscheinen als Unternehmen, bei denen der Schaden zumeist nicht nur einer Person aufgebürdet wird.

II. Haftung bei Mehrfachinfektionen und Rechtmäßigem Alternativverhalten

1. Haftung bei Hinzutreten einer Reserveursache

Ist ein System von mehr als einem Schadprogramm infiziert und hätten beide den gleichen Schaden verursacht, stellt sich die Frage, ob

---

[226] BGH; NJW 1996, S. 2924 (2926); OLG Hamm, MMR 2004, S. 487 (488); OLG Karlsruhe, NJW-RR 1997, S. 554; OLG Hamm, NJW-RR 1992; *Erben/Zahrnt*, CR 2000, S. 88 ff.
[227] *Heckmann*, MMR 2006, S. 280 (281); *Meier/Wehlau*, NJW 1998, S. 1585 (1590).
[228] OLG Karlsruhe, NJW-RR 1997, S. 554; OLG Köln, CR 1994, S. 532; OLG Hamm, NJW-RR 1992, S. 1503.
[229] OLG Hamm, MMR 2004, S. 487 (488); LG Konstanz, NJW 1996, S. 2662.
[230] *Koch*, NJW 2004, S. 801 (807).

der Schädigende sich auf eine Reserveursache berufen kann. Im Rahmen der hypothetischen Kausalität könnte vorgebracht werden, dass der Schaden sowieso wenig später durch ein anderes Schadprogramm eingetreten wäre. Die Behandlung der Fälle hypothetischer Kausalität ist in Rechtsprechung und Literatur umstritten.[231] Weitgehend übereinstimmend wird die Berufung auf einen hypothetischen Geschehensverlauf als gerechtfertigt angesehen, wenn in der beschädigten Sache oder verletzten Person eine Schadensanlage bestand.[232] Ist auf einem Computersystem kein Schutzprogramm installiert bzw. ist es über einen längeren Zeitraum nicht aktualisiert worden, könnte in der Computeranlage eine in Bezug auf Malwareschäden immanente Schadensanlage konkretisiert sein. Allerdings ist allg. anerkannt, dass die Reserveursache den Schädiger nicht entlastet, wenn sie die Handlung eines Dritten darstellt und sich daraus ein Ersatzanspruch begründet hätte.[233] In dieser Situation würde der Dritte nicht haften müssen, so dass der Geschädigte leer ausgehen würde.[234] Dennoch sind bei der Berechnung des Schadensumfangs die Beschränkungen des hypothetischen Anspruchs des Geschädigten gegen den Dritten zu berücksichtigen.[235] Wenn der Anspruch gegen den Dritten z. B. aufgrund Mitverschuldens gemäß § 254 Abs. 1 BGB beschränkt wäre, muss auch der wirkliche Schädiger nur den reduzierten Betrag ersetzen.[236] Hätte der Dritte z. B. eine Minderung seiner Schadensersatzpflicht in Folge mangelnder Datensicherung des Geschädigten begründen können, so hat der Schädiger nur innerhalb des durch das Mitverschulden gezogenen Umfangs zu haften. Eine Berufung auf die Reserveursache in Fällen der Mehrfachinfektion mit Malware ist grds. abzulehnen.[237]

---

[231] *Oetker*, in: MüKo/BGB, § 249, Rn. 203; *Heinrichs*, in: Palandt, § 249, Rn. 98.
[232] RGZ 156, S. 187 (191); BGH, NJW 1956, S. 1027; 1985, S. 676 (677); *Oetker*, in: MüKo/BGB, § 249, Rn. 203; *Heinrichs*, in: Palandt, Vorb. v. § 249, Rn. 99.
[233] BGH, NJW 1958, S. 705; 1967, S. 551 (552); *Schiemann*, in: Staudinger, § 249, Rn. 95; *Oetker*, in MüKo/BGB, § 249, Rn. 208
[234] *Oetker*, in MüKo/BGB, § 249, Rn. 208.
[235] *Schiemann*, in: Staudinger, § 249, Rn. 96; *Oetker*, in MüKo/BGB, § 249, Rn. 208; *Lemhöfer*, JuS 1966, S. 337 (341).
[236] *Schiemann*, in: Staudinger, § 249, Rn. 96; *Oetker*, in MüKo/BGB, § 249, Rn. 208; *Lemhöfer*, JuS 1966, S. 337 (341).
[237] Im Ergebnis so auch *von Gravenreuth*, S. 52 f.

Allerdings können Beschränkungen des hypothetischen Anspruchs den wirklichen Anspruch reduzieren.

