Erschienen in: K&R 2007, 566 (Heft 11/2007)

Die Haftung für kompromittierte Computersysteme - § 823 Abs. 1 BGB und Gefahren aus dem Internet

Von Ref. jur. Reto Mantz. Der Verfasser ist wiss. Mitarbeiter der Anwaltssozietät Heymann & Partner, Frankfurt am Main.

Der vorliegende Beitrag beschäftigt sich mit dem Fall, dass von einem Computersystem ohne Wissen und Zutun des Eigentümers eine Gefährdung für andere Computer ausgeht, indem z.B. ein „eingefangenes“ Virus weiter verteilt wird. Der Aufsatz soll, ausgehend von der bisherigen Rechtsprechung und unter Betrachtung der Ergebnisse der Literatur, allgemeine Leitlinien aufzeigen, die die Pflichtenbestimmung für den Betrieb von Computeranlagen im Rahmen des § 823 Abs. 1 BGB ermöglichen.

I. Einführung

Das Internet ist nicht nur ein Kommunikationsmedium, es kann auch mit Fug und Recht als ein „Gefahrenraum“ bezeichnet werden. Die Verbreitung von digitalen Schädlingen wie Viren, Würmern und Trojanern hat ein enormes Ausmaß erreicht.[1] Betrachtet man die Haftungssituation, so stehen sich der Schädiger, also derjenige, der das Schadprogramm verbreitet hat, und als Geschädigter das Opfer des „Angriffs“ gegenüber. Mangels einer rechtlichen Sonderbeziehung ist für den Betroffenen die deliktische Haftung nach §§ 823 ff. BGB Mittel der Wahl, um einen erlittenen Schaden geltend zu machen. Ist der Schädiger ermittelt, ist zu fragen, ob dieser das Schadprogramm vorsätzlich bzw. schuldhaft in Umlauf gebracht hat. Schwieriger zu behandeln ist die Konstellation, in der der Schädiger sich seines Angriffs gar nicht bewusst war, z.B. weil sein Computersystem von einem Schädling befallen war, und dieser sich anschließend der kompromittierten Anlage zur Weiterverbreitung bediente. Denkbar ist des Weiteren der Fall, dass das kompromittierte System nicht Schadprogramme verbreitete, sondern selbst Angriffe auf fremde Computeranlagen durchführte bzw. sich an ihnen beteiligte.[2] Grundlage der deliktischen Haftung ist menschliches, also willensgesteuertes, bewusstes und beherrschbares Verhalten.[3] Problematisch ist, dass der Nutzer mangels entsprechenden Bewusstseins keine feststellbare Schädigungshandlung vorgenommen hat. Allerdings könnte sich eine Schadensersatzpflicht nach § 823 BGB daraus ergeben, dass der Nutzer es unterlassen hat, seinen Computer ausreichend gegen Bedrohungen aus dem Internet zu sichern, dass er also eine ihm möglicherweise obliegende Verkehrssicherungspflicht im Vorfeld der Schädigung verletzt hat. Als mögliche vorbeugende Maßnahmen stehen insbesondere die Installation eines

---

[1] Zur Wirkungs- und Vorgehensweise *Lang*, JurPC Web-Dok. 205/2001, Rn. 35 ff.
[2] Dazu eingehend *Möller/Kelm*, DuD 2000, 292; BSI-Lagebericht 2007, http://www.bsi.de/literat/lagebericht/lagebericht2007.pdf, 23.
[3] BGH, Urt. v. 12.2.1963 - VI ZR 70/62, BGHZ 39, 103, 106; BGH, Urt. v. 01.07.1986 - VI ZR 294/85, BGHZ 98, 137; *Wagner,* in: MünchKommBGB, 4. Aufl. 2003, § 823 BGB Rn. 297; *Spickhoff* in: Soergel, BGB, 13. Aufl. 2005, § 823 BGB Rn. 3.

Virenscanners, einer Firewall etc. sowie die regelmäßige Aktualisierung des Betriebssystems und der installierten Programme zur Verfügung.[4]

II. Rechtsgutverletzung

Zunächst ist festzustellen, ob überhaupt eine Rechtsgutverletzung vorliegt bzw. vorliegen kann. In aller Regel wird die Hardware des Betroffenen nicht physisch beschädigt. Es treten eher Datenverluste bzw. -veränderungen sowie eventuell Funktionsstörungen des Systems auf. § 823 Abs. 1 BGB schützt Leben, Gesundheit, Freiheit und sonstige absolute Rechte. Eine unmittelbare Schädigung von Leben, Körper und Gesundheit tritt bei Angriffen auf Computersysteme üblicherweise nicht auf.[5]
Es sind auf Seiten des Geschädigten also hauptsächlich Daten betroffen. Daten fallen unter den Schutz des § 823 Abs. 1 BGB, wenn sie in irgendeiner Form verkörpert sind.[6] Der BGH sieht die Verkörperung bereits als gegeben an, wenn die Daten in einem von Strom abhängigen – flüchtigen - Speichermedium vorliegen.[7] Aufgrund des unbefugten Zugriffs auf das System des Opfers liegt bereits dann eine Datenveränderung vor, wenn ein Virus sich im System verankert. Mit dieser Auffassung lassen sich auch Datenverluste erfassen, die durch erfolgreiche Denial-of-Service-Attacken (DoS)[8] verloren gehen. Wird also ein Virus im System installiert, werden anderweitig Daten verändert oder stürzt ein Computer in Folge eines DoS-Angriffes ab und gehen dabei Daten verloren, so greift § 823 Abs. 1 BGB.

III. Verletzung von Verkehrssicherungspflichten

Dem Nutzer des kompromittierten Systems müsste eine Verletzung seiner ihm obliegenden Verkehrssicherungspflichten vorzuwerfen sein.