2. Rechtmäßiges Alternativverhalten

Hat der Schädiger keine Schutzmaßnahmen zur Verbreitung von Malware installiert, ist er grds. ersatzpflichtig. Die Ersatzpflicht könnte entfallen, wenn der Schaden auch unter Anwendung der von einem Internet-Nutzer zu erwartenden Schutzmaßnahmen eingetreten wäre. Es müsste sich mithin um einen Fall des rechtmäßigen Alternativverhaltens handeln. Rechtmäßiges Alternativverhalten ist grds. beachtlich.[238] Können die zu erwartenden Schutzmaßnahmen die schädigende Malware nicht erkennen, kann dem Schädigenden nicht der Vorwurf gemacht werden, er habe nicht ausreichende Maßnahmen ergriffen.[239] Die Beachtlichkeit rechtmäßigen Alternativverhaltens kann entfallen, wenn sich aus dem Schutzzweck der verletzten Norm etwas anderes ergibt.[240] Im Rahmen der Verkehrspflichten bzw. Schutzpflichten i. S. d. §§ 823 Abs. 1, 241 Abs. 2, 242 BGB ergeben die Schutzzwecke der Normen keine Einschränkungen für die Beachtlichkeit des rechtmäßigen Alternativverhaltens.[241]

III. Mitverantwortlichkeit von Online-Diensten

Online-Dienste, wie T-Online oder AOL, speichern fremde Informationen auf eigenen Rechnern und machen sie ihren Nutzern zugänglich. Dabei handelt es sich um Service Provider i. S: d. §§ 8 Abs. 2, 11 Abs. 1 TDG.[242] Werden Daten des Schädigers vor Eintritt des Schadens auf Systemen des Online-Dienstes gespeichert, ist fraglich, ob diese dort auf Schadprogramme hin überprüft werden müssen. Würde eine Pflicht des Service Providers zur Malwareprüfung bestehen,

---

[238] BGH, NJW 1984, S. 1397 (1399); BGH, NJW 1993, S. 520 (521); *Oetker*, in: MüKo/BGB, § 249, Rn. 215; *Heinrichs*, in: Palandt, § 249, Rn. 105.
[239] *Koch*, NJW 2004, S. 801 (806).
[240] BGH, NJW 1986, S. 576 (579); *Oetker*, in: MüKo/BGB, § 249, Rn. 215; *Heinrichs*, in: Palandt, § 249, Rn. 106.
[241] *Koch*, NJW 2004, S. 801 (806).
[242] *Eichhorn*, S. 47.

könnte der Schädiger dies als Einwand gegen den Ersatzanspruch vorbringen. Grds. ist der Service Provider gemäß der §§ 8 Abs. 2, 11 Abs. 1 TDG nicht verpflichtet, gespeicherte Informationen zu überwachen. Als Information wird all jenes verstanden, was der Service-Provider auf seinen Systemen abspeichert.[243] Gelangt eine mit Malware infizierte Datei in das System des Online-Dienstes, stellt das Schadprogramm eine Information i. S. d. § 8 Abs. 2 TDG dar, die grds. nicht überprüft werden muss.[244] Nur wenn der Service Provider Kenntnis über die rechtswidrige Handlung hat oder Kenntnis von Tatsachen und Umstände bekannt sind, die auf die Handlung hinweisen, kann er gemäß § 11 Abs. 1 TDG verantwortlich gemacht werden. Aufgrund der in § 8 Abs. 2 TDG festgelegten Freistellung von Nachforschungs- und Kontrollpflichten,[245] ist der Service Provider nur dann i. S. d. § 11 TDG verantwortlich zu machen, wenn eine rechtswidrige Handlung oder Information in konkreter Form auftritt.[246] Es besteht insbesondere keine Pflicht spezielle Software einzusetzen, um rechtswidrige Informationen aufzufinden.[247] Es gibt daher keine Pflicht des Service Provider die gespeicherten fremden Informationen auf Malware zu überprüfen

IV. Haftung bei Garantie

Sicherheit für die Freiheit von Malware kann es nicht geben. Wenn der Schädiger vor Schadenseintritt dennoch die Malwarefreiheit garantiert, haftet er schuldunabhängig[248] im Rahmen der Zusicherung einer Eigenschaft.[249] Selbst bei Installierung aller nach dem Stand der Technik der IT-Sicherheit zu erwartenden Sicherheitsvorkehrungen kann der Garantierende in Anspruch genommen werden, wenn dennoch ein durch Malware verursachter Schaden auftreten sollte. Derje-

---

[243] BTDrucks. 14/6098, S. 23.
[244] *Koch*, NJW 2004, S. 801 (806); *Schmidtbauer* (zuletzt abgerufen: 12.08.2006).
[245] *Spindler*, in: Spindler, TDG, § 8, Rn. 11.
[246] *Spindler*, in: Spindler, TDG, § 11, Rn. 15.
[247] *Spindler*, in: Spindler, TDG, § 11, Rn. 11.
[248] *Heidrich*, c´t 19/2004, S. 168 (169); Schneider/Günther, CR 1997, S. 389 (391).
[249] *Heinrichs*, in: Palandt, § 276, Rn. 29.

nige der Malwarefreiheit garantiert kann sich nicht darauf berufen, er habe auf Schutzmaßnahmen des Anderen vertraut.