1. Gefahrbeherrschung als Anknüpfungspunkt von Verkehrssicherungspflichten

Verkehrssicherungspflichten sind allgemein Gefahrsteuerungsgebote, die dem über eine Sache Verfügenden zum Schutz der Rechtsgüter Dritter auferlegt werden.[9] Eine haftungsbegründende Zurechnung kommt grundsätzlich bei der Beherrschung einer besonderen Gefahrenquelle sowie bei der Schaffung einer besonderen Gefahrenlage aus vorangegangenem Tun in Betracht.[10] Es sind die notwendigen und zumutbaren

---

[4] *Heibey,* in: Roßnagel, Handbuch Datenschutzrecht, 2003, Kap. 4.5 Rn. 131.
[5] Unmittelbar könnte die Schädigung beispielsweise sein, wenn ein angegriffenes System im Bereich des Gesundheitswesens eingesetzt wird und eine hohe Betriebszuverlässigkeit erforderlich ist. Vgl. *Redeker*, IT-Recht in der Praxis, Rn. 824; *Schneider*/*Günther*, CR 1997, 389, 392; *Sonntag*, Kritische Infrastrukturen, 2005, 61 ff.
[6] BGH, Urt. v. 15.11.2006 - XII ZR 120/04, CR 2007, 75, 75 f.; BGH, Urt. v. 14.7.1993 - VIII ZR 147/92, NJW 1993, 2436, 2438; BGH, Urt. v. 4.11.1987 - VIII ZR 314/86, NJW 1988, 406, 408; OLG Karlsruhe, Urt. v. 7.11.1995 - 3 U 15/95, NJW 1996, 200, 201; *Hoeren/Pichler*, in: Loewenheim/Koch, Praxis des Online-Rechts, 2001, 395 f.; *Mankowski* in: Ernst, Hacker, Cracker & Computerviren, 2004, Rn. 440; *Schneider*/*Günther*, CR 1997, 389, 392 f.; *Koch*, NJW 2004, 801, 802; *Leible*/*Sosnitza*, K&R 2002, 51, 52.
[7] BGH, Urt. v. 15.11.2006 - XII ZR 120/04, CR 2007, 75, 76; „extrem weite Auffassung der Verkörperung“ *Lejeune*, CR 2007, 77, 78.
[8] Dazu o. Fn. 2; s. auch AG Gelnhausen, Urt. v. 06.10.2005 - 51 C 202/05, CR 2006, 209.
[9] *v.Bar*, Verkehrspflichten, 1980, 45.
[10] *Larenz*/*Canaris*, Lehrbuch des Schuldrechts, 13. Aufl. 1994, § 76 III 4b; *Koch*, NJW 2004, 801, 803; *v.Bar*, (o. Fn. 9), 92; ähnlich auch *Libertus*, MMR 2005, 507, 508.

Vorkehrungen zu treffen, um eine Schädigung anderer zu vermeiden.[11] Die Handlungs- bzw. Verkehrssicherungspflicht obliegt aber nur demjenigen, dem eine besondere Gefährdung der geschützten Rechtsgüter des § 823 Abs. 1 BGB zugerechnet werden kann. Die Konkretisierung dieser Pflichten erfolgt unter Betrachtung der berechtigten Sicherheitserwartungen der betroffenen Verkehrskreise,[12] sowie der Möglichkeit und Zumutbarkeit der Gefahrenvermeidung, die auf Seiten des Schädigers sowie des Geschädigten gegeneinander abzuwägen sind.[13]
Der Besitzer eines Computers hat die Verfügungsgewalt über diesen. Um spezifische Verkehrspflichten zu begründen, kommt bei Computernutzern demnach insbesondere die Herrschaft über eine Gefahrenquelle in Betracht. Von einer Computeranlage geht jedenfalls dann eine Gefährdung für die Computer Dritter aus, wenn sie durch einen vorhergegangenen Angriff kompromittiert wurde und in der Folge Angriffe auf fremde Computersysteme ausführt. Beispielhaft seien hier die Versendung von Viren, die Ausnutzung von Sicherheitslücken auf entfernen Rechnern, oder die Mitwirkung an Denial-of-Service-Attacken genannt.

2. Pflicht zur Ergreifung der zur Verfügung stehenden Sicherungsmaßnahmen

Selbst wenn der Nutzer als derjenige identifiziert ist, der eine Gefahrenquelle beherrscht, muss ihn dennoch nicht automatisch die Pflicht treffen, jede ihm zur Verfügung stehende Gegenmaßnahme zu ergreifen. Vielmehr muss es ihm auch zumutbar sein, eine konkrete Sicherungsmaßnahme auszuwählen und durchzuführen. Über die zumutbaren Erwartungen hinaus gehen jedenfalls Lösungen, die für einen normalen Nutzer nicht durchführbar wären oder zu hohe Aufwendungen benötigen würden. Als Bewertungsmaßstab sind aber nicht die Fähigkeiten des einzelnen Nutzers heranzuziehen. Es erfolgt vielmehr eine objektivierte Betrachtung unter Zugrundelegung einer bestimmten Nutzergruppe.
Fraglich ist demzufolge, wie die Bewertung der Pflichten zu erfolgen hat.

a. Die Bekanntheit des Sicherheitsproblems

Erstes Merkmal für die Bewertung hinsichtlich der Ergreifung von Sicherheitsmaßnahmen ist die Bekanntheit des Sicherheitsproblems. Die für den IT-Bereich erste höchstrichterliche Entscheidung, die sich ausdrücklich mit den Pflichten des Computernutzers hinsichtlich der Absicherung seines Systems befasst, ist die Dialer-Entscheidung.[14] In dieser hatte ein Computernutzer ein Programm heruntergeladen, das die Nutzung des Internet beschleunigen sollte. Tatsächlich handelte es sich dabei um einen Dialer, der für alle zukünftig hergestellten Internet-Verbindungen des Nutzers eine teure Mehrwertdienstenummer wählte. Als der Nutzer bemerkte, dass das heruntergeladene Programm ihn nur auf Erotikseiten leitete, löschte er die Datei. Damit änderte er allerdings nicht die Voreinstellung für die Internetanwahlnummer. Im Klageverfahren verlangte die Klägerin, die für den

---

[11] BGH, Urt. v. 30.4.1953 - III ZR 377/51, BGHZ 9, 373; BGH, Urt. v. 4.12.2001 - VI ZR 447/00, NJW-RR 2002, 525 mwN; *Larenz/Canaris*, (o. Fn. 10), § 76 III 4a; *v.Bar*, (o. Fn. 9), 113.
[12] BGH, Urt. v. 4.12.2001 - VI ZR 447/00, NJW-RR 2002, 525, 526; *Spindler* in: Bamberger/Roth, BGB, 2. Aufl. 2007, § 823 Rn. 234; *Hager* in: Staudinger, Eckpfeiler, 2005, 857.
[13] *Koch*, NJW 2004, 801, 804; *Libertus*, MMR 2005, 507, 509; *Spindler* in: Bamberger/Roth, (o. Fn. 12), § 823 Rn. 234.
[14] BGH, Urt. v. 4.3.2004 - III ZR 96/03, NJW 2004, 1590.

Mehrwertdiensteanbieter in ihrer Eigenschaft als Telekommunikationsanbieterin das Inkasso übernahm, die Zahlung der über die Mehrwertdiensterufnummer angefallenen Entgelte. Der BGH lehnte die Klage als unbegründet ab. Die entscheidende Frage des Verfahrens war, ob der Telefonnetzbetreiber oder der Anschlussinhaber das Risiko der heimlichen Installation eines Dialers zu tragen habe. Der BGH nahm hierfür eine Auslegung des Vertrags zwischen dem Anschlussinhaber und dem Telekommunikationsbetreiber vor dem Hintergrund des § 16 Abs. 3 Satz 3 TKV vor.[15] § 16 Abs. 3 Satz 3 TKV findet direkte Anwendung allerdings nur für die Rechtsfolgen von physischen Zugriffen auf den Netzzugang.[16] Deshalb begründete der BGH zunächst, dass der Vertrag in Bezug auf die Risikozuweisung lückenhaft sei und durch den Grundgedanken des § 16 Abs. 3 Satz 3 TKV geschlossen werden könne.[17] Manipulationen, die der Kunde nicht zu vertreten habe, fielen danach in den Risikobereich des Netzanbieters. In dieser Abwägung schloss sich der BGH dem LG Kiel an,[18] das in einem ähnlich gelagerten Fall teurer Interneteinwahl einen gewollten Vertragsschluss als lebensfremd ablehnte.[19] Zusätzlich hatte das LG Kiel dem Telekommunikationsdienstleister vorgeworfen, dem Kunden die Möglichkeit zu nehmen, Einwendungen direkt gegen Mehrwertdiensteanbieter zu erheben, da er nicht in der Lage war, seinem Kunden den Namen des Mehrwertdiensteanbieters zu nennen.[20] Zusätzlich stellte der BGH ausdrücklich fest, dass den Nutzer keine Pflicht zur Überwachung des eigenen Computersystems trifft, solange kein konkreter Hinweis auf einen Missbrauch besteht,[21] und wendet sich damit gegen die vorangegangenen unterinstanzlichen Entscheidungen.[22] Das Gericht stellt also maßgeblich darauf ab, ob die Kenntnis oder wenigstens ein entsprechender Hinweis auf den konkreten Missbrauch bestand. Wesentlicher Ankerpunkt ist demzufolge die Bekanntheit eines Problems.[23] In die Abwägung bei der Risikoverteilung stellt der BGH weiter ein, ob der Nutzer die Manipulation zu vertreten habe. Verallgemeinert man diesen Gesichtspunkt, so kommt es grundsätzlich darauf an, ob ein verständiger objektiver Nutzer von einer entsprechenden Gefahr wusste oder zumindest damit rechnen musste.[24] Bezieht man die Grundsätze der Zurechnung von Verkehrssicherungspflichten in diese Überlegung mit ein, so lässt sich konstatieren, dass der Bekanntheitsgrad eines Problems die Verkehrserwartung der betroffenen Kreise dahingehend zu beeinflussen vermag, Sicherungsmaßnahmen gegen bereits allgemein bekannte Gefährdungen zu verlangen. Im zu entscheidenden Fall war für

---

[15] BGH, Urt. v. 4.3.2004 - III ZR 96/03, NJW 2004, 1590, 1591 f.
[16] BGH, Urt. v. 4.3.2004 - III ZR 96/03, NJW 2004, 1590, 1591 unter Verweis auf BR-Drucks. 551/97, 36.
[17] Zustimmend *Buchinger*/*Pfeiffer*, JA 2004, 589, 590; *Mankowski*, MMR 2004, 312; *Spindler*, JZ 2004, 1128, 1129; aA *Schlegel*, MDR 2004, 620, 621 f.
[18] LG Kiel, Urt. v. 9.1.2003 - 11 O 433/02, MMR 2003, 422.
[19] LG Kiel, Urt. v. 9.1.2003 - 11 O 433/02, MMR 2003, 422, 423; ebenso AG Freiburg, Urt. v. 11.6.2002 - 11 C 4381/01, NJW 2002, 2959; zustimmend *Leible*/*Wildemann*, K&R 2004, 288; *Spindler*, JZ 2004, 1128, 1130.
[20] LG Kiel, Urt. v. 9.1.2003 - 11 O 433/02, MMR 2003, 422, 423.
[21] BGH, Urt. v. 4.3.2004 - III ZR 96/03, NJW 2004, 1590; ebenso AG Freiburg, Urt. v. 11.6.2002 - 11 C 4381/01, NJW 2002, 2959; Mankowski, MMR 2004, 312; aA AG Wiesbaden, Urt. v. 10.8.2002 - 92 C 1328/00, CR 2003, 754; AG München, NJW 2002, 2960; AG Torgau, Urt. v. 3.7.2003 - 2 C 189/03, MMR 2003,759; *Burg*/*Gimnich*, DRiZ 2003, 381, 384 f.; *Schlegel*, MDR 2004, 620, 621.
[22] LG Berlin, Urt. v. 11.7.2001 - 18 O 63/01, ZAP 2002, 565; KG Berlin, Urt. v. 27.1.2003 - 26 U 205/01, NJW-RR 2003, 637; dazu *Feser*, MMR 2003, 402 und im Ergebnis zustimmend *Klees*, CR 2003, 372, der aber die Arglistanfechtung nach § 123 BGB als einschlägig ansieht; s. auch AG München, Urt. v. 4.9.2001 - 155 C 14416/01, JurPC Web-Dok. 391/2002; AG Dillenburg, Urt. v. 13.9.2002 - 5 C 286/02, CR 2003, 686.
[23] Ebenso allgemein *Steiner*, Schadensverhütung als Alternative zum Schadensersatz, 1983, 49.
[24] Vgl. auch LG Köln, Urt. v. 21.7.1999 - 20 S 5/99, NJW 1999, 3206 für Viren.