F. Ergebnisse

Die Malwareverbreitung und die daraus erwachsene Gefahr haben in den letzten Jahren exponentiell zugenommen. Malware entwickelt sich ständig weiter. Die verschiedenen Erscheinungsformen sind auch im Rahmen juristischer Arbeiten voneinander zu trennen, da die Rechtsfolgen variieren können. Absoluter Schutz gegen Schadprogramme ist nicht möglich.

Um Malware-typische Datenverluste bzw. -veränderungen im Rahmen des § 823 Abs. 1 BGB haftungsrechtlich umfassend sanktionieren zu können, sind mit der h. M. Malwareschäden als Eigentumsverletzung erfasst, doch erweist sich dieser Schutz um den Entwicklungen der Informationsgesellschaft gerecht zu werden als nicht mehr ausreichend. Das Recht am eigenen Datenbestand ist nicht zuletzt aufgrund der stets anwachsenden Gefahr durch Malware und der Bedeutung, die Daten bzw. Informationen heute als wirtschaftliches Gut haben als sonstiges Recht im Sinne des § 823 Abs. 1 BGB anzuerkennen. Es hat den Vorteil der Unabhängigkeit von eigentumsrechtlichen Positionen und genügt den Entwicklungen des Outsourcing im IT-Bereich. Die Schutzbereiche der durch § 823 Abs. 1 BGB geschützte Rechtsgüter reichen hier nicht weit genug.

Malware kann sich durch den Nutzer oder selbst weiterverbreiten. Für die Entstehung von Verkehrspflichten macht es keinen Unterschied. Ausschlaggebend ist allein die Möglichkeit Schutzmaßnahmen ergreifen zu können. Allerdings kann der Zeitpunkt der Entstehung der Verkehrspflichten bei selbstständiger Verbreitung früher einsetzen, da die Gefahrenlage z. B. schon durch das Aufnehmen eines Kontaktes in das Adressbuch entstehen kann.

Die Verwendung von aktuellen Schutzprogrammen ist zumutbar und zu erwarten. Die Zumutbarkeit in Bezug auf finanzielle Ausgaben und organisatorische Maßnahmen ist anhand des Gefahrenpotenzials des einzelnen Internet-Nutzers zu bestimmen. Unternehmen werden regelmäßig größere Anforderungen erfüllen müssen, so dass neben der Installierung von Software ein umfassendes IT-Sicherheitsmanagment erforderlich werden kann. Bei neuartigen Malware-Arten können Schutzmaßnahmen entsprechend dem Gefahrenpotenzial des einzelnen unzumutbar sein. Gegen Computerviren hat sich aufgrund der überragenden Bekanntheit dieser Malwareart jeder zu schützen. Bei anderen Schadprogrammen ist unter Berücksichtigung der Möglichkeit und Bekanntheit von Schutzmaßnahmen und dem wirtschaftlichen Aufwand abzuwägen, ob der Schutz zumutbar ist.

Aufgrund vertrauensschutzbedingter Abwägungen haften Private weder gegenüber Unternehmern (C2B) noch gegenüber anderen Privaten (C2C). Bei Unternehmern ist zu differenzieren. Das alleinige Abstellen auf die Unternehmereigenschaft des § 14 BGB führt zu unsachgerechten Ergebnissen. Es ist im Einzelfall zu prüfen, ob Unternehmer das Internet und E-Mail als wirtschaftlichen Faktor einsetzen und daraus Vorteile ziehen, und ob durch gesetzliche, behördliche oder fachverbandliche Normen und Empfehlungen erhöhte IT-Sicherheit erwartet werden kann. Werden diese beiden Aspekte nicht erfüllt, haften Unternehmer wie Private. Zwischen Unternehmern, die nicht wie Private zu behandeln sind, entstehen keine Haftungsansprüche, da das gegenseitige Vertrauen eine Haftung ausschließt.

Im Rahmen (vor-)vertraglicher Beziehungen ist der Schutz vor Malware, wenn nicht vertraglich vereinbart, eine Schutzpflicht, dessen genauer Inhalt auch durch deliktsrechtliche Verkehrspflichten mitbestimmt wird.

Abschließend ist hervorzuheben, dass der Gedanke des Eigenschutzes in Bezug auf Malware-Schäden von höchster haftungsrechtlicher Be-

deutung ist. Schutzsoftware und Datensicherung sind Selbstverständlichkeiten. Wegen unterlassener Datensicherung ist der Ersatzanspruch des Geschädigten im Rahmen des Mitverschuldens zu reduzieren. Bei gewerblichen Nutzern entfällt der Ersatzanspruch zumeist komplett.