den Nutzer erstens nicht erkennbar, dass eine Beeinträchtigung des Systems stattgefunden hatte und diese zudem auch nicht einfach beseitigt werden konnte. Er hatte sogar einen Löschungsversuch unternommen, ohne allerdings zu wissen, dass es dazu eines komplizierteren Verfahrens als des von ihm ergriffenen bedurfte.[25] Weiter hat der BGH festgestellt, dass der Nutzer nicht grundsätzlich misstrauisch sein musste.[26] Als Folge traf ihn auch keine Pflicht zur Ergreifung von entsprechenden Sicherungsmaßnahmen.

Die Entscheidung des BGH ist mitnichten auf Dialer beschränkt. Vielmehr lässt sich an ihr die allgemeine Risikoverteilung im Bereich der Gefahren beim Einsatz von Computersystemen ableiten. So hat das LG Stralsund die Grundsätze auf installierte Trojaner übertragen.[27] Im Fall aus dem Jahre 2001 war auf dem Computersystem des Beklagten nachweislich ein Trojaner installiert gewesen. Dieser hat nach Auffassung des Gerichts die Nutzerdaten des Beklagten ausgespäht und es so einem Dritten ermöglicht, vom Computer des Beklagten kostenpflichtige Verbindungen zu Mehrwertdiensterufnummern aufzubauen. Zwar verkennt das Gericht, dass diese Nutzerdaten gar nicht notwendig sind, sondern Mehrwertdienste über den Anschluss abgerechnet werden,[28] allerdings ist der Trojaner trotzdem einem Dialer vergleichbar oder hat sich selbst eines solchen bedient. Unter Verweis auf die Dialer-Entscheidung des BGH führt das LG Stralsund aus, dass sich der Nutzer auch gegen Trojaner nicht habe absichern müssen.[29]

Als tatsächliche Frage ist demnach bei einem Sicherheitsproblem jeweils zu entscheiden, ob dieses konkrete Sicherheitsproblem als allseits bekannt angesehen werden kann. Die Behandlung dieser Frage ist bisher noch ungeklärt. Man kann jedoch davon ausgehen, dass ein Problem erst weithin bekannt ist, wenn eine ausführliche und mehrfache Berichterstattung in Massenmedien erfolgt ist. Ist das Sicherheitsproblem lediglich in Fachzeitzeitschriften aufgegriffen worden, so kann gerade der weniger interessierte Nutzer, und damit die für die Pflichtenbestimmung wesentliche Gruppe der Mehrheit der Nutzer, die Problematik kaum kennen. Auch wer IT-spezifische Informationskanäle nicht nutzt, muss zumindest die Möglichkeit gehabt haben, vom Sicherheitsproblem in seinen Grundzügen erfahren zu haben.

Ob angesichts der weiteren Entwicklung und mehrfachen Berichterstattung und Information über Dialer heute noch davon ausgegangen werden kann, dass die Allgemeinheit bzw. ein verständiger Nutzer keine Kenntnis von dem Problem des Dialers und von möglichen Schutzmechanismen hat, erscheint zweifelhaft.[30] Schließlich sollte man nicht aus den Augen verlieren, dass die Bekanntheit durchaus auch wieder schwinden kann, z.B. wenn mehrere allgemein rezipierte Berichte nahe legen, dass das Sicherheitsproblem nicht mehr besteht bzw. gelöst wurde, und der Nutzer keine Maßnahmen ergreifen muss.

---

[25] Nämlich der Umstellung der Standardrufnummer für Internetverbindungen, vgl. KG Berlin, Urt. v. 27.1.2003 - 26 U 205/01, NJW-RR 2003, 637.

[26] BGH, Urt. v. 4.3.2004 - III ZR 96/03, NJW 2004, 1590, 1592.

[27] LG Stralsund, Urt. v. 22.2.2006 - 1 S 237/05, MMR 2006, 487; aufgehoben durch BGH, Urt. v. 23.11.2006 - III ZR 65/06, MMR 2007, 178. Die Aufhebung wird allerdings nicht mit einer fehlerhaften rechtlichen Würdigung, sondern mit den tatsächlichen Feststellungen bzw. den daraus gezogenen Schlussfolgerungen begründet.

[28] So u.a. auch die Kritik in BGH, Urt. v. 23.11.2006 - III ZR 65/06, MMR 2007, 178.

[29] LG Stralsund, Urt. v. 22.2.2006 - 1 S 237/05, MMR 2006, 487, 489.

[30] Ebenso *Buchinger*/*Pfeiffer*, JA 2004, 589, 591; *Leible*/*Wildemann*, K&R 2004, 288, 289; *Schlegel*, MDR 2004, 620, 621; wohl auch *Spindler*, JZ 2004, 1128, 1129.

b. Bekanntheit auch der Sicherungs- bzw. Gegenmaßnahmen

Während der BGH in der Dialer-Entscheidung noch maßgeblich auf die Kenntnis des Nutzers von der möglichen Beeinträchtigung seines Systems als Voraussetzung für entsprechende Handlungspflichten ausging, kann dies alleine noch nicht für die Begründung entsprechender Obliegenheiten ausreichen. Die mögliche Kenntnis eines Sicherheitsproblems besagt nämlich nichts darüber, ob der Handlungspflichtige auch dazu in der Lage ist, Sicherungsmaßnahmen zu ergreifen. Im Rahmen der Zumutbarkeitsprüfung muss auch dieser Punkt beachtet werden.

Um aber überhaupt Sicherungsmaßnahmen ergreifen zu können, benötigt der Pflichtige die Kenntnis vom Vorhandensein dieser Sicherungsmöglichkeiten.[31] Im Dialer-Fall hatte der Betroffene versucht, die Einwahl über die Mehrwertdiensterufnummer zu unterbinden, indem er das heruntergeladene Programm löschte. Da aber das Programm bereits die Standardverbindung modifiziert hatte, reichte dieses Vorgehen nicht aus. In der Folge sah der BGH keine Pflicht, die geeigneten Maßnahmen zu ergreifen, weil offensichtlich von ihnen keine Kenntnis bestand.

Mit dem Urteil zur Haftung für die Telefonkosten aus R-Gesprächen Dritter[32] hat der BGH dieses ohne expliziten Hinweis auch bereits in der Dialer-Entscheidung mitschwingende Merkmal deutlich herausgestellt. R-Gespräche, also Reverse-Charge bzw. rückwärts berechnete Gespräche, sind solche, bei denen nicht der Anrufer die Gesprächskosten trägt, sondern der Angerufene. Dazu ruft der Anrufer kostenlos bei einem R-Gespräch-Anbieter an, der anschließend den gewünschten Empfänger kontaktiert, (meist) automatisiert erfragt, ob der Angerufene die Kosten für das Gespräch übernehmen will und dann die Verbindung herstellt.[33] Im behandelten Fall hatte der Freund der Tochter der Beklagten mehrfach mit der Tochter solche R-Gespräche geführt. Die Beklagte weigerte sich, die aufgelaufenen Kosten zu zahlen. Während sich der BGH intensiv mit der Frage zu beschäftigen hatte, ob ein wirksamer Vertragsschluss erfolgt war, hat er zudem, erneut unter Anwendung von § 16 Abs. 3 Satz 3 TKV, festgestellt, dass der Telefonanschlussinhaber nicht verpflichtet ist, technische Vorkehrungen gegen die Annahme von R-Gesprächen zu ergreifen.[34] Dafür stellte er auch darauf ab, dass die Beklagte bis zur ersten Rechnung des R-Gespräch-Anbieters keine Kenntnis von den R-Gesprächen hatte.[35] Anschließend verweist er deutlich darauf, dass es bisher keine technisch zumutbaren Möglichkeiten zur Verhinderung von unerwünschten R-Gesprächen gebe.[36] Technisch zumutbar seien diese nämlich nur, wenn sie auch bekannt seien.[37] Ebenso hatte bereits das AG Völklingen entschieden[38] und ausdrücklich formuliert: „Selbst dem Gericht ist es nicht bekannt, dass eine derartige technische Möglichkeit überhaupt besteht.“[39] Das LG Flensburg hat ebenfalls deutlich auf die Bekanntheit des

---

[31] Ebenso AG Völklingen, Urt. v. 23.2.2005 - 5c C 575/04, MMR 2005, 482, 483.
[32] BGH, Urt. v. 16.3.2006 - III ZR 152/05, NJW 2006, 1971.
[33] Eingehend zu den unterschiedlichen Varianten *Janal*, K&R 2006, 272.
[34] BGH, Urt. v. 16.3.2006 - III ZR 152/05, NJW 2006, 1971; zustimmend *Janal*, K&R 2006, 272, 279; *Zagouras*, NJW 2006, 2368, 2369; aA *Schütz*/*Gostomzyk*, MMR 2006, 11 aber unter Hinweis auf in den Tageszeitungen verbreitete Informationen.
[35] BGH, Urt. v. 16.3.2006 - III ZR 152/05, NJW 2006, 1971, 1972.
[36] BGH, Urt. v. 16.3.2006 - III ZR 152/05, NJW 2006, 1971, 1973; zustimmend *Böttcher*, VuR 2006, 256, 259.
[37] BGH, Urt. v. 16.3.2006 - III ZR 152/05, NJW 2006, 1971, 1973 unter Hinweis auf *Grabe*, MMR 2005, 483, 484; zustimmend *Mankowski*, MMR 2006, 458, 459.
[38] AG Völklingen, Urt. v. 23.2.2005 - 5c C 575/04, MMR 2005, 482; zustimmend *Grabe*, MMR 2005, 483.
[39] AG Völklingen, Urt. v. 23.2.2005 - 5c C 575/04, MMR 2005, 482, 483.

Problems sowie der Sicherungsmaßnahmen abgestellt und darauf hingewiesen, dass zum Zeitpunkt der Annahme des im dort behandelten Fall des Jahres 2003 noch keine Warnungen von Verbraucherzentralen vor R-Gesprächen herausgegeben oder bekannte Gerichtsentscheidungen getroffen worden waren.[40] Anders könnte sich nach den Ausführungen des BGH die Lage darstellen, wenn es ein Register gebe, in das sich Anschlussinhaber eintragen könnten, um R-Gespräche zu verhindern.[41] Dem BGH ist in diesem Zusammenhang nur bedingt zuzustimmen. Die Auferlegung von Pflichten muss sich jeweils an der Zumutbarkeit ausrichten. Notwendig ist zusätzlich zum Vorhandensein dieser kostenlosen Datenbank schließlich auch das allgemeine Bewusstsein, dass sie existiert und eine effektive Möglichkeit zur Verhinderung von R-Gesprächen darstellt. Davon bereits mit Einrichtung der Datenbank bei der Bundesnetzagentur auszugehen, ist zu weit gegriffen.[42]
In der Zusammenschau des Dialer-Urteils und der R-Gespräch-Entscheidung muss, um eine Pflicht des Nutzers zum Ergreifen von Sicherungsmaßnahmen zu begründen, nicht nur das Sicherheitsproblem, sondern eben auch die generelle Lösungsmöglichkeit bekannt sein. An die Bekanntheit dürften indes dieselben Maßstäbe anzulegen sein.[43]

c. Technische Zumutbarkeit

Wenn davon ausgegangen werden kann, dass sowohl die Sicherheitslücke als auch die Möglichkeiten zu ihrer Behebung bekannt sind, so liegen darin bereits die wichtigsten Voraussetzungen für die Handlungsverpflichtung des Nutzers. Zusätzlich muss überprüft werden, ob dem Nutzer die Sicherungshandlung technisch zumutbar war. Die Ermittlung der Zumutbarkeit ist ein Prozess der Abwägung zwischen dem Ausmaß der Pflichten und dem drohenden Schaden am Rechtsgut bei Nichtergreifung der Maßnahmen.[44] Daraus ergibt sich, dass zumindest Maßnahmen, die ein hohes Maß an Expertise erfordern, technisch aufwändig und zeitintensiv sind, durch den Durchschnittsnutzer nicht geleistet werden können und müssen. Im Fall der R-Gespräche hat das AG Völklingen nicht nur festgestellt, dass ihm keine technisch möglichen Gegenmaßnahmen bekannt wären, sondern zusätzlich zum Ausdruck gebracht, dass es sich, gesetzt den Fall, eine Möglichkeit durch Einstellung an der Telefonanlage des Nutzers bestünde, nicht in der Lage sähe, diese zu ergreifen.[45] Auch der BGH hat sich dieser Schlussfolgerung angeschlossen. Wenn allerdings andere, technisch zumutbare Lösungen bestehen, so sind diese selbstverständlich zu ergreifen.[46]
Schließlich ist noch festzustellen, dass die technische Zumutbarkeit nur bei privaten Nutzern eine maßgebliche Rolle spielen kann. Grundsätzlich könnte man verlangen, für technisch anspruchsvolle Aufgaben einen Experten herbeizuziehen.[47] Bei privaten Nutzern dürfte dies allerdings regelmäßig im Rahmen der Abwägung einen zu hohen wirtschaftlichen Aufwand ergeben, so dass die Prüfung einer technischen Zumutbarkeit hier eher angebracht ist. Bei

---

[40] LG Flensburg, Urt. v. 16.9.2005 - 7 S 18/05, MMR 2006, 47, 48; ähnlich *Schütz*/*Gostomzyk*, MMR 2006, 11.
[41] BGH, Urt. v. 16.3.2006 - III ZR 152/05, NJW 2006, 1971, 1974; kritisch *Böttcher*, VuR 2006, 256, 259; mittlerweile wurde eine solche Datenbank aufgrund von § 66i Abs. 2 TKG eingerichtet, vgl. *Zagouras*, NJW 2007, 1914, 1916.
[42] Ebenso *Mankowski*, MMR 2006, 458, 460.
[43] Vgl. o. III.a.
[44] BGH, Urt. v. 19.12.1989 - VI ZR 182/89, NJW 1990, 1236, 1237.
[45] AG Völklingen, Urt. v. 23.02.2005 - 5c C 575/04, MMR 2005, 482, 483; *Grabe*, MMR 2005, 483, 485.
[46] BGH, Urt. v. 16.3.2006 - III ZR 152/05, NJW 2006, 1971, 1973 f.
[47] So LG Hamburg, Urt. v. 26.7.2006 - 308 O 407/06, MMR 2006, 763, 764; kritisch zu einem ähnlichen Fall *Solmecke*, K&R 2007, 138, 143.

kommerziellen Nutzern ist schon aufgrund des wirtschaftlichen Nutzens hauptsächlich auf die wirtschaftliche Zumutbarkeit abzustellen.[48]

d. Wirtschaftliche Zumutbarkeit

Konkret muss die Ergreifung der Maßnahme auch wirtschaftlich zumutbar sein. Während viele Lösungen kostenlos und nur unter Erbringung eines gewissen Zeitaufwands genutzt werden können, sind viele Vorsorgemaßnahmen maßgeblich davon abhängig, dass Leistungen Dritter in Anspruch genommen und auch vergütet werden.
Das Ergreifen einer Sicherungsmaßnahme ist zumutbar, wenn es nicht außerhalb eines angemessenen Verhältnisses steht.[49] Zu beachten sind in diesem Zusammenhang insbesondere die Wahrscheinlichkeit des Gefahreneintritts sowie die Intensität und Höhe des möglichen Schadens. Als ein Beispiel für kostenpflichtige Lösungen, die auch von Privatnutzern genutzt werden sollten, sind Virenscanner zu nennen, bei denen zusätzlich zum Erwerb der Software[50] ein regelmäßiges Update erforderlich ist. Für diese Dauerleistung müssen sowohl Telekommunikationskosten als auch die Gebühren des Anbieters eingerechnet werden.
Zusätzlich kann auch eine Rolle spielen, ob der Nutzer bereits ein hohes Eigeninteresse am Schutz hat, wenn z.B. wirtschaftliche bedeutsame Daten betroffen sind.[51]

e. Aktualität

Schließlich spielt in diesem Rahmen auch die Aktualität der eingesetzten Software eine wesentliche Rolle. Virenscanner bieten beispielsweise nur dann adäquaten Schutz, wenn sie regelmäßig auf neue Viren eingestellt werden.[52] Ebenso verhält es sich mit Updates von Software, um bestimmte Sicherheitslücken zu schließen. Die Bemessung der notwendigen Aktualität gehört demnach zur Bestimmung des Pflichtenprogramms des Nutzers.[53]

f. Das allgemeine Lebensrisiko als Begrenzung

Fraglich ist, ob eine Begrenzung der Haftung nicht erst im haftungsausfüllenden Tatbestand über das Mitverschulden nach § 254 BGB,[54] sondern bereits in der Haftungsbegründung aufgrund der Verwirklichung eines allgemeinen Lebensrisikos zu erfolgen hat.[55] Anders formuliert könnte der Anspruch des Geschädigten ausgeschlossen sein, weil die Schädigung des eigenen Computersystems durch Computerschadprogramme Dritter heutzutage als allgemeines Lebensrisiko angesehen wird.

---

[48] Vgl. *Spindler in:* Bamberger/Roth, (o. Fn. 12), § 823 Rn. 240; *Wagner* in: MünchKommBGB, (o. Fn. 3), § 823 Rn. 250 mwN.
[49] Vgl. *Lang*, JurPC Web-Dok. 205/2001, Rn. 8 ff.
[50] Es gibt allerdings auch effektive kostenfreie Lösungen.
[51] Ähnlich *Spindler in:* Bamberger/Roth, (o. Fn. 12), § 823 Rn. 240 mwN.
[52] *Heibey in:* Roßnagel, (o. Fn. 4), Kap. 4.5 Rn. 131.
[53] Beispielhaft für Virenscanner-Update: keine ständige Pflicht *Schmidbauer*, Schadensersatz wegen Viren, http://www.internet4jurists.at/news/aktuell36a.htm; wöchentlich oder kürzer *Koch*, NJW 2004, 801, 807; ebenso IT-Grundschutzhandbuch 2005, M 4.3.
[54] S.u. IV.
[55] Zur Einordnung des Merkmals bei der Prüfung *Mädrich*, Das allgemeine Lebensrisiko, 1980, 96 f.

Ein Schaden fällt nicht unter den Schutzzweck einer Norm, wenn er sich gerade nur als Verwirklichung eines allgemeinen Lebensrisikos darstellt.[56] Ein allgemeines Lebensrisiko kann vor allem dann vorliegen, wenn die von einem Nachteil betroffene Person den Gefahren unabhängig vom Eintritt der haftungsrelevanten Handlung, also meist dem Hinzutreten Dritter, latent ausgesetzt war.[57] Als sozial adäquat werden Einschränkungen bezeichnet, die im Rahmen des Soziallebens allgemein hingenommen und nicht mehr als Verletzung der allgemeinen Rechtssphäre empfunden werden.[58] Ein gewisses Maß an geschaffener Gefährdung wird nämlich von der Rechtsordnung geduldet.[59] Beispiel für die Realisierung eines allgemeinen Lebensrisikos wäre die Infektion mit einer Erkältung. Allerdings unterscheiden sich die Infektion mit einer Erkältung und die Computerinfektion. Gegen eine Erkältung oder Grippe kann man sich nur unzureichend schützen, es kommt vielmehr auf ein gut ausgebildetes Immunsystem an. Dieses kann man zwar fördern, aber nicht tatsächlich und sicher mit vertretbarem Aufwand aufbauen. Anders ist dies beim Computervirus. Durch die Installation eines Antiviren-Programms kann man sich tatsächlich vergleichsweise effektiv schützen. Hinzu kommt, dass die Viren- oder Trojanerinfektion ein eindeutiges Ärgernis darstellt und nicht allgemein akzeptiert wird. Sie wird regelmäßig unter dem Gesichtspunkt der Datenspionage und des Entzugs der Kontrolle über das eigene Computersystem als wesentliche Einschränkung und damit als Verletzung der allgemeinen Rechtssphäre empfunden. Diese Schlussfolgerung muss erst recht für andere, eher unbekanntere Gefährdungen gelten. Das allgemeine Lebensrisiko begrenzt den Anspruch aus § 823 BGB demnach nicht.

3. Ergebnis

Die Beurteilung, ob den Nutzer einer Computeranlage Verkehrssicherungspflichten zum Einsatz von Sicherungsmaßnahmen treffen, erfordert demnach mehrere Schritte, die jeweils in Abwägung des Aufwands und der Gefährdungslage zu beurteilen sind: Bekanntheit des Problems, Bekanntheit der Problemlösung, Technische Zumutbarkeit, Wirtschaftliche Zumutbarkeit sowie Beurteilung der notwendigen Aktualität

Die Betrachtung dieser Punkte kann durchaus zum Ergebnis führen, dass auch derjenige, der selbst nicht bewusst gehandelt hat, aber dessen Computersystem nicht ausreichend gegen Gefahren gesichert war, für Schäden einzustehen hat, die bedingt durch die nicht ausreichende Absicherung entstanden sind. Grund hierfür ist, dass ihn entsprechende Vorsorgepflichten treffen.

IV. Mitverschulden des Geschädigten, § 254 BGB

Der Anspruch könnte jedoch zumindest teilweise deshalb ausgeschlossen sein, weil der Geschädigte die ihm möglicherweise obliegende Pflicht zum Selbstschutz nicht beachtet hat. Ein Mitverschulden bei der Entstehung eines Schadens liegt u.a. vor, wenn der Geschädigte

---

[56] BGH, Urt. v. 6.11.1979 - VI ZR 254/77, BGHZ 75, 230; *Heinrichs* in: Palandt, BGB, 66. Aufl. 2007, vor § 249 Rn. 88; vgl. auch *Schiemann* in: Erman, BGB, 11. Aufl. 2004, § 823 Rn. 20; *Hager* in: Staudinger, BGB, 1999, § 823 Rn. B33 f.; BGH, NJW 1996, 1533; BGH, NVwZ-RR 1994, 400, 401.

[57] *Mädrich*, (o. Fn. 55), 43; *Deutsch*, VersR 1993, 1041, 1042.

[58] *Deutsch*, Allgemeines Haftungsrecht, 2. Aufl. 1996, Rn. 600; *Esser*/*Schmidt*, 8. Aufl. 1995, 63.

[59] *Heinrichs* in: Palandt, (o. Fn. 56), § 276 BGB Rn. 21; *Huber*, Verschulden, Gefährdung und Adäquanz, 304; *Esser*/*Schmidt*, (o. Fn. 58), 63.

eine vorhandene Gefahrenquelle nicht abgestellt bzw. nicht überwacht hat.[60] Der Geschädigte hat diejenige Sorgfalt zu üben, die ein verständiger Mensch im eigenen Interesse aufwendet, um sich vor Schaden zu bewahren.[61] Diese Pflichten gelten auch gegenüber dem seine Verkehrssicherungspflicht verletzenden Schädiger,[62] sofern die Gefahr erkennbar und vermeidbar war.[63]
Insoweit ist zu beachten, dass das Mitverschulden nach § 254 BGB in diesem Bereich im Grunde spiegelbildlich zu den Verkehrssicherungspflichten nach § 823 Abs. 1 BGB steht. Knüpft man an das zeitliche Element der Haftungszurechnung an, so zeigt sich, dass beim Schädiger gegenüber Dritten auf den Moment abgestellt wird, in dem sein eigenes System betroffen wird. In diesem Augenblick hat sich die Vernachlässigung seiner Verkehrssicherungspflichten realisiert. Beim Geschädigten wiederum verwirklicht sich in genau diesem Moment bzw. durch die unmittelbar bzw. kausal folgende schädigende Einwirkung die Gefahr zum Schaden. Schadenseintritt und „Schädigungshandlung" im Sinne eines Unterlassens der Ergreifung von Sicherungsmaßnahmen als Begründung der späteren Haftung decken sich folglich zeitlich, was die Bewertung als spiegelbildliche bzw. zusammenhängende Ereignisse bestätigt.
Dieser Befund deckt sich mit der gesetzgeberischen Wertung, Schädiger und Geschädigten bei der Behandlung ihres Verschuldens grundsätzlich gleich zu behandeln.[64] Ein Verhalten, das bei Eingriffen in fremde Rechtsgüter eine Ersatzpflicht zu begründen vermag, muss bei einem Eingriff durch einen Dritten in die eigenen Güter einbezogen werden und kann nicht zu Lasten des Schädigers gelten.[65] Auch kann vom Geschädigten grundsätzlich genausoviel verlangt werden wie vom Schädiger.[66] Schließlich sind dem Geschädigten eventuelles Spezialwissen bzw. Spezialfähigkeiten, also möglicherweise sogar ein Vorsprung in der Fähigkeit, Gefahren abzuwenden, anzurechnen, so dass der ihn treffende Sorgfaltsmaßstab sogar höher sein kann als beim Schädiger.[67]
Im Ergebnis kann der Schädiger dem Geschädigten, der ebenso wenig die notwendigen Sicherungsmaßnahmen ergriffen hat, dieses Fehlverhalten im Rahmen des Mitverschuldensvorwurfs nach § 254 BGB vorhalten. Folge ist eine Reduzierung bzw. Teilung des Schadensersatzanspruchs nach dem jeweiligen Grad des Verschuldens.[68]

V. Fazit

Während in Rechtsprechung und Literatur die Frage der Verantwortung bei Dialern und R-Gesprächen sowie für die Weiterverbreitung von Viren bereits aufgegriffen wurde, sind weitergehende Sicherheitsprobleme in ihren rechtlichen Implikationen bisher kaum bzw.

---

[60] *Looschelders*, Schuldrecht Allgemeiner Teil, 4. Aufl. 2006, Rn. 1018; *Oetker* in: MünchKommBGB, 5. Aufl. 2007, §254 BGB Rn. 29.
[61] BGH, Urt. v. 17.10.2000 - VI ZR 313/99, NJW 2001, 149, 150; *Lange*, Schadensersatz, 3. Aufl. 2003, §10 VI 1d; *Oetker* in: MünchKommBGB, (o. Fn. 60), § 254 Rn. 30; *Schiemann* in: Staudinger, (o. Fn. 56), § 254 Rn. 38.
[62] *Heinrichs* in: Palandt, (o. Fn. 56), § 254 Rn. 25 ff.; *Schiemann* in: Staudinger, (o. Fn. 56), § 254 Rn. 53.
[63] *Schiemann* in: Staudinger, (o. Fn. 56), § 254 Rn. 53, 55.
[64] *Deutsch*, (o. Fn. 58), Rn. 571; *Looschelders*, (o. Fn. 60), Rn. 1014.
[65] *Lange*, (o. Fn. 61), § 10 VI 1d.
[66] *Lange*, (o. Fn. 61), § 10 VI 2.
[67] *Deutsch*, (o. Fn. 58), Rn. 573; *Lange*, Schadensersatz, § 10 VI 2.
[68] *Looschelders*, (o. Fn. 60), Rn. 1015, 1037; *Oetker* in: MünchKommBGB, (o. Fn. 60), § 254 Rn. 105 ff., 113; *Heinrichs* in: Palandt, (o. Fn. 56), § 254 Rn. 59.

nicht behandelt worden. Geht es um die Frage, ob den Nutzer eine bestimmte Pflicht wie z.B. zur Installation einer Firewall trifft, sind aber jeweils die selben Fragen zu stellen. Die Pflichtenbestimmung lässt sich demnach in der hier vorgeschlagenen Art und Weise verallgemeinern. Festzuhalten bleibt, dass bereits dem durchschnittlichen Computernutzer im Rahmen des § 823 Abs. 1 BGB Verkehrssicherungspflichten zum Eigen- und in der Folge auch Drittschutz obliegen, wobei die Pflichtenbestimmung jeweils den Einzelfall zu betreffen hat, und die Beurteilung der Entwicklung auch der allgemeinen Rezeption von Sicherheitsproblemen unterliegt.